A Comparative Assessment of Electronic Voting

Prepared for Elections Canada by
Canada-Europe Transatlantic Dialogue

February 2010

Table of Contents

Executive Summary **7**

Introduction **9**

Part I: Methodology and Justification for the Cases Examined **11**
What is Meant by Electronic Voting and Internet Voting? What Types are Examined in this Report and Why Do We Predominately Focus on Remote Internet Voting? 13

Part II: Benefits, Drawbacks and Risks Associated with Internet Voting **15**
Benefits 15
Drawbacks and Risks 16
Public Attitudes 17

Part III: Canadian Municipal Trials **23**
Markham 24
Peterborough 26
Halifax 28
Municipal Trials and Developing a Model for Canada 31

Part IV: European Trials **33**
Estonia 33
Geneva, Switzerland 36
United Kingdom 39

Part V: Kiosk and Telephone Voting Methods **43**
Kiosk Voting 43
Telephone Voting 45
European Trials and Developing a Model for Canada 46

Part VI: General Considerations for Canada **49**
The Trade-off Between Accessibility and Security 49
Steps Needed to Achieve Internet Voting in Canada 55

Conclusion **57**

Bibliography **59**

Note to the Reader

This paper was prepared by the Strategic Knowledge Cluster Canada-Europe Transatlantic Dialogue for Elections Canada. Canada-Europe Transatlantic Dialogue is a network of experts on the European Union and European affairs funded by the Social Sciences and Humanities Research Council of Canada under its Strategic Knowledge Clusters program, with the goal of more effectively bringing research findings to stakeholders and the public. Authors of the report: Nicole Goodman, Jon H. Pammett, Joan DeBardeleben. Research assistance: Jane Freeland.

Executive Summary

In the past decade various types of electronic voting, particularly Internet voting, have won considerable attention as possible additional voting methods that promise to make the electoral process simpler and more efficient for political parties, candidates, election administration, and most importantly, for electors. Many types of Internet or remote voting have been implemented with varying degrees of success. While some systems have worked well, pilots of prototypes in other jurisdictions have been cancelled, some even before they were introduced, because of concerns or issues relating to security, technical reliability and privacy. The variable results of these projects highlight that there are important risks as well as benefits associated with Internet voting, and both should be weighed when considering including electronic voting as a method of voting in elections.

The models that enjoy success are effective because they have been tailored to meet the specific needs of a particular jurisdiction. The lesson behind these success stories for Canada is that no specific model should be directly copied for use here, although specific features of them may be. The development of an electronic voting model should be based on the requirements of the electoral process as well as the specific needs of electors and other affected parties. Compared to other countries where Internet voting has been trialled or implemented more fully, there appears to be sufficient accessibility and public support in Canada to introduce that method. Furthermore, the basis for a legal framework that supports Internet voting and a government mandate to conduct Internet voting research are important facilitating factors.

Various measures need to be considered before the next steps are taken for implementing Internet voting in Canada. These could include the gathering of additional data to measure public attitudes and those of political parties and candidates towards electronic voting. Consideration should also be given to establishing clear requirements that an additional method of voting would fulfill, as well as creating and consulting with an interdisciplinary committee of experts. Before selecting a type of software and specific system design features to suit Canada and drafting an electronic voting proposal to present before Parliament (including policies and procedures), further research should be conducted on various Internet voting models. This would lay the groundwork for designing an initial small-scale trial and then progressively increasing the number of electors who vote electronically with each additional trial. These are important aspects of the process which, based on the experiences of other jurisdictions and a review of the academic literature, appear to be both relevant and necessary toward creating a successful framework upon which an electronic voting model can be effectively developed in Canada.

Introduction

In the past decade the Internet has grown exponentially. Private companies, governments, civil society groups and individual citizens all rely on the Internet for business, networking, research and a variety of other uses. Today, citizens can use the Internet to conduct their banking, make purchases and donations, sign petitions, renew and apply for government licenses and pay their taxes. The power of the Internet to transform the nature of traditional service delivery, particularly to improve communication and access to information, has raised interest in its uses to enhance the accessibility of the electoral process as well. Its ability to create new participative spaces as well as expand existing ones suggests it has the capacity to improve accessibility to voting for many electors. Furthermore, the Internet's influence on other aspects of elections and government, such as campaigning, fundraising, membership recruitment, protest, lobbying and access to information for media and citizens, signifies that it now has an increasingly important relationship with electoral politics and will likely continue to have a considerable impact on the character of democracy in nations worldwide. The newly emergent concept of electronic democracy suggests it may be useful to further explore the potential of the Internet to improve the electoral process for parties, groups, election administration, and of course, citizens. At the same time however, there remain many concerns surrounding the notion of Internet voting, primarily related to public confidence and trust in the security of the voting process. The goal of this report is to assess the considerations involved in the potential introduction of various types of electronic voting in Canadian elections.

Canada is one of the more technologically advanced countries in the world and, at the federal level, has one of the most efficient and respected election administration bodies (KPMG, 1998). Compared to other member countries of the Organisation for Economic Co-operation and Development, Canada is among those with the highest percentage of households having access to a home computer and the Internet (OECD, 2009). National election studies indicate substantial public support for the introduction of Internet voting within all age groups, particularly among younger cohorts of electors. Currently, the *Canada Elections Act* includes a provision authorizing research regarding alternative voting methods and the potential to study and/or test electronic voting processes (*Canada Elections Act*, s. 18.1). Taken together, these elements provide a foundation of support for the implementation of electronic voting pilot projects in Canadian federal elections.

This report is structured in six sections. First, it presents a discussion regarding methodology and a justification for the cases selected and examined throughout the report. Second, it offers an overview of the meaning of electronic voting and the available types of such voting as well as an inventory of their potential benefits and risks. The report primarily examines remote Internet voting, since it has been the subject of the greatest number of trials, and appears to have the greatest potential to improve accessibility for electors and impact voter turnout. The section concludes with a brief analysis of public attitudes in Canada, drawing on data from Elections Canada surveys. Public attitudes toward Internet voting are examined, particularly expressed public willingness to make use of it, as well as reported rationales for not voting.

Third and fourth, the report proceeds with critical overviews of experiences of electronic voting trials in other jurisdictions. This portion is divided into two sections. The first pays special attention to the three large municipalities within Canada that have conducted Internet voting pilot projects: Markham, Peterborough and Halifax. The second addresses cases in Europe, including Estonia, Geneva and the UK, to give an overview of the scope and dynamics of the implementation of remote Internet voting projects on larger scales (either national or sub-national). An overview of these case studies addresses the models of development used to implement electronic voting and the benefits and risks associated with them, levels of public acceptance and public confidence in government and election administration, as well as the effect, if any, on voter turnout. Technical elements such as legal implications, financial cost, security considerations and specific methods of implementation are also reviewed where information is available. An overview of each group of jurisdictions is followed by an assessment of remote Internet voting from the examples and their potential applicability in Canada. Canadian and European lessons are examined separately given that their contextual differences make direct comparison difficult.

The fifth section of the report examines two other types of electronic voting, namely telephone voting and remote kiosk voting, and their potential implementation and effectiveness for Canada. Particularly, it assesses whether one or both of these methods could be used in conjunction with remote Internet voting.

Finally, the report examines what general assessments can be made, and lessons learned, from Canadian municipal and European trials, concerning the potential for electronic voting, particularly remote Internet voting, in Canada. It reviews considerations Canada may face in exercising such an undertaking – be they technical, cultural, political, economic or social. An overview of steps that could be taken in the development of a Canadian Internet voting model is also provided. The report concludes by offering an overview of general conclusions and suggesting directions for further research, particularly interdisciplinary projects with the co-operation of election officials, researchers and IT personnel.

Part I: Methodology and Justification for the Cases Examined

The material for this report comes from government documents, academic books and articles, newspaper and magazine articles, personal interviews and communications, and survey data where available and applicable. Aside from examining the theoretical literature addressing remote electronic voting, the report also closely examines trials that have taken place in Canada at the municipal level, notably the cases of Markham, Peterborough and Halifax, and at the local, state and national level in Europe by drawing on the experiences of Estonia, Geneva and the UK. All of the Canadian trials were initiated from and administered by municipal governments. The European cases by contrast, regardless of the level at which the remote electronic voting pilot took place, were all launched and overseen at the national level, although local authorities did have input. The difference in scales, contexts and the magnitude of issues associated with both the Canadian and European examples justify examining them as separate sets of cases, even though some elements may be closely related.

While the report examines Canadian and some of the more prominent European instances of remote Internet voting, we can initially consider the situation in the United States. Although widely discussed, there has been no actual implementation of Internet voting in regular American elections. Furthermore, the debate surrounding Internet voting in the USA is considered poorly informed because of a lack of research (Alvarez and Hall, 2004). The bulk of the discussion focuses on the technical requirements of Internet voting, and has not proceeded to a real-world implementation of such a project. In fact, some argue that many of the problems that have occurred in the trials are the result of insufficient testing (Alvarez and Hall, 2004).

There has been an abundance of research and smaller trials of Internet voting in the USA, such as a state-wide straw poll of Republican party members in Alaska in January of 2000, the Arizona Democratic Party primary in March of 2000, as well as an experimental project (Voting Over the Internet Pilot Project) as part of the Federal Voting Assistance Program (FVAP) in conjunction with the 2000 presidential election, and the 2004 Michigan Democratic Party's Democratic caucus vote. Nevertheless, no larger scale projects have been implemented because of a culture of uncertainty surrounding the safety and security of Internet voting (Alvarez and Hall, 2004; Alvarez and Hall, 2008; Mohen and Glidden, 2001). In addition, the recommendations of the major American voting reports, the California Internet Voting Task Force report, the Report of the National Workshop of Internet Voting and the Caltech/MIT Voting Technology Project, all warn against the introduction of Internet-based voting methods given the perceived level of risk associated with them – notably the potential for fraud, vote buying and voter coercion as well as security issues and the threat of attacks (Alvarez and Hall, 2004). The advice of these reports serves to reinforce security concerns and acts as a deterrent from pursuing such projects or pilots.

All remote Internet voting projects that have been initiated for use in USA elections have been terminated in the planning stages of the projects. The 2000 California project is an important example of this. It was considered an ideal jurisdiction to trial Internet voting because the state possessed a high rate of Internet access (compared to the national average), an abundance of Internet related business and, according to survey research, general support for the notion of Internet voting. Prior to implementation however, the California legislature passed a bill,

The Digital Electoral System Act, which required the state of California to assemble a task force to study the feasibility of using technology in elections (Alvarez and Hall, 2004). The final task force report concluded that Internet voting could not be used as a replacement for existing paper ballot procedures for a variety of reasons relating to security (notably computer security and voter identification) and made two major recommendations: (1) that, for the time being, Internet voting be tested solely within the absentee voting process; and (2) that it be very gradually phased in throughout the state, after considerable additional research. Overall, the report's findings regarding Internet voting were very tentative and any recommendations to proceed with an Internet voting program were laced with caution (Alvarez and Hall, 2004; California Secretary of State Bill Jones, 2000).

Created to target absentee electors, the one major initiative, the Department of Defense's *Secure Electronic Registration and Voting Experiment* (SERVE), which developed as an extension of FVAP, was created to test Internet voting as an alternative to traditional absentee voting for military personnel, their dependents and overseas citizens. Though more than 6 million citizens qualified for the program, it was decided to only offer it to 100,000 people for the 2004 primary and general elections to allow for adequate testing and evaluation. Even on that reduced scale, the project was cancelled before it could come to fruition due to opposition from a small segment of the scientific community. Specifically, SERVE was terminated not because of its system design or architecture, but rather due to concerns surrounding the Internet itself and the view that any transaction conducted over the Internet is not secure and considered vulnerable to system breakthroughs. It has been observed that the report that raised these concerns failed to note that the threats associated with Internet voting are analogous to threats surrounding traditional absentee voting such as vote selling, buying and coercion and denial of service attacks that occur without the Internet (Alvarez and Hall, 2008).

Other major American research projects, such as the *National Workshop on Internet Voting* and the *Caltech/MIT Voting Project*, also take negative positions on the introduction of remote Internet voting and have helped to affirm the legitimacy of fears surrounding Internet voting (Internet Policy Institute, 2001; *Caltech/MIT Voting Project Report*, 2001). Despite recognizing its potential to enhance accessibility for certain groups of electors, these reports come to similar conclusions that such systems pose "significant risk," such as potential attacks to the elector's computer, the server and/or network as well as issues of ballot legitimacy and secrecy, and conclude that Internet voting should not be introduced on a large scale (Alvarez and Hall, 2004:23). A culture of uncertainty in the USA surrounding the notion of Internet voting has prevented serious research and testing.

While there is lack of testing and practical research in the USA, Europe by contrast has been a breeding ground for Internet election projects and, as a whole, can be considered to have advanced the furthest with respect to Internet voting technologies and approaches. The important differences between the USA and Europe in this regard are aptly highlighted by Alvarez and Hall in their most recent book, *Electronic Elections* (2008), on the applicability of electronic elections in the USA:

> When we published *Point, Click, and Vote: The Future of Internet Voting* in January 2004, we had little idea that we should have been publishing the book in Europe,

> not the United States. The road map we lay out in the book is being followed, just not in the United States. Instead, it is in countries like Estonia, Switzerland, the Netherlands, and France that e-voting experiments are being conducted (71).

Though the concerns raised in American literature are important, they are taken into consideration in Internet voting experiments in Canada and Europe. Furthermore, in these settings, the potential problems are examined in the context of real-life examples and pilots, rather than in theoretical discussions. Therefore, the remainder of this report concentrates on European as well as Canadian trials.

What is Meant by Electronic Voting and Internet Voting? What Types are Examined in this Report and Why Do We Predominately Focus on Remote Internet Voting?

The term electronic voting is a blanket term used to describe an array of voting methods that operate using electronic technology. There are three primary types of electronic voting, namely machine counting, computer voting and on-line or Internet voting.[1] With respect to the last of these types, there are four kinds of electronic voting that use the Internet; these include kiosk Internet voting, polling place Internet voting, precinct Internet voting and remote Internet voting (Alvarez and Hall, 2004). Kiosk Internet voting typically involves the use of a computer at a specific location that is controlled by election officials. This differs from electronic machine voting because, among other things, the ballot is cast over the Internet. Polling place Internet voting is conducted at any polling station through the use of a computer that is controlled by election representatives. Precinct Internet voting is analogous to polling place voting except that it must occur at the voter's designated precinct polling place (Alvarez and Hall, 2004). Remote Internet voting is voting by Internet from a voter's home or potentially any other location with Internet access.

The following section discusses the benefits and risks associated with Internet voting in general, primarily concentrating on remote Internet voting. This is because, in the first place, in most of the literature addressing electronic voting the term 'Internet voting' has become synonymous with remote Internet voting and is addressed as such (Mercurio, 2004). Furthermore, remote Internet voting has the greatest potential to positively impact accessibility for voters. Internet voting machines that are either located at a polling station or another central location still require electors to travel to the poll or location. While in some cases travel to a central location such as a mall or supermarket may be convenient, their use still requires additional effort that voting from home or work does not. Finally, remote Internet voting is most consistent with the development of other political aspects of society that have changed with technology. While kiosks and machines can be useful, people are now using home computers to conduct more transactions than ever before and this will only increase in the next decade.

[1] Machine counting requires voters to punch a hole in their ballot which is then scanned and counted by a central computer. Computer voting or direct-recording electronic voting machines involve the use of either a keyboard, touch screen or some kind of pen or pointer and computer terminal and are immediately factored into the tally of votes (Parliamentary Office of Science and Technology, 2001).

Part II: Benefits, Drawbacks and Risks Associated with Internet Voting

Benefits

Proponents of electronic voting, particularly Internet voting, make a number of arguments in favour of its implementation. These are related to technology, social issues and election administration. First, electronic voting has the potential to make the **voting process easier** and **more accessible** for electors. This is especially true for remote Internet voting and telephone voting given that ballots can be cast from any computer with an Internet connection or any working telephone. These latter methods substantially lower the cost of voting for many electors by creating many more access points from which they are able to vote. There is the potential to eliminate long line-ups at polling stations and better address accessibility issues for persons with disabilities, those suffering from illness, those serving in the military or living abroad, those away on personal travel, snowbirds and other groups of citizens such as single parents who may find it difficult to visit a traditional polling station. Additionally, remote methods of Internet voting, and in some cases kiosk Internet voting, afford electors the opportunity of being able to **vote at any time**, a feature that further enables electors' ability to cast a ballot.

With regard to special populations of electors, Internet (especially remote) and telephone voting may also be methods of engaging those voters who are considered the hardest to reach, particularly **young people** aged 18 to 30. These electors are most familiar with the technology, are the most frequent reported users and would likely benefit the most from the extension of remote types of electronic voting. Remote Internet and telephone voting seem to be especially useful ways of engaging young people away at university and who are not registered to vote in that particular constituency.

Second, Internet and telephone voting could allow **greater secrecy** for special populations of electors with disabilities (including visually or hearing impaired). By voting electronically and therefore unassisted, these electors are afforded a greater degree of anonymity when casting a ballot. Enabling secrecy for these groups enhances the equality of the vote.

Third, enhancing accessibility and creating more participatory opportunities for electors holds promise to positively impact **voter turnout**. Generally, the academic literature addressing electronic voting and turnout decline presents inconclusive results concerning whether the extension of on-line voting has a positive effect on electoral participation. In most cases where polling place voting machines that relied on the Internet for operation were used turnout did not increase. However, cases in which remote methods were implemented have produced mixed results. Though some areas, such as the UK, have not consistently noted increases, others, such as Estonia and Geneva as well as the Canadian municipalities, do report some instances of increased turnout. The length of time remote Internet voting options remain in place appears to be related to increases in both its use and in voter turnout.

Fourth, related to administration, Internet and telephone voting are claimed to produce **faster and more accurate election results**. Internet and telephone voting systems are said to deliver a faster official ballot tabulation process and are alleged to be more accurate than other types of machine counting (such as punching cards) which are sometimes criticized for error.

Fifth, over the long term all types of Internet voting have the potential to be **less expensive** to operate and execute than traditional paper ballots which require setting up and staffing polls. However, the start-up costs for machines or kiosks can be very high.

Finally, all types of Internet voting and telephone voting have the potential to improve the overall quality of ballots cast by reducing or eliminating ballot errors and by creating better informed electors. There can be **no ballot errors**, and, depending on the system, **no spoiled ballots** because the computer will not permit it. However, if the legal structure in a jurisdiction requires the option to spoil a ballot or allows for protest votes, a button can be added in some programs to give electors the option to cast a protest vote (or decline to vote). Furthermore, depending on the architecture of the Internet voting system, there is the possibility for additional information to be displayed regarding candidates and their policy positions in conjunction with the on-line vote. This would provide voters with basic information about the candidates and party platforms, and therefore better informing them to vote.

Drawbacks and Risks

Those opposed to, or skeptical of, electronic voting point to several drawbacks and perceived risks that are associated with types of Internet voting and telephone voting methods. The most prominently cited risk relates to **security**. Threats of computer viruses or hacker-orchestrated 'denial of service' attacks are most commonly mentioned as problems that could compromise an election and public confidence in electronic voting. This concern is most prevalent with regard to the security of personal computers. In light of this, the maintenance of **ballot secrecy** is presented as an issue when using computers that are unprotected, located in public places, or which may be susceptible to virus attacks. Other potential technical problems or issues include power outages or malfunctions in Internet connectivity as well as the possibility of servers shutting down or crashing. The reliable recording and storage of votes is also an important consideration.

Second, problems with **access** are raised. The material on remote Internet voting discusses the potential for a "digital divide", which can occur in two ways. There is a digital divide between those who have home computers with Internet connections and those who do not. Second, there may be a digital divide between those who have faster access and those who have slower connections and hence lower quality access. People with higher incomes are more likely to be able to afford access. Furthermore, access is often less expensive and of higher quality in urban areas. Those with lower incomes and who live in rural areas are at a disadvantage. Therefore, the extension of Internet voting has the potential to create divides with respect to many socio-economic variables, namely income, education, gender, geography and race and ethnicity. These potential divides could be problematic for participation and representation.

Third, it is said that remote Internet and telephone voting present greater opportunity for **fraud** and **coercion** or vote-buying. Fraud occurs when someone votes on another's behalf without their permission, whereas coercion or vote-buying takes place when a voter is pressured by others to vote in a way that he or she would not have otherwise. Both present problems for ballot integrity since it is important that every vote cast be tallied as the voter intended. There is additional opportunity for fraud in electronic voting systems if voter notification cards, which contain unique passwords required to cast a ballot, are intercepted. In the case of ballots not cast in person it is more challenging to verify a voter's identity. Remote voter authentication can be a problem since it may be difficult to confirm that the person voting is actually who he or she claims to be. While digital signatures and passwords can help, they are not foolproof and could potentially be shared.

Fourth, the issue of **voter education** is cited as a concern. A lot of time and money must be invested to ensure that the public is aware that electronic voting is an option and that voters are able to understand and use the on-line system to cast a ballot. Without correct marketing and advertising it will be difficult to engage electors.

Fifth, **privatization** is a concern when electoral administrators cede control to a hired firm. Contracting elections out to private companies to run the electronic operations has negative implications for some people, and hence has the potential to negatively impact public confidence and trust in government and elections.

Finally, perhaps the most significant social concern is the threat of **disintegration of social capital** or civic life. The proliferation of electronic election services has the power, some say, to alter the nature of electoral participation by causing more electors to vote alone instead of at a polling place with others. This threatens to erode civic life, local social networks and groups related to elections (see Putnam, 2000).

While this provides a general treatment of the major advantages and drawbacks to Internet and telephone voting, there are pros and cons which are unique to each particular electronic method. These are presented in Table 1 (pp. 19–21). It also includes instances where these methods have been trialled or implemented.

Public Attitudes

Implementation of electronic voting would not be possible without a culture of support from citizens. It is important that the public retain a strong sense of confidence and trust in the electoral process and be generally supportive of the notion of electronic voting. In the jurisdictions to be described in the next part of the report, where types of electronic voting have been successfully trialled, developed and maintained as a component part of the vote in elections there has been no widespread opposition to its use. Any public concerns about it seem to have been addressed at the time. Although there is no directly comparable data for Canadians' public attitudes over time since the wording in survey questions differs slightly from year to year in Canadian election studies, it is possible to gain an understanding of general public attitudes toward Internet voting and whether electors would use the service if it were an option. Both acceptance of Internet voting and reported levels of use are important considerations in developing a model or trial of Internet voting. To assess whether the Canadian public would be

supportive of the introduction of alternative voting methods in elections at the federal level the report draws upon data from Elections Canada survey data from 2000 to 2008.[2]

Elections Canada survey data offers important insights regarding the Canadian publics' expressed likelihood to vote by Internet. Overall, the data shows that there is a moderate increase in the proportion of respondents who report being likely to make use of Internet voting over time. While in 2000, for example, 47 percent of respondents report being likely to vote on-line, in 2008, interest rose to 54 percent of respondents. We also see that respondents' reported likelihood to use on-line voting either increases over time or remains consistent for all age groups. In fact, aside from those electors over the age of 54, a majority of respondents in all age groups indicate that they would be likely to make use of on-line voting if the service were available.

Except in 2008, where the numbers are virtually identical, non-voters responding to election surveys are more inclined than voters to say that they would be more likely to vote on-line in the future. In fact, a greater proportion of respondents aged 18 to 34 reports being likely to make use of on-line voting than having voted.[3] This suggests that some non-voting electors may be encouraged to participate through Internet voting. Overall, the figures suggest that the extension of Internet voting may be a useful way of appealing to younger electors as well as encouraging some non-voters to participate in the electoral process.[4] It also highlights that older electors are less likely to make use of on-line voting.

Another important consideration with respect to public attitudes is the rationale provided by electors for not voting. If the extension of Internet voting is to encourage participation then it should address one or more of the reasons respondents cite for not casting a ballot. Elections Canada survey data reveals that among the general population in all survey years time constraints or accessibility issues are mentioned most commonly to account for respondents not voting. For example, three of the top four reasons respondents provided as rationales for not voting in 2008 include being too busy (16 percent), traveling or holidays (16 percent) and their work or school schedule (11 percent). In 2006 by comparison, 27 percent of respondents reported not voting because their work or school-related obligations prevented them from casting a ballot. In 2004, two of the top four reasons mentioned for not voting were being too busy with work (12 percent), or personal and family life (11 percent). Twenty-seven percent of respondents rationalized not voting in the federal election in 2000 by citing a lack of time or work obligations. In addition, reasons for not voting, such as illness, absence from the country or constituency, and missing registration information (including poll location), could potentially be remedied with an available remote Internet voting option.[5]

---

[2] This comprises data from four federal elections in 2000, 2004, 2006 and 2008.

[3] For instance, whereas 63 percent of youth aged 18 to 24 reported voting in 2008, 70 percent said they would be likely to vote on-line if it were an option. Among those electors aged 25 to 34, self-reported voter turnout was 62 percent, while 67 percent report being likely to make use of Internet voting.

[4] However, since voter turnout is often over-reported in election surveys there is also the chance that likelihood of making use of on-line voting is being over-reported as well. Voting is typically over-reported for reasons relating to social desirability.

[5] See Table 4, page 312 in Lawrence LeDuc and Jon H. Pammett, "Voter Turnout in 2006: More than Just the Weather", in Jon H. Pammett and Christopher Dornan, eds., *The Canadian Federal Election of 2006* (Toronto: Dundurn, 2006).

Table 1: Benefits and Drawbacks of Various Electronic and Remote Voting Methods

System Type	Benefits	Drawbacks and Risks	Where Method Has Been Used[6]
Remote Internet voting	– Convenience and accessibility for electors who have computers with Internet access at home, at work, or abroad; and for certain groups of electors (persons with disabilities, the military, single parents, electors who are traveling, etc.) – Flexible voting time for electors – Flagging of ballot errors – Replication of ballot images without voter information for counting or audit purposes – Lower cost than traditional methods – Potential to increase voter turnout – Potential to enhance electoral efficiency – Faster and more accurate election results – Elimination of long line-ups – Instant absentee ballot – Font size and screen language can be modified	– Limited access to Internet or limited understanding on part of some electors – Possibility of stolen voter packages or identification cards – Misuse of elector's ID card and personal information voting by others without the knowledge of the elector – Difficulty verifying voter ID – Possible pressure on electors to vote a certain way if in the presence of others – Hacks or viruses attacking the system and altering election results – Technical difficulties, programming errors or server malfunctions – Inaccuracies on the voters' list, resulting in one elector receiving a card intended for another elector	– Australia (for military and persons with disabilities only and the project has since been cancelled), Austria, Canada, Estonia, Netherlands, Switzerland, USA (for military only project was abandoned), UK (project also cancelled)
Kiosk Internet voting	– Placement in convenient high-traffic locations (e.g. malls and supermarkets) – Flexible voting time for electors – Flagging of ballot errors – Replication of ballot images without voter information for counting or audit purposes – Potential to help address the voting needs of certain groups of electors (persons with disabilities, single parents, etc.) – Potential to enhance electoral efficiency – Faster and more accurate election results – Elimination of long line-ups	– Lack of paper trail to allow auditing and recounts – In the case of a power outage, no alternate method is available – Expenses of machines – Software can sometimes be unreliable – Electors may leave the voting screen before ballot is officially cast – Hacks or viruses attacking the system and altering election results – Electors may be pressured to vote a certain way if in the presence of others – Technical difficulties, programming errors or server malfunctions – Machine updating and cost	– France

[6]Country information taken from www.tiresias.org.

System Type	Benefits	Drawbacks and Risks	Where Method Has Been Used[6]
		– Candidate representative's scrutineer function may be diminished – Inaccuracies on the voters' list could result in one elector receiving a card intended for another elector	
Polling place Internet voting	– Eliminates mismarked or spoiled ballots and other invalid results – Programmable machines to dispense ballots for any riding – Removal of authentication questions so voter identification is most similar to the traditional process – Assistive devices to improve accessibility for electors with disabilities – Faster and accurate election results – Font size and screen language can be modified	– Auditing and recounts can be questioned if there is no paper trail – In the case of a machine failure (i.e. power outage) no alternate method is available – Machines are expensive – Software can sometimes be unreliable (many of these machines have a negative reputation based on failure in USA trials) – Electors may leave the voting screens before their ballot has been officially cast – Little advantage for electors in terms of convenience – Machine updating could also be an issue and costly	– Australia, Belgium, Brazil, Canada, Finland, France, Germany, India, Ireland, Netherlands, Norway, Portugal, Spain, Switzerland, UK, USA
Precinct Internet voting	– Elimination of mismarked or spoiled ballots and other invalid results – Programmable machines to dispense ballots for any riding – Removal of authentication questions so voter identification is most similar to the traditional process – Assistive devices to improve accessibility for electors with disabilities – Faster and accurate election results – Font size and screen language can be modified	– Auditing and recounts can be questioned if there is no paper trail – In the case of a machine failure (i.e. power outage) no alternate method is available – Machines are expensive – Software can sometimes be unreliable – Electors may leave the voting screens before their ballot has been officially cast – Little advantage for electors in terms of convenience – Machine updating could also be an issue, and be costly	

System Type	Benefits	Drawbacks and Risks	Where Method Has Been Used[6]
Telephone voting	– Convenience and accessibility for electors who have telephones; and for certain groups of electors (persons with disabilities, military, single parents, electors who are traveling, etc.) – Flexible voting time for electors – Flagging of ballot errors – Familiar technology, especially for those familiar with telephone banking – No ballot printing – Fewer election staff and poll locations – Less costly – Potential increase in voter turnout – Enhance electoral efficiency – Eliminate long line-ups	– Traditional recount not possible because no paper trail – Possibility of stolen voter packages or identification cards – Difficulty verifying voter ID – Must ensure candidate representative's function is written into the program (e.g. Halifax candidate module) – Electors may be pressured to vote a certain way if in the presence of others – Possibility of telephone lines overloading or phone service interruption – Inaccuracies on the voters' list could result in one elector receiving a card intended for another elector	– Netherlands, UK

Part III: Canadian Municipal Trials

To date, the Internet has been used to conduct a number of elections in Canada at the local level. The following section examines the experiences of Markham, Peterborough and Halifax with remote Internet voting to shed light on the potential of an Internet voting system in Canada. To date, six provinces have passed legislation as part of their respective *Municipal Elections Act* affording municipalities the opportunity to either implement alternative voting methods or some form of electronic voting, or to pass a bylaw that would authorize the use of alternative voting methods. Alberta, British Columbia, New Brunswick, Nova Scotia, Ontario and Saskatchewan have all done so (see municipal or local government election act of each province).[7] Though the option of using another method of voting is written into Ontario and Nova Scotia legislation, before implementing an alternative approach it was required that the local councils of Markham, Peterborough and Halifax pass bylaws specifying the type of method they wished to use and a rationale for its execution.[8] Along with this, the three municipalities created a formal list of procedures to be followed and forms to be used in the context of electronic voting. This was done for Internet and vote tabulators in the cases of Markham and Peterborough and Internet and telephone voting for Halifax (Brouwer, August 27, 2009; Grant, August 25, 2009).

There have been many instances where Internet voting has been actively used in elections in Canada, but these occurrences were all at the local level, either in municipalities or townships. The first experiences with electronic voting by the Internet occurred in 2003. These trials occurred in the town of Markham; in six municipalities in Stormont, Dundas and Glengarry (as part of a joint trial); and in five municipalities in Prescott-Russell (City of Peterborough, 2005).[9] In 2006, Markham and Peterborough used the Internet in their municipal elections, as did eight townships throughout Ontario who also offered telephone voting with an Internet option.[10] In 2008, Halifax, and the Nova Scotia towns of Berwick, Windsor, and Stewiacke, conducted their municipal and school board elections by incorporating the Internet and telephone voting as an alternative voting method and Halifax recently implemented an expansion of that approach in a September 19, 2009 by-election. In this report we focus on experiences of Markham, Peterborough, and Halifax, since these jurisdictions adopted more developed models and also have higher populations than the other cases noted above.

---

[7] Prince Edward Island also has legislation approving the use of electronic voting, but only for referendums or plebiscites.

[8] Halifax had to pass two separate by-laws for the 2008 and 2009 elections given that the 2008 election only offered electors the opportunity of voting online for three days during the advance poll, whereas in the 2009 election Internet and telephone voting were an option for the entire election period including election day (Grant, 2009).

[9] Ten of these municipalities used both Internet and telephone voting in their elections. The electronic services in these elections were supplied by CanVote, a company based in L'Original, Ontario. Markham only offered Internet voting in addition to their paper balloting; the Internet voting portion of the election was supplied by ES&S. The Halifax and other Nova Scotia elections were conducted with Intelivote, a Nova Scotia based company. In terms of turnout, East Hawkesbury, with only 3,100 electors, experienced a turnout rate of 65 percent, South Dundas with 8,417 electors had a turnout of 58 percent, North Dundas with an electorate of 8,289 had an overall turnout of 48 percent, South Glengarry with 10,988 electors had a turnout of 53 percent, and North Glengarry with 8,900 electors had an overall turnout of 60 percent. The average voter turnout in 2003 for all eleven municipalities in these regions was 52 percent (City of Peterborough, 2005; Smith, August 26, 2009).

[10] These townships include Addington Highlands, Archipelago, Augusta, Cobourg, Edwardsburgh–Cardinal, Perth, South Frontenac and Tay Valley and their elections were also conducted by Intelivote (Intelivote, 2009).

Markham

Rationale for introducing electronic voting

Markham was the first municipality in Canada to introduce electronic voting as part of a comprehensive engagement strategy to increase participation in elections.[11] By increasing the range of services available to electors and making voting more convenient for residents, the Town of Markham hoped to not only increase electoral involvement, but also have a positive effect on voter turnout. In addition to the Internet voting option, vote tabulators were introduced as part of the engagement strategy to help incorporate electors with disabilities (including visually or hearing impaired) and allow them to cast a secret ballot. Tabulators had audio, touch and sip and/or puff abilities to enable these groups of electors to vote unassisted. Tabulators were also incorporated because the town believed they provide a more efficient counting mechanism than traditional tabulation procedures (Brouwer, August 27, 2009).

Development, technical features, cost and general operations of the Markham model

Prior to introducing electronic voting, the town conducted considerable research in anticipation of the 2003 and 2006 projects. Though more extensive research was carried out prior to 2006, some of these initiatives included evaluations of trials in other jurisdictions; a comparative risk analysis of traditional, Internet and other types of voting; consultations and recommendations from information technology companies; and examination of public attitude data from the Delvinia reports (Brouwer, August 31, 2009). The electronic model used by Markham included the option of remote Internet voting in advance polls during the 2003 and 2006 municipal elections as well as the use of optic scan vote tabulators in every polling station on election day. The electronic portion of the elections was run by Election Systems & Software (ES&S), of Omaha, Nebraska, a company that previously conducted multi-channel voting trials in the U.K. Markham paid ES&S $25,000[12] in 2003 and $52,000 in 2006 for the development, execution and operation of the Web site.[13] The vote tabulators were rented to the town at an additional cost of around $160,000 per election (Town of Markham, 2007).

On-line voting was only offered during the advance polls, and electors wishing to vote in this manner were required to pre-register. In 2003, electors were able to vote on-line during a five-day period and in 2006 the advance polling period lasted for six days.[14] Every elector received an on-line registration package by mail as part of the voter notification process. The rationale behind pre-registration was that it would serve as an additional security precaution and would give the town a better sense of which electors opted to use electronic voting. When electors registered they were prompted to create a unique security question whose response was required before casting their ballots. Registration also removed elector names from the manual voter list and they no longer had the option of voting at a traditional polling station. Upon registering, electors were also mailed a unique PIN. Use of the PIN and the response to the unique security

[11] Previously remote Internet voting had been trialled in some small townships in 2000 (Nicholson, September 23, 2009).
[12] Markham was able to negotiate such an excellent price on the contract given that the company was new to Canada and wanted to break through the market here (Brouwer, August 27, 2009).
[13] Printing, postage, communications and IT resources were an additional cost. In 2006 for example Markham spent $104,000 in additional costs related to Internet voting (Town of Markham 2005, 2007).
[14] In 2003 electors were able to vote from November 3rd to 7th and in 2006 from November 4th to 9th.

question allowed electors to vote on the Town of Markham Web site (Brouwer, August 27, 2009; Flaherty, August 28, 2009; Town of Markham, 2007).

The Town of Markham also took a unique outreach approach to inform its electors of the electronic voting service by working with Delvinia Interactive, a firm that specializes in creating digital experiences to create awareness of on-line voting. Delvinia created an interactive Web site that not only encouraged electors to register to vote on-line and informed them of how the process worked, but also educated them on the importance of voting. The Web site also included links to the various candidates' Web pages in case electors wanted to learn more about them or their mandates. The town advertised both the Web site and on-line voting through mailings, fridge magnets, print ads, in malls and by e-mail and telephone. This aggressive marketing approach is very likely one of the keystones to the success of Internet voting in Markham, and the notable increases in voter turnout. The same services were used in both election years. (Froman, October 2, 2009; Froman, December 8, 2009).

Model success and elector and government feedback

While turnout overall remained unchanged in the 2003 election (28 percent), turnout in the advance polls increased by 300 percent. To put this in perspective, voter turnout in most other Ontario municipalities declined during the 2003 election. Markham electors had the option of voting from home, their workplace, a library or public place where Internet was available as well as touch-screen kiosks that were set up in city hall (Sibley, 2003). In 2003, 12,000 out of 150,000 electors pre-registered to vote on-line and slightly over 7,000 voted on-line. In 2006, advance voting on-line increased by 48 percent, as 10,639 voters chose to use the service to cast their ballots (Internet News Unlimited, 2006). Eighteen percent of all votes cast in 2006 were electronic ballots, a one-percent increase from 2003, and a 38-percent increase in turnout overall (CANARIE, 2004). Public attitude data that was collected by Delvinia highlights use of and satisfaction with on-line voting in Markham.

In terms of remote location, 82 percent of electors who voted on-line did so from home and 88 percent of on-line voters cited convenience as the primary reason for doing so (Delvinia, 2007).[15] When asked if they would like to see on-line voting offered in elections at other levels of government 90 percent report being very likely to vote using the Internet in a provincial election and 89 percent in a federal election (Delvinia, 2007). These percentages indicate that there is strong public support for remote Internet voting in the Town of Markham, at least among those who use the service. In addition, a portion of previous non-voters (25 percent in 2003 and 21 percent in 2006) declared that they had decided to cast a ballot because of the convenience of Internet voting (CANARIE, 2004; Delvinia, 2007). One hundred percent of the voters who voted on-line in 2003 reported they would vote on-line again in the future and 91 percent in the 2006 survey indicated they would be "very likely" to do so (CANARIE, 2004; Delvinia, 2007). Overall, based on the positive public feedback and increase in turnout, Markham plans to continue to refine its model and employ a similar electronic strategy in the forthcoming 2010 election.

[15] These statistics are based on the 2006 election.

Peterborough

Rationale for introducing electronic voting

The rationale behind the introduction of Internet voting in Peterborough was to reduce the need for proxy vote applications and to enhance accessibility for electors, creating more opportunities for them to cast a ballot. In addition, the city was impressed by the increase in voter turnout in Markham's advance polls in 2003 and perceived on-line voting as a means of increasing turnout in the municipality. The potential to lower election costs was also an important consideration. Overall, the extension of Internet voting was seen as a positive step toward making elections more accessible by creating more voting options for electors (City of Peterborough, January 30, 2006; Wright-Laking, November 23, 2009).[16]

Peterborough initiated electronic voting for the first time in its 2006 municipal election and like Markham plans to continue and expand the use of electronic voting in its 2010 election.[17] Peterborough is demographically different from Markham, in that it is less urban, and has a smaller electorate with 52,116 electors. Nevertheless, its experience with electronic voting was very similar to that of Markham. A large percentage of its electors have home computers with access to the Internet.[18] Peterborough is particularly interesting because it has a very large senior population (the second largest in Canada) and so to see a high rate of use among older electors highlights that remote Internet voting is not just something to attract young people.

Development, technical features and general operation of Peterborough's model

Prior to the introduction of Internet voting, the City of Peterborough did not collect public attitude data to gauge electors' reactions toward the service; however, they did analyze previous cases as well as different Internet voting providers and the types of alternative voting methods available. They also closely reviewed the ability to provide Internet voting and vote anywhere technology. The city also implemented an aggressive promotional campaign to inform electors of the service, which primarily involved visiting seniors' residences and community centres in hopes of appealing to older electors. Like Markham, Peterborough chose to use remote Internet voting for a five-day period in its advance polls and introduced vote tabulators into all polling stations on election day.[19] City officials awarded the electronic election contract to a Toronto-based company, Dominion Voting Systems, for a total cost of $180,400, including the rental fee for the tabulators.[20] The system operated on a two-step process very similar to the one used in Markham (City of Peterborough, January 30, 2006; Wright-Laking, October 1, 2009; Wright-Laking, November 23, 2009).

---

[16] By using Internet voting and vote tabulators, the city of Peterborough was able to reduce the cost of the 2006 election by less than the 2003 budget (City of Peterborough, January 30, 2006).

[17] The Clerk's office hopes council will approve continuous Internet voting in the 2010 election right up until and on election day (Wright-Laking, October 1, 2009).

[18] Although the City of Peterborough is unsure of exact percentages in terms of home computers and Internet access, it reports that access is relatively high within the area (Wright-Laking, October 1, 2009).

[19] Twenty-one vote tabulators were used for faster and more reliable reporting of election results as well as to reduce manpower and costs (City of Peterborough, January 30, 2006).

[20] This price excludes PST and GST (City of Peterborough, January 30, 2006). This was the first time Dominion Voting Systems had provided Internet voting (Wright-Laking, October 1, 2009).

All electors on the voters list were mailed a notice of registration card or letter with, among other information, a unique elector identifier (EID). To access the on-line election services electors were required to login to the system prior to registering using their EID as well as retyping a security code called a CAPTCHA challenge[21]. To register, electors were required to provide their address (as shown on their notice card) and their year of birth. They also had the option of choosing whether they preferred to have their PIN mailed (as in the Markham trials) or e-mailed to them. Registered electors were then either mailed or e-mailed another card with a PIN. Both the PIN and the login information (EID number and CAPTCHA challenge entry) were required prior to casting a ballot on the City of Peterborough Web site (City of Peterborough, 2006)

Model success and elector and local government feedback

Overall, the introduction of electronic voting in Peterborough can be considered a success. Public reaction to the introduction of Internet voting was positive and although initially negative media coverage was an obstacle, this was overcome by providing media sources with additional resources and educating them about the Internet process and the security of the system (Wright-Laking, October 1, 2009; Wright-Laking, November 23, 2009). No security issues or risks required attention. The City of Peterborough reports that they put "tremendous security methods in place and felt very comfortable the system was secure" (Wright-Laking, November 23, 2009). The only drawback of the process cited by city officials was that Internet voting was limited to advance polls only and this is something they would like to see expanded in future elections (Wright-Laking, November 23, 2009).

There was no noticeable effect on turnout overall (it remained unchanged from 2003 at a rate of 48 percent), but turnout in the advance polls was moderately higher than the figures for 2003 (Hoover, August 27, 2009). The increase in advance turnout may be a consequence of the fact that aside from the on-line polls, only one traditional advance polling station was open to the public. Also, turnout may have been artificially high in the 2003 election given that there was a referendum question on the ballot (Wright-Laking, October 1, 2009). In all, 14 percent of electors who voted cast their ballots over the Internet (3,473 of 25,036). The largest group of on-line voters was baby boomers (City of Peterborough, 2009; Wright-Laking, October 1, 2009). Specifically, 70 percent of on-line voters were 45 and older, and the highest rate of use was among electors aged 55 to 64. Only 14 percent of those aged 18 to 34 voted on-line (Sawatzky, December 9, 2009). The higher rate of use among baby boomers is interesting because most survey data indicates that young people are more inclined to report using, or saying they would make use of, Internet voting than other cohorts of electors. If seniors, or older cohorts of electors, are interested in making use of on-line voting, its implementation is more likely.

[21] CAPTCHA (Computer Assisted Program to Tell Computers and Humans Apart) is a security procedure whereby the user is prompted to re-type a series of distorted characters located in a blurred box (Bousquet, 2008; Smith, August 26, 2009).

Halifax

Rationale for introducing electronic voting

Halifax Regional Municipality (HRM) first introduced remote Internet voting in its municipal and school board elections in 2008 as part of a pilot project that sought to establish the viability and reliability of electronic voting. The municipality decided to offer remote Internet and telephone voting, given that voting over the phone appealed to a wider demographic; especially older electors who might have greater difficulty using the Internet. Furthermore, HRM contains both an urban core and suburban areas, so while some areas are highly connected to the Internet, other parts are only now getting Internet connectivity. By implementing both remote Internet and telephone voting Halifax offered those residents who have limited or no Internet access the possibility of voting electronically (Mellett, September 29, 2009).

Prior to the 2008 trial, HRM researched electronic options for three years and closely monitored the experiences of other municipalities that had used the Internet as a voting method. There were five main principles to which Council wanted the introduction of an alternative voting method to adhere. These were, foremost, maintaining the integrity of the electoral system, as well as increasing voter choice by incorporating additional voting methods, potentially increasing voter turnout, improving cost effectiveness, and improving the speed of both tabulation and the reporting of results. The four most important considerations in the process were deemed to be outsourcing to a trusted partner, the level of security (HRM decided on two shared secrets)[22], the quality of the voter data (to control potential duplicates and have verifiable data), and finally a credible audit process to give voters confidence in the voting process. In the case of HRM this last consideration was accompanied by the development of a very detailed bylaw as well as a policies and procedures document (Mellett, September 11, 2009).

Development, technical features and general operation of Halifax's model

The trial included a potential 276,000 voters and was contracted to a locally established company, Intelivote, who had previously run elections for eight small Ontario townships in 2006,[23] and for two districts in the UK in 2007[24]. For a total cost of $487,151[25] Intelivote incorporated remote Internet and telephone voting as a component of the advance polls. The remote Internet and phone portion of the election took place during a three-day period two weeks prior to election day (Bousquet, September 18, 2008; HRM, January 22, 2008; Smith, August 26, 2009).

---

[22] There are different levels of sign-in security that may be selected with using remote Internet voting, namely pre-registration, just a PIN, or two shared secrets. Although using shared secrets requires the electoral office to have access to a reliable second data source and increases the complexity somewhat, HRM went with this option because officials felt it was more secure and had the greatest potential to affect turnout. HRM decided not to use pre-registration, unlike Markham and Peterborough, based on the UK's experience with it and how it greatly reduced electronic voting participation rates there. The use of only a PIN was deemed to be too insecure (Mellett, September 11, 2009).

[23] The largest of these townships was South Frontenac with a total of 18,528 voters (Bousquet, September 18, 2008).

[24] This includes the district of Rushmoor Borough (101,000 voters) and South Bucks (68,000 voters). Intelivote has now worked extensively in the USA, Bermuda, Bulgaria, Romania and Poland (Smith, August 26, 2009).

[25] This portion of the cost is just the contract with Intelivote. The actual election cost of $1.3 million, which is more expensive than a regular municipal election given that the school board elections were held simultaneously (Grant, 2009; HRM, January 22, 2008).

The Halifax experience differs slightly from the Markham and Peterborough projects given that electors were not required to register prior to using remote Internet or telephone voting – residents were instead able to choose to use the service at any time. Whereas in the other two trials electors who expressed a willingness to use remote Internet voting (by registering on-line) were taken off the manual voting lists, the technology used in the Halifax trials enabled voters to select their preferred method of voting when they wanted to cast a ballot and not before (Smith, August 26, 2009). The Halifax approach is also exceptional in that electors were able to spoil a ballot. Not being able to spoil a ballot is often cited as a major disadvantage of electronic voting systems since many typically do not offer an official way to decline a ballot. Intelivote created a "decline to vote" button which was presented along with the candidate names so that electors could exercise this right. Another important feature of the model used in Halifax is that voters were able to switch voting channels if they wished. For instance, an elector could start voting on his or her cell phone on the way home from work (e.g. vote for mayor) and then continue voting for the remaining positions (e.g. councillors and school board members) from his or her home computer (Smith, August 26, 2009).

To ensure security and anonymity, a specific set of steps was undertaken. Every resident of HRM on the voters list was mailed a letter explaining how to vote electronically and providing a PIN. At any point during the three-day period electors were able to log on to a secure Web site controlled by Intelivote or call a phone number and cast their ballot electronically. The on-line process required electors to complete a CAPTCHA challenge, and then use their PIN and date of birth to confirm their identity. Once these security steps were complete a menu prompted electors on how to vote for mayor, councillor and school board representatives (Bousquet, September 18, 2008).[26]

In terms of security more specifically, the system used in HRM (developed by Intelivote) used four levels of security checks. The first, a "penetration test", involved a contracted IT firm trying to break through the Intelivote system to evaluate whether existing security mechanisms were capable of adequately preventing another person or group from tampering with the system. The second check involved analyzing the encryption system used in the communication between computer servers.[27] The third was an external audit of the entire voting process undertaken by an auditing firm.[28] Finally, the fourth check analyzed the network's overall security to ensure prevention of attacks and problems (Bousquet, September 18, 2008).

[26] The telephone vote walked electors through a similar system (Bousquet, September 18, 2008). The telephone system is the same network used in *Canadian Idol* and can accommodate more than 6,000 calls at once (MacDonald, November 22, 2006).

[27] During an election computer servers share and pass on information regarding the votes; this information must be encrypted to prevent someone or some other server from gaining access to this information. In the case of Halifax the Intelivote servers are so close together that this is not really an issue, but it is taken into consideration as a general precaution (Bousquet, September 18, 2008).

[28] Halifax used Ernst & Young in 2008. The auditing process involves a careful examination of the treatment of the voters' list, the distribution of PINs and the protection of voters' identity (Bousquet, September 18, 2008; Grant, August 25, 2009; Smith, August 26, 2009).

Continuous by-election, model success and elector and local government feedback

Public acceptance and support of electronic voting in Halifax was relatively strong. As early as 2004, HRM began conducting polls in which more than 70 percent of respondents said they would be in favour of HRM implementing an electronic voting option. While 44 percent reported that voting at the polls was their preferred method, 35 percent indicated that they would prefer Internet voting if it were available. No objections were raised at council meetings and there was no public protest.[29] Though voter turnout did not increase overall (from 2004 to 2008 it dropped from 48 percent or 125,035 voters to 38 percent or 100,708 voters), turnout on advance voting days (where remote Internet and telephone voting were offered as options) increased by more than 50 percent (from 14,000 electors in 2004 to 29,000 electors in 2008) despite it only being offered for a three-day period (Mellett, September 11, 2009; Smith, August 26, 2009).[30] Though the 2008 election was deemed a close mayoral race it was also held near the Canadian federal election and this may have been an important factor in the lower turnout (Bousquet, October 19, 2008).[31]

Municipal officials were sufficiently pleased with the 2008 pilot project[32] that they recently conducted another remote Internet and telephone voting trial as part of a special by-election that took place on September 19, 2009 (Mellett, September 11, 2009). This time, however, the option to vote using the Internet or telephone from remote locations was continuous (from the first voting day up until and including election day).[33] Voter turnout was 35 percent, a 12 to 25 percent increase from turnout in the three previous by-elections (21, 10 and 23 percent respectively) and 75 percent of all votes cast were electronic (Mellett, September 29, 2009).

This by-election was also unique in that HRM launched a candidate module (designed by Intelivote), which allowed candidates the opportunity to track participation by searching electors by name or address to see if they had participated. This module was received well by all candidates and used by most of them to varying degrees. It was also positively received by election administrators, who reported being pleased that candidates' representatives were not crowding the polling place during the election. While candidates' representatives still had the legal right to attend the polls, being able to track participation on-line apparently eliminated the need to do this (Smith, October 3, 2009).[34]

Overall, HRM personnel are sufficiently pleased with the trials that they plan to eliminate a substantial number of polling stations in the 2012 municipal election. Council anticipates this

[29] There was only one letter in a local newspaper questioning the issue (Bousquet, September 18, 2008).
[30] It should be noted that turnout in the 2004 election saw a 12 percent increase given that there was a question regarding Sunday shopping on the ballot, which had been an important issue in the municipality (Smith, August 26, 2009). In addition, an important consideration is that although turnout overall did not increase, it did not decrease either, which it did in both provincial and federal elections held the same year (Mellett, September 11, 2009).
[31] HRM's 2nd advance polls were held the same day as the federal election, Tuesday, October 14, 2008, but the ordinary polls were held Saturday, October 18, 2008 (Mellett, November 25, 2009).
[32] Council rated it a 9 out of 10 based on their evaluation criteria (Mellett, September 11, 2009).
[33] This contract is also with Intelivote with an approved budget of $85,000. Electors were still able to vote by traditional paper ballots (Mellett, September 11, 2009).
[34] This module was not tested in 2008 because officials had concerns that it may make some changes to how campaigning occurs, but were ready to pilot it in the more controlled environment of a by-election (Mellett, September 11, 2009).

will result in "increased turnout, lower election costs, and happier electors" (Smith, August 26, 2009). If these considerations are accurate, the Halifax model may be an important methodology to consider in the development of an electronic voting program in other Canadian jurisdictions.

Municipal Trials and Developing a Model for Canada

The experiences of Markham, Peterborough and Halifax indicate some broad consequences when voter participation becomes more convenient (Hoover, August 27, 2009). While general conclusions cannot be drawn regarding the effect of alternative voting methods on overall turnout, these instances illustrate that there can be a positive effect on accessibility. The three most prominent communities to introduce electronic voting programs so far (notably remote Internet voting) are different in nature. Markham is urban, has a higher average income among its residents than the others, and is one of the largest municipalities in the Greater Toronto Area. The Markham community also has a high comfort level with and access to technology (Brouwer, August 27, 2009). Halifax, although the most urban and developed of the Atlantic municipalities, still has considerable undeveloped areas, some which are just gaining Internet access. It also has a larger electorate than Markham (approximately 276,000 electors in Halifax compared with 156,000 in Markham), is located in a different region of the country, and has contrasting contextual features and demographic characteristics. Peterborough's electorate consists of approximately 52,000 electors, is less urban, and its residents have a lower average income (Smith, August 26, 2009; Wright-Laking, October 1, 2009). Despite these demographic and cultural differences, the introduction of Internet voting was well received by the public in all three communities and is something residents would like to see continue. These examples illustrate the importance of public acceptance, and also that alternative voting methods can be effectively implemented in a variety of communities with different characteristics and in different contexts.

While the public opinion data cited earlier indicate that there is general public support for the extension of Internet voting, particularly among young electors, it should not be discounted that there may be some negative attitudes towards it. Discontent with electronic voting, even if it is not widespread and isolated to one area, is an important consideration and something that should be researched and surveyed further. However, evidence from Peterborough's experience suggests that older cohorts of electors may become comfortable with and make use of Internet voting, particularly if awareness is created among the group.

With respect to voter turnout, making assessments from these municipal cases regarding the impact of remote Internet voting on turnout is difficult given that, with the exception of HRM's recent by-election, remote electronic voting options were only offered for a specific time during advance polling and so it is not possible to know what effect these options might have had on overall turnout. The extension of remote Internet voting did have a positive impact on advance turnout in Markham and Peterborough (albeit very modestly in Peterborough). And, while it is difficult to evaluate how much turnout increased in Halifax's advance polls since they were only open for a three-day period, 30 percent of electors who voted in the 2008 HRM election did so electronically. Though overall turnout in Halifax decreased from the previous election, in 2004 there was a plebiscite on Sunday shopping held in conjunction with municipal elections, which

increased turnout in all municipalities.[35] Furthermore, turnout in the recent by-election increased substantially to 35 percent (the three previous special elections had voter turnout of 21 percent, 10 percent and 23 percent) (Mellett, September 28, 2009; Mellett, November 25, 2009). So, while we cannot evaluate the overall impact of remote electronic voting on turnout until there are more substantive trials, its effect in the recent by-election is promising.

Other important considerations can also be taken from these trials, particularly the marketing scheme employed in Markham and some specific elements from HRM's approach. Making electors aware of the availability of electronic voting methods and informing them of how they may access these services is an important prerequisite. The strong positive impact Markham experienced with respect to voter turnout may also very well be linked to the town's aggressive marketing campaign. This may also be the case with regards to the promotional campaign Peterborough targeted to older groups of electors.

The Halifax case is particularly valuable to study given that it did not require electors to pre-register to vote on-line, offered a "decline to vote" button enabling electors to refuse a ballot, offered telephone and Internet voting simultaneously, allowed voting for the whole election period in its most recent by-election, and implemented a candidate module that allowed for the maintenance of candidates' representatives for electronic ballots. This combination of features had the goals of reducing barriers to voting, maintaining the traditional integrity of the voting process, and increasing ballot accessibility. The absence of pre-registration in Halifax makes the remote Internet and telephone voting options of maximal utility.

Further, HRM's incorporation of both remote Internet and telephone voting was an important decision to maximize accessibility. While a majority of households in a given jurisdiction may have access to the Internet, many rural areas may experience limited connectivity and those with lower incomes may not be able to afford access. Instituting Internet kiosks in public places such as shopping malls, libraries and community centres is one method of making remote Internet voting more widely accessible to these groups of citizens, but the extension of remote telephone voting offers these electors the option of remote voting. Traveling to an electronic polling location may very well present as much of a barrier as traveling to a traditional polling station. In addition, the ability of Intelivote's system to allow electors to switch voting channels is a model of enhanced accessibility and efficient delivery of service. A multi-channel model such as this, where remote voting options are interchangeable, makes voting much more feasible for certain groups of electors, notably those who are out of the country, busy professionals and single parents as well as electors with disabilities.

Finally, the introduction of a candidate module, which allowed candidates' representatives to exercise the same scrutineer function they do in traditional polling places helps maintain tradition as well as the integrity of the voting process. Taken together, these features as well as the marketing campaign adopted by the Town of Markham are salient features that should be seriously considered in the development of a Canadian model because they add value to the electoral process while allowing for technological advancement.

[35] Turnout in 2000 is a more accurate comparison given that there was no plebiscite. It was 39 percent in 2000 (Mellett, November 25, 2009).

Part IV: European Trials

Estonia

The country of Estonia is a significant case with regard to Internet voting for several reasons. First, Estonia is the only country worldwide to have introduced remote Internet voting on a national scale. Second, its model of remote electronic voting incorporates plans to expand and incorporate other remote electronic voting methods, such as SMS text message voting, by 2011. Third, Estonia is the only country in the world to have legislated Internet access as a social right (Trechsel, 2007:9). Estonia is one of the most electronically enabled countries in Europe, rating fourth among the EU-25 in terms of the availability of on-line public services (Estonian National Electoral Committee, 2009). These elements, and the fact that Internet voting in Estonia can be considered an electoral success, make it an important case for examination, particularly to observe features that have supported and allowed for the successful operation of a remote Internet voting system.

Rationale for introducing remote Internet voting and necessary preconditions

The motivation to introduce remote Internet voting in Estonia was primarily to increase the number of voting methods that are available to electors and to make the process simpler and more convenient. One of the objectives of making the voting process more accessible was to increase turnout and dissipate feelings of political alienation, particularly among youth. The Estonian Parliament also felt remote Internet voting allowed for more efficient use of existing technical infrastructure, and that voting on-line remotely should be considered an essential convenience in modern society (Lumi, September 19, 2009; Madise and Martens, 2006). More generally, the Estonian government is focused on developing policies and services that are citizen-centric and highly inclusive (Estonian National Electoral Committee, 2009).

A number of key features were present that made introducing remote Internet voting viable and that have enabled it to work well in Estonia. These include the degree of Internet penetration and electronic readiness among citizens, a supportive political culture, a legal structure that addresses remote Internet voting, a digital identification system, modern infrastructure and government IT programs, as well as a partnership between public and private sectors (Alvarez et al., 2009; Lumi, September 19, 2009). Data from the European Commission reports that Estonia is among the top 12 in the European Union in terms of Internet penetration: 53 percent of all Estonian households own a computer, and 89 percent of these are connected to the Internet (Alvarez et al., 2009; Estonian National Electoral Committee, 2009).

Estonia has also taken great care to develop a legal framework that supports the development and use of remote Internet voting. This began with the passage of the *Digital Signature Act* in 2002, which allows citizens to use approved digital signatures to confirm their identity in on-line transactions, including government transactions and voting. While the USA has also legislated digital signatures, Estonia is the only country to have simultaneously mandated and introduced an identity card with an embedded digital certificate. The card is the basis for the Estonian remote Internet voting model and allows for remote identification with the use of the signature and a unique personal identification number. The cards can be used at home with the addition of

a smart card reader, or at a public access terminal (55 terminals per 100,000 citizens) (Alvarez et al., 2009; Lumi, September 19, 2009; Madise and Martens, 2006).

The second part of the legal framework was the passage of various acts that permitted the use of electronic voting in the different types of Estonian elections and specified their administration. The laws also established related procedural elements such as the period of time wherein on-line ballots could be cast, the process for certifying that on-line ballots could not be cast on election day, the authentication process, and the process for merging and counting all ballots after the election.[36] The Estonian system also allows on-line electors to change their electronic ballot any number of times, with only the final ballot counting toward the actual vote (Alvarez et al., 2009; Madise and Martens, 2006).[37]

Development, technical features and general operation of Estonia's model

Remote Internet voting in Estonia was introduced in the 2005 municipal elections, and then used again in 2007 for national parliamentary elections and in 2009 for European Parliament elections. The Estonian model is based on three principles: (1) the identity card for voter identification, (2) the possibility of re-voting electronically with only the final ballot counting, and (3) the priority of traditional voting (should an elector vote by paper ballot on election day their electronic ballot is deleted). Other basic principles to which the system is required to adhere include a reliable, secure and accountable method of counting, simplicity for electors as well as experts who may audit the system, transparency, and one vote per voter. All ballots must be uniform and secure and all electors must be able to vote (Maaten, 2004).

To use remote on-line voting, electors require a smart card reader and relevant software, an Internet connection and a Windows, MacOS or Linux operating system. The voting process begins by inserting a valid ID card into a computer whereby a list of candidates is displayed based on the elector's personal identification number. The voting system uses a "double envelope scheme", typically used in other countries for postal voting, and was designed to ensure voter privacy and security. Once the voter completes the ballot it is encrypted by the voting application (i.e. the voter seals the ballot in a blank inner envelope). The voter then confirms his or her choice with a digital signature and receives confirmation that the vote has been recorded (i.e. the voter puts the inner envelope into the outer one and writes his or her name and address on it) (Estonian National Electoral Committee, 2009). When the votes are counted, the digital signature (outer envelope) is removed and the anonymous encrypted vote (inner envelope) is placed in the ballot box. Remote Internet voting is only available for a certain period, usually from four to six days prior to advance voting days, and therefore not on election day. Electors are able to change their vote as many times as they like as long as the on-line polls are open and can still vote by paper ballot on election day, although this would disqualify their electronic ballot (Maaten, 2004).

[36] Although passed in 2002, the legislation specified that remote Internet voting not be applied until 2005.
[37] This rule was brought before the Supreme Court based on the argument that it constitutionally violated the principle of uniformity, that each citizen has the right to vote once and in a similar manner. The Court upheld the legislation arguing that electors who voted electronically still only cast one ballot and had the same effect on the final results as any other voter (Madise and Martens, 2006).

Indicators of success

The Estonian model can be considered a success on a number of levels, particularly with respect to public use and voter turnout. For example, while in the 2005 local elections only 1.9 percent of votes were cast remotely by Internet, in the 2007 parliamentary elections it increased to 5.4 percent, and in the 2009 European Parliament elections to 14.7 percent of votes cast (Estonian National Electoral Committee, 2009).[38] Estonian officials now describe remote Internet voting as an accepted and expected feature of the electoral process, and one that is essential in engaging electors. Turnout in parliamentary elections increased from 58.2 in 2003 to 61.9 percent in 2007 and from 26.8 percent (2004) to 43.9 percent (2009) in the European parliament elections, which had record-low turnout levels among some other countries (International IDEA, 2009). Furthermore, recent research confirms that electors have a high degree of trust in remote electronic voting (Alvarez et al., 2009; Lumi, September 19, 2009). Research also shows that the Estonian system is neutral with respect to many socio-economic factors such as income, education, gender and geography. This finding suggests that no undemocratic biases or digital divides (specifically biases that are socio-economic in nature) have developed as a consequence of remote Internet voting with respect to those variables. Research also supports that there is no left/right political bias among remote Internet voters in Estonia (Alvarez et al., 2009:501).

Not surprisingly, electors who choose to vote remotely by Internet have better computer knowledge than others. Twenty percent of remote on-line voters in 2005 reported that they otherwise would have abstained, and 11 percent in 2007 reported that they "probably wouldn't have" or "for sure wouldn't have" voted if not for the option of an Internet ballot. This suggests that the accessibility of the Internet from remote locations has an impact on the engagement of some types of electors. Nearly one quarter of electors who cast an Internet ballot voted when the paper ballot polls would have been closed, indicating that accessibility may be a factor. There is also a "faithfulness effect" present, as in the Canadian municipal trials, whereby those who vote remotely by Internet are very likely to continue to do so. For example, all electors who used remote on-line voting in 2005 did so again in 2007. Furthermore, survey data shows that Internet voters are greater consumers of on-line election information. This may mean that more informed votes are being cast as a result of remote Internet voting, or perhaps that those who seek to better inform themselves about the election are drawn to on-line voting. Finally, although remote Internet voting in Estonia is considered more attractive for younger electors than seniors, the highest levels of usage are among those aged 18 to 44 and those 60 and older (Alvarez et al., 2009), suggesting that the conclusions about age usage may be overdrawn. The facts that remote Internet voting appears to be engaging non-voters to a certain extent, is used after hours, has a devoted following in terms of use, and that many on-line voters actively seek out information regarding candidates, are significant points in its favour.

[38] In the most recent set of local elections held on October 18, 2009, the number of Internet voters increased to 15.75 percent of all voters. Turnout in this election was 60.6 percent, an increase of about 13 percent from the 2005 local elections, which had a turnout of 47.4 percent (Estonian National Electoral Committee, 2009).

Addressing challenges

The most prominent concerns surrounding the implementation of remote Internet voting in Estonia were related to potential fraud and privacy. In response, the principle of multiple votes was created, which allows electors to cast an electronic ballot as many times as they like during the on-line voting period. In case an elector is pressured at any point in time to vote a certain way, that individual can go back and change his or her vote from a secure and private place or can vote in person on election day, mitigating vote-buying and ensuring voter secrecy (Madise and Martens, 2006).

There were also concerns regarding the possibility of a digital divide or disparities in Internet access related to generation, gender and socio-economic factors. To mitigate these effects, the state launched an Internet and computer training program for adults in 2001 as well as the Village Project which provided more libraries with computers and Internet access. More recently, they have launched public/private projects, such as "Computer Security 2009" and the state-run Information Society Awareness Program that seek to promote the use of electronic services by targeting security issues and improve the identity card application process (Estonian National Electoral Committee, 2009; Maaten, 2004).

There are also some problems with the system that have not been addressed. Foremost, the electronic voting system is only provided in Estonian (the official language) despite the fact that there is a very large Russian-speaking population in Estonia. This has created a barrier resulting in many Russian speakers not voting on-line (Alvarez et al., 2009).

In terms of accessibility, more than 80 percent of Estonians have identity cards, but this means that for some citizens voting on-line is not an option. Furthermore, even with an identity card citizens must have a smart card reader, which costs about 20 euros (Maaten, 2004). While smart card readers are available at public access points, these are still obstacles to voting that have not been fully resolved.

Geneva, Switzerland

There are several reasons for examining Geneva's experience with Internet voting. Switzerland was one of the first countries to develop a remote Internet voting application, and because it developed and fully implemented a remote Internet voting program, the Swiss model is much more advanced. Second, the remote Internet voting program in Geneva is the most experienced worldwide, having conducted more elections than any other country or jurisdiction where remote Internet voting is a viable voting option (Alvarez et al., 2009). Third, the Geneva model has followed a tightly controlled development process, which has been cited in large part as contributing to its success (Chevallier et al., 2006). Finally, Geneva has established a permanent legal basis for Internet voting. Since the Genevan model of remote Internet voting is perhaps the most refined in the world, the Internet application it relies on during elections is of importance when developing models elsewhere.

Rationale for introducing remote Internet voting

Geneva decided to pursue remote Internet voting for several reasons; foremost among them was enhancing convenience for electors and increasing turnout. Swiss voter turnout is one of the lowest of established democracies worldwide, averaging about 50 percent (Auer and Trechsel, 2001). Partially this is because of Switzerland's direct democracy system whereby electors are called to the polls an average of 4 to 6 times yearly (Geneva Internet voting system, 2003). Switzerland also had great success with postal voting, suggesting that the introduction of remote Internet voting might yield similar benefits. Familiarity with postal voting also meant that voters were accustomed to voting from home and having several weeks to vote. Other reasons include the large proportion of Swiss citizens who live abroad (580,000 of 7 million) and a norm that Geneva's public service prides itself on its proactive attitude toward technologies (BeVoting, 2007; République et Canton de Genève, 2009; Geneva Internet voting system, 2003). Internet penetration in Switzerland is such that slightly more than half the households have Internet access (55 percent), and survey data showed that two thirds of Internet users wished they could vote on-line.

At the federal level there were several parliamentary motions in 1999 and 2000 "that called the Confederation to do something in the field of" information and communication technologies, although Internet voting was not mentioned specifically, and in 2002 Parliament adopted an article that allowed for Internet voting trials (Chevallier, 2009). At the Geneva level, in 1982 Parliament passed a law on political rights enabling experimentation with voting methods. This provision was used to develop Internet voting until Parliament (June 2008) and the citizens (February 2009) approved a constitutional amendment that permitted Internet voting (Chevallier et al., 2006; Chevallier, 2009). Other factors that supported the success of the Swiss remote Internet voting application include a centralized and computerized voters list, experience with direct democracy and a "soft" approach to voter secrecy (République et Canton de Genève, 2009).[39]

Development, technical features and general operation of Geneva's model

In 1998, the Swiss Federal Executive first launched its e-government project, which included the possibility for remote Internet voting and other forms of electronic participation. The federal government invited three of the most urbanized cantons (Neuchâtel, Geneva and Zurich) to pilot remote voting methods and agreed to jointly fund the project. In Geneva, beginning in 2001, the system underwent numerous trials, initially restricted to participation in referendums, and later followed by eight official ballots between 2003 and 2005 (Chevallier et al., 2006; Kies and Trechsel, 2001).[40] During these trials electors were able to vote by traditional ballot, postal voting or remote Internet voting, although postal voting and remote Internet voting were only available prior to election day. The success of these initial trials prompted the federal

[39] Though the Swiss constitution guarantees voter secrecy it can still be considered customary in some cantons to vote by a show of hands. This is considered to be a "soft" approach to voter secrecy as opposed to frameworks that are more strict with regard to privacy (République et Canton de Genève, 2009).

[40] The legal basis for this project was established in 2002, with an amendment to the 1976 federal law on political rights (Braun and Brändli, 2006). In addition, authorities also adhered to the recommendations of the Council of Europe, which required that e-voting follow all the principles of democratic elections, and be as reliable and secure as traditional voting (République et Canton de Genève, 2009).

government to legalize remote Internet voting throughout the country in 2006 (République et Canton de Genève 2009).

The remote Internet model used in Geneva is an adaptation of its postal model. All electors are sent a voting card, which can be presented when voting by paper ballot, mailed back with a postal vote or used to obtain codes which permit on-line voting. Each card contains a unique 16-digit number designating the particular election, a 4-digit control key, and a secret 6-digit code that is concealed under a scratch-away opaque layer (Chevallier et al., 2006:439).[41] The elector begins by entering the 16-digit code on-line. This code is verified by the server and the 4-digit key is sent back to the user as a self-authentication. The server then constructs the electronic ballot and establishes a protected connection between the elector and the ballot. Once the ballot is completed the choices are presented to the voter for confirmation. Selections are then either confirmed or altered by the elector, who is prompted to provide his or her date of birth, municipality of origin and the 6-digit secret code printed on the voting card. The vote is then authenticated and the voter receives electronic confirmation that a ballot has been cast (Chevallier et al., 2006).

In terms of security Geneva does not use digital signatures or require additional computer hardware like Estonia. The system does however operate similarly with respect to the envelope feature which keeps the ballot and voter's identity separate. Once cast, the ballot is encrypted with alphanumerical characters, which masks its content (the first envelope is sealed). When the voter confirms and attaches his or her identity to the ballot, it is encrypted with another protective layer (second envelope). Once the vote is received, the identity and the ballot (the two envelopes) are kept in different files. Before the ballot box is opened the ballots are shuffled so that they do not correspond with the voter registry. Other security mechanisms include a certified Web site, and a secure channel between the elector's computer and the server facilitating the vote (Chevallier et al., 2006; République et Canton de Genève, 2009).

Indicators of success

Overall the system is considered highly successful, notably because the public is very responsive and actively makes use of remote Internet voting, and because it appears to have a positive effect on voter turnout. For example, public opinion data revealed that electors who chose to vote remotely on-line were likely to continue to do so (90 percent of voters) and that remote Internet voting is used as the primary voting channel for electors under the age of 50 (République et Canton de Genève, 2009).[42] Data reveals that there is no digital divide with respect to education or gender, but one is visible in terms of age and Internet competence. Furthermore, although there are no comprehensive figures regarding turnout, 12 to 27 percent of on-line voters previously described themselves as being frequent abstainers, particularly among electors aged 18 to 39 years (République et Canton de Genève, 2009). These statistics suggest that the extension of remote Internet voting has positively impacted turnout and encouraged the participation of younger electors.

[41] If this layer is removed on-line voting is no longer possible because the elector controls the card (Chevallier et al., 2006).

[42] It also displayed a positive relationship with education and income level. That is, the greater an elector's education and income the more likely he or she was to vote on-line.

System approval can be attributed to three aspects of the development process. First, the project was initiated and sponsored by the highest official of political rights in Geneva, the State Chancellor. The Chancellor delivered regular progress reports to government as well as representatives from all political parties, confirming each step of the way that system developments met the needs and expectations of the parties and the public. Second, system development and implementation took a step by step approach in which trials were gradually expanded along two dimensions: the stakes of the vote and the number of potential voters (Chevallier et al., 2006:439). This process allowed officials to improve the project as it developed and to better manage risk. Finally, the teams assigned to project development were multidisciplinary, including experts from a variety of fields. This combination of knowledge and alternate perspectives helped foster a well-rounded system that was not overly centered on any one aspect of model development, such as security or technical considerations (Chevallier et al., 2006).

Addressing challenges

Despite its success, Geneva faced some important challenges. Two obstacles in particular are worth noting. In terms of legalities, the right of every Swiss citizen to attend ballot counting at his or her polling station was solved by creating an electoral commission with representatives selected by political parties and appointed by government to oversee the counting of postal ballots. The body controls the ballot box reading and the role of the electoral commission was expanded for the introduction of Internet voting.[43] Furthermore, though initially the issue of vote-buying was also a prominent concern, this was mitigated by providing voters with confirmation that their ballot had been cast, but including no details regarding its content.[44] There have been no concerns or problems with regard to remote Internet voting that are considered insurmountable in Geneva.

United Kingdom

The UK is an important case study because it was one of the first countries to experiment with multiple types of remote Internet voting and because of the sheer number of trials and types of electronic voting methods it has tested. Furthermore, the UK experience is salient because its Electoral Commission decided to end electronic voting trials. While it is useful to examine cases where Internet voting models have been implemented successfully, it is also important to look at the considerations that led another jurisdiction to terminate the project.

Rationale for introducing remote electronic voting and necessary preconditions

The UK chose to pursue an electronic voting model in an effort to modernize the electoral system and generate public confidence in these modifications, attract younger voters and, most importantly, increase electoral participation. Making the process more accessible for electors of all kinds was also an important consideration (Local Government Association, 2002). By introducing remote voting options the government had the option of extending the voting period, further enhancing accessibility for electors.

[43] That said there are still questions surrounding the development of this part of Internet voting (E-voting, 2009).
[44] In Estonia this was addressed by allowing the voter to update his or her ballot while the polls remained open.

The government created the Electoral Commission in 2000, a body whose mandate is to organize some elections, carry out research, and seek out reforms that have the potential to positively impact British elections. The Commission was supported by two bodies, the Department of Constitutional Affairs and its Electoral Modernization Unit, which initially pressured the government to investigate establishing new voting opportunities to increase turnout. The UK's Electoral Commission conducted extensive research prior to the inception of the trials, notably a full analysis of all potential options and technologies, a review of experiences in other jurisdictions, legal framework analysis as well as survey research probing the perceptions of different stakeholders and public attitudes and opinions toward electronic voting (this included data regarding reported likelihood of use and public confidence). In terms of public acceptance for example, survey research revealed widespread support for electronic voting. More than half (55 percent) of eligible voters reported that the extension of electronic voting would encourage them to vote in the next election. Among young people (aged 18 to 24 years) this figure rose to 75 percent (The Electoral Commission, 2003).

The development of the UK's legal framework is also particularly interesting because before the trials could proceed an amendment to existing legislation was required whereby the local authority ceded control to the central government and relinquished its autonomy with respect to elections (Liptrott, 2006). The passage of the *Representation of the People Act* (2002) enabled this and allowed Parliament to develop regulations which permitted the conduct of pilots with alternate voting arrangements (Barry et al., 2002). These prerequisites were considered important steps before proceeding with actual implementation.

Development, technical features and general operations of the UK trials

Aside from the research conducted by the Electoral Commission, the actual model development for each local council began when the Department of Transport, Local Government and Regions (the department responsible for electoral policy) issued a request for proposals from companies to supply electronic voting and electronic vote counting and recording. Upon selecting a list of successful providers, local councils were invited to submit suggestions for pilots that held promise to modernize the electoral process. Those councils whose proposals were selected chose an industry partner from the list of providers and the pilots were developed on an individual basis.

The first electronic voting pilots took place in May 2002.[45] Thirty different electoral districts from across the country took part in the trial, sixteen of which piloted electronic methods. The trials were made available to 2.5 million electors and operated with a budget of 4.1 million pounds (Barry et al., 2002). Electronic trials used a variety of technologies and combinations of those technologies in different districts, including touch-screen kiosks (in polls and remote locations), remote Internet voting, telephone, SMS text message voting and electronic counting schemes. While some districts trialled one or two methods, many piloted multiple channels of electronic voting, making two or more methods available (4 in 2002 and 13 in 2003). The

[45] The 'modernisation' process actually began in 2000 with postal voting trials. Although postal voting was successful in that most localities in which it was offered reported an increase of at least 50 percent in electoral participation and it improved the public's reported satisfaction with the electoral process, overall turnout declined prompting the government to expand the project and experiment with other methods (Barry et al., 2002; Norris, 2005).

multi-channel approach was facilitated by an on-line electoral register that was developed to provide the necessary infrastructure for districts trialing more than two electronic methods (Xenakis and Macintosh, 2004).

In May 2003 the UK Electoral Commission conducted another 59 pilots in local districts, 18 of which trialled various types of electronic voting, at a cost of 18.5 million pounds (Open Rights Group, 2007). Again, the electronic trials offered different electronic services depending on the jurisdiction. The same potential methods that were used in 2002 were again made available, with the addition of digital television voting and smart card technology (Xenakis and Macintosh, 2004). In most instances different combinations of multi-channel voting were offered. For example, the council of Ipswich made remote Internet, telephone and SMS text messaging ballot options available, whereas Shrewsbury and Atcham offered remote Internet, telephone, digital television and all-postal voting as well as electronic counting. Sheffield, by comparison, used remote Internet voting, telephone, public kiosks and mobile phone text messaging as alternative voting channels. All-postal ballots were offered in over half of the municipalities and electronic counting was implemented in many areas, as were extended voting hours (Norris, 2005). Overall, the 2002 and 2003 pilots consisted of 14 trials of remote Internet voting, 12 trials of telephone voting, 8 trials of electronic voting at polling stations, 4 trials of SMS text message voting, 3 trials of touch-screen kiosks, and 1 digital television trial reaching approximately 6.4 million electors (BeVoting, 2007; Liptrott, 2006).

It is difficult to offer a summary account of the specific procedures or technical features of the electronic voting methods used in the UK for two reasons. First, many combinations of these technologies were offered simultaneously, resulting in the application of many different combinations of electronic voting systems. Second, there was no consistent framework used for each type of technology. With respect to remote Internet voting for example, the locales of Swindon Council, Liverpool Council and St. Albans Council all offered remote Internet voting to electors, but used different electronic systems with different features, operated by different providers. These differences also make evaluating these models challenging since different approaches may produce different consequences even if the same technology is being used. Additionally, it is difficult to decipher what is working and what is not when multiple channels are offered concurrently.

Unsuccessful trials

Despite extensive research and the fulfillment of the noted prerequisites, part of the problem with the UK trials is that from the beginning they did not allow sufficient time for testing or development given that they chose to trial so many methods of electronic voting simultaneously. Whereas most jurisdictions in other countries chose to develop and test one or two methods, the UK attempted to pilot as many potential combinations of electronic voting methods as possible, in order to identify the most effective options. Unfortunately, the amount of diversity in the trials made it very difficult for the UK Electoral Commission to determine the impact of any one method.

The Electoral Commission officially terminated all electronic voting trials in August 2007 and in 2008 the government announced that electronic voting would not be used in either the 2009 local or European elections. The continued presence of concerns in government reports regarding the

underdevelopment of electronic voting systems, security and secrecy as well as the success of postal voting, and highly critical reports from other sources (the BBC and Open Rights Group) diminished support for electronic voting. Finally, a serious problem with electronic counting in the May 2007 Scottish elections led to multiple reviews and was the final catalyst to end the electronic voting projects in Britain. On the whole, the decision to halt electronic voting can be attributed to two sets of concerns, the first relating to the ability of the Internet and other electronic methods to increase turnout, and the other to security considerations (The Electoral Commission, 2007).

First with respect to turnout the results of the UK trials were mixed. Turnout overall in the 2003 local elections rose to 37 percent, a 3-percent increase from 2002 and 5-percent increase from 1999. Despite this modest increase, it is difficult to tell how much of the rise can be attributed to the extension of electronic voting options. While in 2003 three municipalities noted a rise in participation ranging from 9 to 12 percent (these include Vale Royal, Shrewsbury and Atcham and South Salisbury), two-thirds of the other districts recorded a modest drop in turnout (Norris, 2005). Furthermore, in terms of use in 2003 only 9 percent of voters cast their ballots electronically. Overall, when presented with the option to vote by paper or electronic ballot most electors chose to use paper ballots (BeVoting, 2007). Surveys conducted among the councils that participated suggest that of the methods offered remote Internet voting was not only used most frequently, but also had the greatest positive impact on turnout, even if only marginally and allowing for the fact that in some cases overall turnout showed no increase (Barry et al., 2002). However, the government did not feel turnout increased sufficiently, or rates of use were high enough, for the pilots to be considered successful.

Second, major concerns about security and malfunctions influenced the decision to end the project. These included the possibility of hacking, viruses, lack of a paper trail, a lack of security testing prior to the trials, and breeches of ballot secrecy with door-to-door canvassers helping electors cast their ballots. Technical issues included some voting channels (such as laptops) becoming inoperable, polling cards being mailed with incorrect log-in information, and delays in the delivery of electoral registers to polls. In one municipality electors who experienced technical difficulty were not permitted to vote at traditional polling stations and so effectively disenfranchised. Most seriously, the technical counting problems that occurred in Scotland highlighted that more development and testing were needed (The Electoral Commission, 2007; Open Rights Group, 2007). Taken together, these reasons and challenges motivated the Electoral Commission and UK government to end all electronic voting projects.

Leaving aside these valid concerns about security, the electronic voting project in Britain was not given enough time to germinate or develop, and was expected to achieve too much. It appears to have failed because of the many different types of electronic voting that were introduced simultaneously and the multitude of models used to carry these out. The push for rapid implementation also imposed time constraints that resulted in best practices not always being followed and in some instances a lack of security testing (Barry et al., 2002).

Part V: Kiosk and Telephone Voting Methods

The above sections have focussed primarily on remote Internet voting methods primarily involving use of computers not under the direct control of the electoral authorities. Here we examine more closely two other remote voting options, namely remote Internet kiosk voting and telephone voting methods.

Kiosk Voting

Next to remote Internet voting, remote kiosk Internet voting seems to have the highest potential to positively impact the electoral process, given its ability to enhance accessibility for electors. Unfortunately however, there has been little written on the subject of kiosk Internet voting and few trials of the technology. Although remote Internet kiosks can make the voting process more convenient for electors, they do not have the same potential to do so as remote Internet voting given that the latter enables so many more points of access for electors. And while they have lower potential to enhance accessibility, kiosks generally raise the same concerns with respect to security and secrecy since in most cases voting kiosks are unsupervised. The need to secure data, lack of a paper trail for recount and auditing purposes, and the susceptibility to machine malfunctions are also concerns. Notably, the kiosk fallibility caused Ireland and the Netherlands to end the use of the voting machines which were to be trialled as remote Internet kiosks (Evans, 2001).[46] Controversy over voting machines and negative experiences with electronic voting machine trials in the USA have also tarnished the reputation of voting machines in general and kiosks by association. The UK, Ireland, the Netherlands and Finland are four countries that have conducted, or attempted to commence, remote kiosk voting trials. In all instances the projects were terminated.

As outlined above, the UK offered touch screen Internet kiosks in councils that elected to use the service. In total, 808 kiosks were tested, some in traditional polling places and others in remote locations, such as supermarkets and other places within the city centre. However, as explained, the project was cancelled because of security concerns and the fact that the extension of electronic voting methods did not have a significant positive effect on voter turnout. Survey research conducted by the UK Electoral Commission also revealed that respondents were more positive toward remote Internet and telephone voting than toward kiosk voting (BeVoting, 2007). For example, 87 percent of telephone voters and 81 percent of remote Internet voters reported feeling positively about the secrecy of the vote compared with 57 percent of Internet kiosk voters. Furthermore, 87 percent of telephone voters reported being positive about the security of the vote, whereas remote Internet voters (59 percent) and remote kiosk Internet voters (60 percent) reported similar assessments. Electors who voted electronically reported finding remote Internet (93 percent) and telephone voting easy to use (88 percent) in slightly greater proportions than those who used kiosks (84 percent) (BeVoting, 2007).

[46] Machine security can be increased by employing certain measures, such as a centralized account system, whereby voters must register before being allowed to vote, or by issuing electors a personalized card that must be inserted into the machine (Evans, 2001:3).

In 2000, the Netherlands implemented remote Internet kiosks in the 2003 Provincial Council Elections as part of a program to enable non-place-dependent voting. With a budget of 8.1 million euros, the goal of the Remote (Electronic) Voting project was to allow electors the option of voting from remote electronic kiosks installed in public areas other than polling places. In 2002 however, two government ministers informed the House of Representatives they felt the original program would not be feasible and decided to pursue an alternate model. So, while the remote electronic voting project continued, it deviated from its original intention, instead focusing on allowing internal electors the option of voting at any polling place and external Dutch electors the possibility of remote Internet and telephone voting.

While the specific concerns that prevented the introduction of remote Internet kiosks in the Netherlands are not entirely clear, media reports indicate that the chosen Nedap machines produced radio emissions which could allow remote detection of how a vote was cast. While the government also had security concerns regarding remote Internet voting and telephone voting, they felt these issues were manageable enough to proceed with implementation (BeVoting, 2007; Kitcat, 2007). In fact, the Netherlands' experience with kiosk Internet voting was so negative that a 2007 government commission concluded that it was not feasible to introduce kiosk Internet voting and suggested that paper and pencil voting remained the best method for complying with election requirements, including transparency, controllability and integrity (Dutch News, 2007; Slashdot, 2007).

The impetus for electronic voting in Ireland was unrelated to turnout, having the purpose to "improve the speed, efficiency, accuracy and user friendliness of the Irish elections" (BeVoting, 2007:29). Since turnout was not a consideration, the government selected the Nedap voting machines. A substantial amount of money (51 million euros) was invested in the purchase of the machines that were to be used in polling places as well as remote locations. They were tested in 3 and then 7 constituencies in 2002 and although they were supposed to be tested in the local and European elections in 2004, the electronic voting project was abandoned just prior to these pilots. More recently, in 2009, the electronic voting system was officially cancelled.

Skeptical and unfavourable reports came from the Commission on Electronic Voting concerning issues with the software (they recommended it be open source code). Protest groups, such as the Irish Citizens for Trustworthy eVoting, also created considerable controversy concerning the lack of a paper-based audit trail, the initial cost of the machines, the 700,000 euros it cost to store them annually and the additional 20 million euros Nedap speculated would be necessary to adequately develop the machines. These efforts resulted in the termination of the project (BeVoting, 2007; Electronic Voting in Ireland, 2009). The failure of the Dutch experience has also been an important consideration for not pursing machine development in Ireland, but the government is not ruling out the possibility of trying to introduce electronic voting again (BeVoting, 2007; MacCárthaigh, 2009).

Finland also sought to incorporate remote Internet kiosks into its electoral process by placing the machines in three small municipalities in its 2008 local elections. Approximately 30 kiosks were used and although they were not all remote, they were all supervised by election officials. For example, one supervised remote Internet kiosk was located in a mobile library (on a bus) that drove around the municipality. Electors could use the kiosks both on advance voting days and on

election day. The system attempted to integrate software provided by a Spanish company (Scytl) with the standard Finnish Election Information System. Overall however, the trial was considered a failure due to flaws in the machines. A total of 232 votes were not recorded because the voting was interrupted and so the ballots did not register into the electronic ballot box. Finnish officials also report no noticeable effect on voter turnout. The government is currently discussing whether it will use electronic methods of voting in the future (Aaltonen, October 7, 2009).

These examples illustrate that more research and thorough testing and development are needed prior to the implementation of (remote) kiosk Internet voting, at least with respect to the machines that have been trialled in Europe. Though Internet kiosk voting can enhance accessibility while still giving election officials a moderate degree of control, cost is a serious consideration and there appear to be more technological problems associated with machine voting in general (whether polling place Internet kiosks or machines or remote Internet kiosks) than with remote Internet or telephone voting options.

Telephone Voting

Telephone voting holds considerable promise for improving the operation of elections, most of all by increasing accessibility. It not only enables remote accessibility and allows electors the option of voting at any time, but the presence of telephones in Canadian households is also nearly universal. The existence of cell phones makes this method even more mobile than Internet voting and creates many more access points from which electors could cast a ballot. Furthermore, many electors, especially older cohorts of potential voters, are much more accustomed to telephone technology than the Internet, and so the opportunity cost of voting by telephone is lower because electors would not have to familiarize themselves with new technology. It is also much less costly than voting machines.

Telephone voting has the same benefits for election administration as other types of electronic voting in terms of efficiency and accuracy of electoral results, but does pose risks regarding security and ballot secrecy, especially since election officials have little or no control over the process. Generally however, concerns relating to security and secrecy of the ballot can be minimized through system design, as shown in Halifax's experience with telephone voting. Other issues however, such as the impossibility of a traditional recount (because there is no paper trail), and the possibility of a service interruption, are aspects which should be given consideration. Despite its potential, there have been few trials of telephone voting in Europe with the exception of the UK (detailed above) and the Netherlands. In both cases the development and use of telephone voting has been stopped. There have been multiple instances where it has been used in Canada at the municipal level in small townships.

The Netherlands offered remote Internet and telephone voting to citizens living abroad. To permit these remote types of voting in the 2004 European Parliament election, an on-line voting experiments act was passed in December 2003. Electors were required to pre-register by mail and were then sent a vote code or login and a list of candidates, each with their own candidate code. Of a potential 600,000 electors (20 to 30 thousand of whom would normally vote by postal ballot), 5,351 votes were cast electronically, 480 by telephone and 4,871 over the Internet. Most of the concerns raised in government reports related to the security of voting over the Internet,

although a lack of transparency about the software programs that operated both systems, provided by LogicaCMG, was also criticized. Public attitude surveys showed that electors reported using the services because they were simple and fast. Sixteen percent of voters who cast their ballots electronically reported only having voted because these methods were available. The majority of positive feedback however centered on remote Internet voting, and in 2006, when the government decided to pursue another trial, telephone voting was removed as an option and only remote Internet voting was available (BeVoting, 2007).

Overall, while there has not been much testing using telephone voting, the potential benefits are worthy of further exploration and discussion. Notably, that telephone voting appears to be a useful complement to remote Internet voting given electors' familiarity with the telephone and its widespread presence in households. As the case of Halifax highlights, offering telephone voting in conjunction with remote Internet voting is one solution to accessibility problems associated with a remote Internet option. At the same time, rates of use of telephone voting are much lower than remote Internet voting for the data that is available and so, while it is more accessible, it may not have the same effect with respect to engagement as the Internet.

European Trials and Developing a Model for Canada

The preceding European examples impart some salient lessons for the development of Internet voting models elsewhere. In particular, there are eight important considerations that should be taken away from the experiences of Estonia, Geneva and the UK.

First, prior to model development it is essential to clearly establish the principles that the electoral process must live up to as well as lay out any constitutional or legal requirements. It is imperative that the characteristics of the selected model fulfill these obligations and requirements. Where applicable, the criteria used to evaluate an electronic voting system should be the same as those benchmarks used to assess the effectiveness of the traditional paper ballot voting system. The principles and criteria will be different for every country and jurisdiction, given variations in expectations, legal structures and political, cultural and contextual features. Therefore, while we can learn about model development from other cases and experiences, a Canadian application must be customized to the benchmarks and features required by the Canadian electoral process to ensure system success and maintain electoral integrity. The success of remote Internet voting systems in Estonia and Geneva can be attributed to this approach to development.

Second, while there may be a desire to test multiple methods of electronic voting, it is more useful to pick one or two methods and work on developing and integrating those before considering others. Further, whatever types of electronic voting are selected, each should be based on a unified prototype. Adopting a single approach is likely to produce a system that is more thoroughly developed and will make it easier to identify which elements do and do not work well. This is the major lesson imparted from the UK experience. Evidence from Estonia and Geneva suggests that a unified model is a superior approach in terms of administrative and technical considerations.

Third, a step-by-step approach in developing a model is important, and was one of the primary reasons for the success of remote Internet voting in Geneva. Each successive trial reached more electors and occurred in elections of greater prominence. Gradually increasing the salience of the vote across these two dimensions allowed for optimal risk management and enabled officials to measure and understand the effects of the extension of electronic voting. This approach allows election officials to systematically build on established success before progressing. Part of the failure of the UK trials was due to its overly hasty and ambitious approach. The time constraints imposed as a result of rushed implementation made adequate testing impossible, resulted in technical malfunctions and likely undermined support for the project as a whole.

Fourth, the engagement of key stakeholders seems to be a useful mechanism to ensure all affected parties are satisfied with proposed changes or additions to the electoral process. While there was not much mention of these with respect to Estonia and the UK – with the exception of government officials, election administrators and public attitudes – the approach taken by Geneva focused on regular communications with representatives from all the political parties, feedback from all levels of government, and an emphasis on what the public wanted. This is considered to be one of the major contributing factors to the success of remote Internet voting in Geneva (Chevallier et al., 2006).

Fifth, it may be useful for the system to be made available in multiple languages, in order to maximize accessibility. A large Russian-speaking minority in Estonia is hindered from voting remotely by Internet because the interface is only available in Estonian, the only official language in the country.

Sixth, the Estonian and Swiss examples suggest that it is possible to adequately address concerns pertaining to security and secrecy. While the USA and UK cases do raise valid issues regarding the security of Internet voting, their significance should be placed in perspective. The USA has not attempted formal testing in official polls. The UK did encounter technical issues, but mostly with regard to Internet machines and kiosks rather than remote Internet voting. On the other hand, all successful trials examined in this report illustrate that, with careful model development, potential security and secrecy problems can be minimized. The feature of the Estonian system that allows electors the option of recasting the ballot is a good example of how the system can be adapted to prevent the threat of vote buying. The intricate envelope schemes used in both Estonia and Geneva are examples of how concerns about voter anonymity can be addressed. These examples show that it is possible to develop model features that not only meet the requirements of the political and legal framework, but can also effectively address important concerns.

Seventh, while some digital divides appear to be of less concern, there are others which should be taken into account. Available evidence from the European trials illustrates that a digital gap is not necessarily a concern in terms of gender, education or geographical location. However, there appears to be a distinct gap with respect to age, as younger electors are more likely to make use of Internet voting than older electors. Furthermore, there is a gap in use among those who have better computer knowledge than others. The more knowledgeable are naturally more likely to use on-line voting. The Estonian case suggests some program options that could be instituted to

educate older electors and increase their comfort with using the technology. The age and knowledge disparities are important considerations in ensuring equality of access and potential for engagement.

Finally, although broad conclusions regarding the potential of Internet voting to positively affect voter turnout are not possible, there is evidence (particularly in the cases of Estonia and Geneva) that the extension of remote Internet voting can engage some groups of electors who do not currently vote at high levels. There are two trends in particular. One is that, where data is available, we see electors voting on-line who previously classified themselves as abstainers or said they would not have been likely to vote otherwise. Second, there is evidence of a 'faithfulness effect', whereby electors who opt to vote on-line will continue to do so in subsequent elections if given the opportunity. It appears that making voting accessible through the Internet has the potential to engage additional electors in the voting process, and these electors will faithfully continue to use the service.

Part VI: General Considerations for Canada

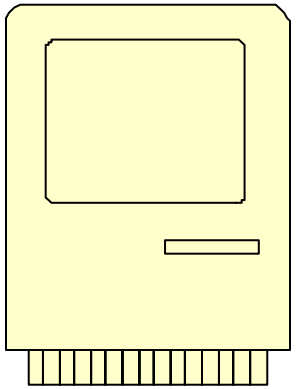
As noted above, while we can learn from the experience of others, a Canadian application of remote Internet voting must take account of specific features of the Canadian context. This section identifies some of factors that might be considered in the development of a Canadian model.

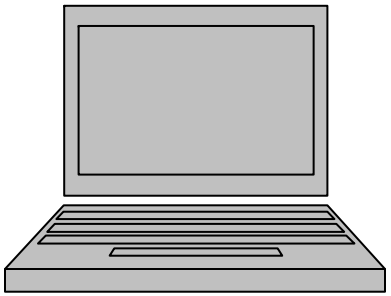
The Trade-off Between Accessibility and Security

Though remote voting has the highest potential to enhance accessibility and encourage participation, it also gives election officials the lowest amount of control over the process. In selecting a voting method, it is useful to evaluate the types of Internet voting in the model below (Figure 1). For the most part, as election officials sacrifice direct control over the voting process access is enhanced. However, a loss of direct control need not imply an unacceptable increase in security risks. Practical cases have shown that more technical difficulties appear to be associated with Internet voting machines located in polling places or Internet kiosks than with remote Internet voting. The decision to pursue remote Internet voting does hold promise to yield the greatest benefit to electors in terms of increasing access while minimizing security risks, assuming adequate protective measures are put in place. However, these benefits must be weighed against the effect of reduced control on election administration and the electoral process more generally.

Figure 1: Types of Internet Voting

High degree of control Higher degree of security	Moderate degree of control High degree of security Greater technical issues	Low degree of control Moderate to low security Fewer technical issues
Polling Place Internet Voting →	**Remote Kiosk Internet Voting** →	**Remote Internet Voting** **Telephone Voting**





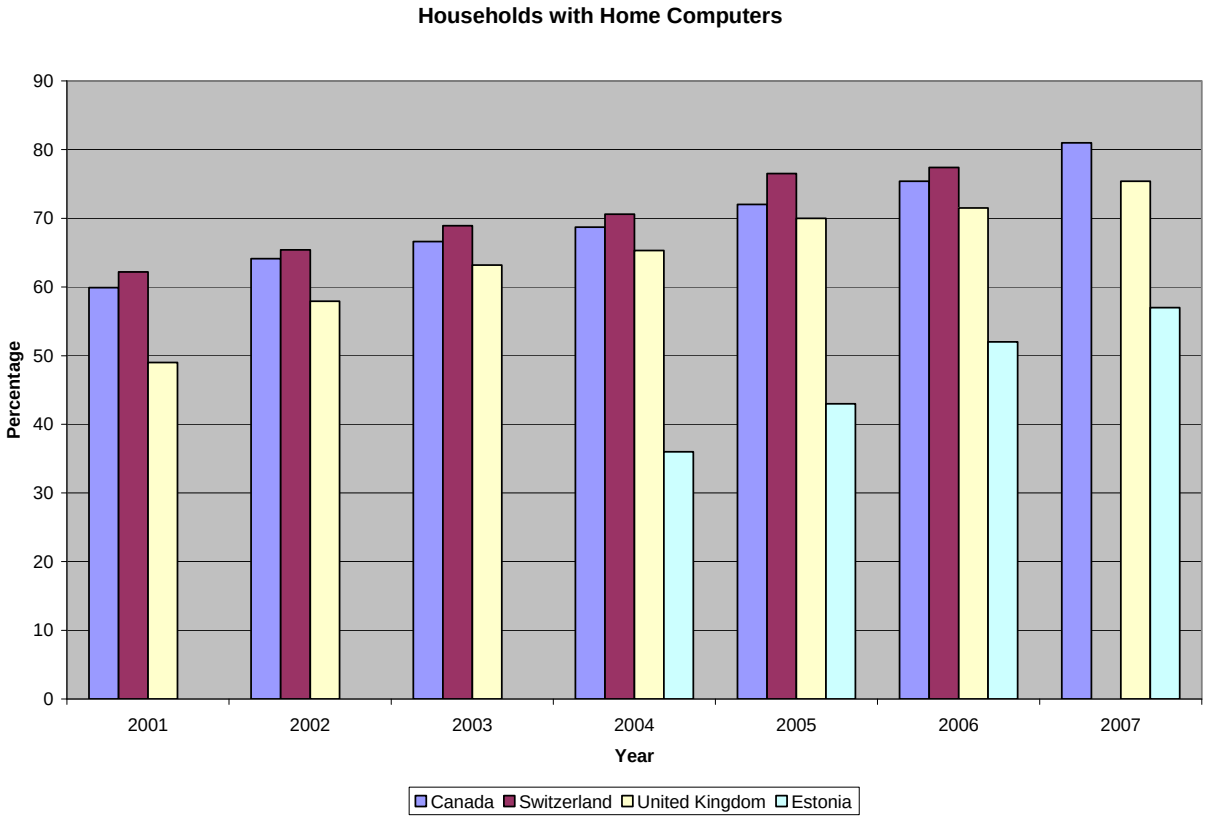
Less accessibility	Slight increase in accessibility	Increased accessibility

Access

While a key goal of remote Internet voting is to improve access, it depends on a substantial proportion of the population having computers and Internet connectivity. In the remote Internet voting projects discussed above, the governments instituting the programs believed that the rates of access in their areas were high enough to successfully proceed (though Halifax chose to also offer telephone voting). Comparative data suggests that Canada, overall, compares well with other countries in terms of Internet access.[47] The number of households with personal computers and Internet connectivity in Canada is actually higher than the European countries examined here.

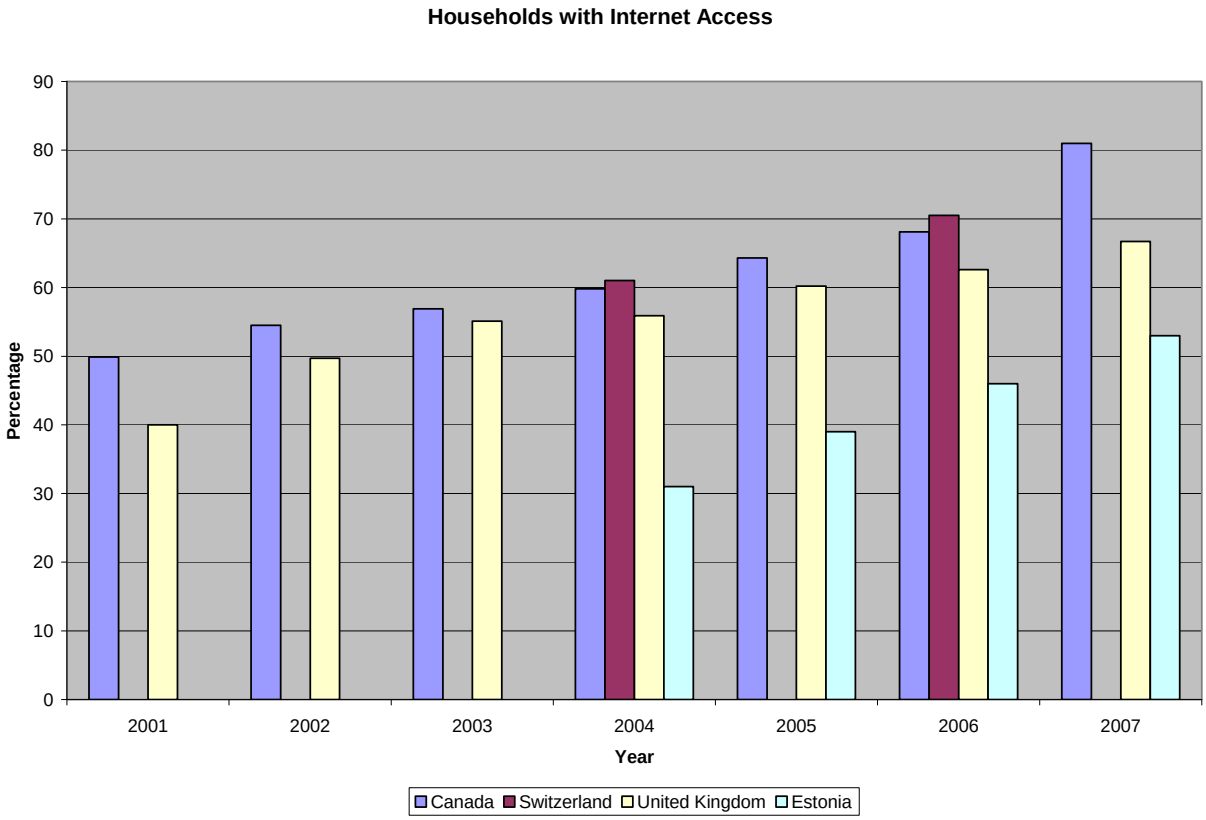
However, Internet access may be unevenly distributed in various parts of the country. Rural areas, the North, and other regions may have reduced access. The size and diversity of the country might suggest a diversified approach, where traditional balloting methods, kiosk voting or telephone voting may be more appropriate in areas where Internet access is less widespread. In addition, trials of various methods would need to take account of this factor.

Figure 2: Households with Home Computers



[47] Please note that the Canadian percentages for 2007 are actually based on the 2008 figures because no 2007 data were available. The 2008 data were obtained from the *Survey of Electors Following the 40th General Election*.

Figure 3: Households with Internet Access



Note: Data are taken from the Organisation for Economic Co-operation and Development Web site and are not complete for all years.

Turnout

The potential impact of electronic voting on voter turnout has been an important reason for considering such a system in the European and Canadian municipalities that have implemented pilot projects. While it is difficult to generalize from these examples, in all Canadian municipal trials conducted thus far, turnout increased in whichever part of the election electronic services were offered. For example, in the cases of Markham and Peterborough, although remote Internet voting was only offered during advance polling, turnout in those polls registered strong increases from past elections that relied solely on paper ballots. Halifax, Markham, Estonia and Geneva all noted significant increases in the second official ballot where remote Internet voting was an option. And, with respect to Estonia and Geneva (the only cases that offered remote Internet voting in three elections), turnout climbed again in the third contest. It does appear, therefore, that where remote Internet voting is offered, increasing numbers of people use that method over time. It is still unclear, however, whether this results in an overall turnout increase.

Cost

Cost is an important consideration in election administration. Methods of electronic voting may be more costly in the initial stages than traditional paper ballots, but many of the companies responsible for running electronic elections claim they have the potential to save the jurisdictions that use their services a large amount of money over the longer term. In Canada, for example, the

2008 federal election cost approximately ten dollars[48] per eligible voter. This money covered expenses relating to the printing of ballots, staffing the polling stations and other general costs associated with running the election. Typically a provincial election can cost anywhere from seven to nine dollars per eligible voter, whereas municipal elections range from four to six dollars. While kiosk Internet voting and polling place Internet voting machines can be very cost-intensive to initiate, maintain and store, the cost to conduct remote Internet and telephone voting is substantially lower. Though exact prices differ based on the service provider, the standard rate worldwide is approximately two dollars[49] per elector plus the cost of the mailer or any voter cards that the electoral agency mails out with PINs and other essential information. This cost includes the general operation of an electronic election (services like a call centre for electors to phone if they have questions, a scrutineer system for candidates' representatives, and all other protocols required by election officials) (Smith, August 26, 2009).

Initially, these electronic election costs would be in addition to the normal cost of the paper ballot process currently employed. In addition, advertising expenses would be required to familiarize the public with the operation of the electronic system. Over time, however, as use of the electronic election methods increased, costs associated with the regular election process could be reduced, rendering the ultimate situation more cost-neutral. Reliable cost estimates are impossible to make in advance.

Legal implications

At the local level in Canada, municipalities are able to pass by-laws that allow for the use of alternative voting methods. If there is any conflict between a by-law and the existing legislation, the by-law supersedes anything contradictory in the legislation. At the federal or provincial levels, since there is no by-law option, the government must grant the chief electoral officers the power to try different forms or methods of voting. At the federal level, for instance, section 18.1 of the *Canada Elections Act* (introduced by Bill C-2 and assented on May 31, 2000) authorizes the Chief Electoral Officer to carry out studies and tests on alternative voting means, including electronic voting processes. However, prior to the implementation of such a process in an official vote, it is required that the proposed method or system be approved by House of Commons and Senate committees.

In addition to the approval of parliamentarians, the introduction of electronic voting may require the passage of legislation or an amendment to the Act allowing for the use of alternative voting methods, especially if the methods were to become a permanent fixture in the electoral process. The wording could be more open, allowing for multiple alternative voting methods, or could specify the exact methods to be used such as remote Internet and telephone voting. This would depend on whether Parliament wanted to be able to approve any specific methods that may be proposed for use in the future. Official approval of electronic voting would have to be accompanied by an election policies and procedures document that would establish the rules and guidelines outlining various components of the election. Three items that must be outlined in this

[48] The cost was actually $13 per eligible elector, but the remaining $3 per elector goes toward paying back the political parties for their campaigning costs (Smith, August 26, 2009).
[49] This cost is based on remote Internet and telephone voting and not the electronic machines.

document include the form of a ballot,[50] a mechanism to count the ballots and a process to contest a ballot (Smith, August 26, 2009). Other items could cover issues pertaining to authority, definitions, secrecy, voters lists, voter qualifications, the voting process, the electronic voting system, candidates' representatives, results, recount procedures, emergencies, financial disclosure for candidates and various other aspects of the election process (Intelivote, 2009).

Implications of the federal structure

European experience indicates that a step-by-step approach, involving introduction of only one or two Internet options at a time, in a well-designed program, increases the likelihood of success. If federal, provincial and municipal election offices simultaneously introduce their own mix of Internet or remote voting options, using different approaches and technologies, this may result in voter confusion. An open consultative process between various jurisdictions within Canada would be important to reduce the likelihood of such a situation**.**

Software

When selecting a type of Internet voting software, there are two options: proprietary and open-source. The central distinction between the two relates to ownership and intellectual property. Proprietary software is owned by the company that provides it, unless otherwise stipulated, and can only be used based on licensing conditions. Open source software by comparison still has a software licence, but the licence exists to protect the freedom of the software and the users (Gallagher, October 2, 2009).

All Internet voting projects to date, with the exception of the Australian Capital Territory project, have used proprietary software. Geneva, in particular, hotly debated the issue and then held a referendum concerning which type of software it was going to use. In the end, it decided that proprietary software would instil greater public confidence in the on-line voting process. Interestingly, although the USA has yet to trial remote Internet voting, many prominent American scholars (particularly Alvarez and Hall, 2004 and 2008) are proponents of open-source software. One of the major criticisms of the kiosk Internet voting project in Ireland was the lack of transparency with respect to the source code because it was not open-source. In the future consideration of electronic voting methods, the Commission on Electronic Voting recommended that only open-source software be considered for use (Interim Report of the Commission on Electronic Voting, 2006). Given these conflicting opinions, it is important that Canadian electoral agencies be informed of and carefully considers both types of software prior to developing a model for the conduct of elections.

In Canadian local elections, no municipalities chose to use an open-source software provider for the electronic portion of their elections because of convenience and small or non-existent research budgets. In addition, there are no Canadian companies that offer open-source election programs, so it is easier and more convenient for municipalities to select a company that not only has a program, but has also implemented it in official votes in other jurisdictions.

[50] The form of a ballot is what the ballot actually looks like, i.e. the order in which the candidates are arranged on the ballot and so on.

There are several important benefits associated with an open-source software product. For one, the source code (the language the computer program is written in) is open. That means it is transparent and can be peer-reviewed by anyone, anywhere. It is a common misconception that closed-source software is more secure than an open-source product because it is assumed that security is created by obscurity instead of by design (Gallagher, October 2, 2009). The development of Internet voting machines using open-source code in the Australian Capital Territory is a practical example of the benefit of the transparency open-source software provides. A local academic identified a mistake in the code that, although not a functional or security error, was a serious flaw nonetheless. Were it not for the code being open to public scrutiny, this flaw may not have been detected (Zetter, 2003). While some proprietary companies will allow their software to be peer-reviewed, provided the reviewing party signs a non-disclosure agreement, this is not always the case.

Furthermore, with proprietary software, a fee must be paid for every use and the software provider is relied upon for updates. This is not the case with open-source software, since the copyright could be owned by the purchaser. Open-source software products also allow for a greater role in product development and degree of control in verifying the development of desired software elements (Gallagher, October 2, 2009). Finally, the open nature of the code allows the model to be copied and used by others. While no one else is able to change the framework, if an open-source Internet voting model is used in Canada, there would be the potential for other governments to refer to it as an 'ideal type' for Internet voting. In this sense, the open-source software could provide an opportunity for others to follow and learn directly from the Canadian experience.

Other effects on the electoral process

The emergence of Internet voting in Canada would not only impact electors' choices and the way they vote, but also other aspects of the electoral process, notably the nature of campaigning. The implementation and popularity of Internet voting would have a significant effect on the campaign and the predictability of elections as well as on how candidates and parties mobilize voters. In Markham, for instance, one notable comment from officials was that on-line voting altered the landscape of how candidates needed to campaign. While canvassing, candidates encountered many electors who had already voted. A greater number of electors voting in the advance polls because of Internet convenience meant there were fewer votes to mobilize on election day. In addition, in Halifax, candidates were able to keep track of supporters during campaign timelines using an Internet candidate module. This allowed for the generation of multiple support lists such as a special list of undecided voters or categorization by area (i.e. street), which was a useful vehicle for mobilization. It also reduced the need for the traditional candidates' representative function because parties were able to track participation on-line. Though these are only some examples, there are many other potential effects that the extension of Internet voting could have on the campaign process, particularly voter mobilization.

Steps Needed to Achieve Internet Voting in Canada

Many of the steps needed to achieve Internet voting in Canada have been outlined throughout the report. The following eight steps can be identified in particular, although they would not be required to occur sequentially.

First, ensuring access is essential. This includes making sure that an adequate number of households have computers with access to the Internet, while taking account of differences between constituencies. Ensuring equality of access may require the inclusion of additional public Internet voting sites or making other voting methods more accessible in areas of lower income or rural areas where connectivity may be an issue.

Second, a culture of support – from government, the election administration body, political parties and candidates as well as electors – is required. To allow for a smooth introduction, it is important that all parties affected by the change are generally supportive, and that concerns are addressed.

Third, there is a need for a legal framework that supports the use and implementation of alternative electronic voting methods. In most cases, Canadian trials will require approval of the specific method by parliamentarians, and likely additional legislation if the method is to become a permanent fixture of the Canadian electoral process.

Fourth, thorough research and an assessment of trials and tests in other jurisdictions as well as an analysis of their outcomes is essential. It will be helpful to pursue the cases discussed in this report to identify particular features of superior approaches that may be useful in developing a given model for Canada.

Fifth, it is important that there be a clear picture of the benchmarks and requirements an additional voting method would be expected to fulfill, as this will provide a framework for distinguishing which electronic or Internet voting method is a good fit for the Canadian electoral process.

Sixth, a marketing and information campaign appears to be an important step toward not only launching, but also maintaining a successful Internet voting program. In addition to informing electors of the choice of alternate voting methods, information concerning the importance of voting or other details regarding candidates or their platforms could be included.

Seventh, gradual, practical testing appears to be a necessary step. Gradual trials would involve introducing Internet voting in sequential electoral races whereby the number of voters affected would increase with each pilot as well as the perceived importance of the election.

Finally, adequate evaluation of pilots is recommended to ensure the method is meeting desired objectives, and that all stakeholders are satisfied with the change and its consequences. This would involve conducting surveys among political parties, candidates, election administrators and electors.

Conclusion

This study indicates that no one specific model of remote or Internet voting used elsewhere is directly transferable to a Canadian context. Selectively adopting features tested in other jurisdictions will best help to assure maintenance of the integrity of the Canadian electoral system. In terms of what will work in Canada, there is a particular need for more research and pilot projects related to remote Internet voting. And while theoretical research is useful, only practical experience and trials can determine the particular impact Internet voting would have on Canadian electoral democracy.

Interdisciplinary research may be able to provide further guidance on which variants of the available models would be best suited to the Canadian context. In particular, it would be useful to collect additional attitudinal data that probe electors' reported level of comfort and trust with Internet technology and specific types of Internet voting. It would also be useful to gauge how likely Canadian electors would be to make use of telephone voting. In addition, it would be important to investigate regional and other socio-demographic features of the likely use of electronic voting methods.

It would also be useful for the Canadian electoral agencies to develop a number of principles or benchmarks that Canadians would expect an electronic voting system to live up to. This could include and expand upon their operational values and principles, such as maintaining the integrity of the electoral system, increasing accessibility and convenience for electors, the potential to increase electoral participation, being innovative while maintaining traditional customs and conventions, improving the speed of tabulation and the reporting of election results, maintaining or enhancing the inclusiveness of the electoral process, responding to technological and attitudinal changes in society, preserving or increasing system transparency, continuing to earn and maintain public trust, and ensuring cost effectiveness. Additional research on the type of software, security protocols, and risk assessment methods would be beneficial as well.

Practical testing and pilot projects are the only ways of knowing what will work and what will not. Trials of particular methods will give the best insight into understanding what requirements must be met for Internet voting to work well in Canada as well as the actual pros and cons of electronic approaches. A by-election is perhaps a useful starting point, but a more expansive trial would be necessary prior to the introduction of Internet voting nationally. A regionally concentrated trial, or a group of selected constituencies that are regionally representative, would be a useful approach to testing. Only after such testing would it be feasible to offer remote Internet voting as an option for all Canadian electors, as a complement to the traditional process.

Careful examination of the literature on Internet voting as well as the pilot experiences of many jurisdictions suggests that both the extremely optimistic and pessimistic positions about the effects of Internet voting are overstated. Internet voting will not act as a panacea for the social causes responsible for electoral disengagement, nor will it remedy negative attitudes toward political entities. It will, however, increase voting opportunities for electors and make casting a vote more accessible. On the other side, Internet voting will not erode democracy or result in vote buying and election fraud any more than does the existing system. The Internet will undoubtedly change the political landscape in Canada with or without the introduction of Internet voting, since it already is impacting electoral campaigns and overall election administration. While there are valid concerns that should be considered and thought out in the development of a given model, the successful operation of Internet voting in other jurisdictions shows that it can be implemented and, in fact, improve the electoral process for electors and election administrators.

Bibliography

Aaltonen, Jussi, Ministerial Adviser, Ministry of Justice, Government of Finland, Personal communication, October 8, 2009.

Alvarez, Michael R., and Thad E. Hall. 2002. *Point, Click & Vote: The Future of Internet Voting*. Washington: Brookings Institution Press.

Alvarez, Michael R., and Thad E. Hall. 2008. *Electronic Elections: The Perils and Promises of Digital Democracy*. New Jersey: Princeton University Press.

Alvarez, Michael R., Thad E. Hall and Alexander H. Trechsel. 2009. "Internet Voting in Comparative Perspective: The Case of Estonia." *PS: Political Science and Politics* 42:497–505.

Author not available. 2003. "Internet Voting Wins by a Landslide in Markham Municipal Election: Town Sees 48 Per Cent Jump in Online Voter Turnout Over 2003." *Internet News Unlimited*, July 23.

Author not available. 2007. "Red Pencils to Return to Polling Stations." *Dutch News.nl*, www.dutchnews.nl/news/archives/2007/09/time_not_right_for_electronic.php (September 27).

Barry, Colin, Paul Dacey, Tim Pickering, and Tim Evans. 2002. *eVolution not Revolution: Electronic Voting Status Report 2*. Australia: Victorian Electoral Commission.

BeVoting: Study of Electronic Voting Systems, Part 1, Version 1.1, April 15, 2008, www.ibz.rrn.fgov.be/fileadmin/user_upload/Elections/fr/presentation/bevoting-1_gb.pdf.

Bousquet, Tim. 2008. "iVote: Can Electronic Voting Save Democracy?" *The Coast*, September 18.

Bousquet, Tim. 2008. "Did Internet Voting Effect the Election Outcome?" *The Coast*, October 19.

Braun, Nadja, and Daniel Brändli. 2006. "Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed." *Electronic Voting 2006: 2nd International Workshop Co-organized by Council of Europe, ESF TED, IFIP WG 8.5 and E-Voting*, Robert Krimmer (Ed.). Bonn: Köllen Druck+Verlag GmbH.

Brouwer, Andrew, Deputy Clerk, Town of Markham, Personal interview, August 27, 2009.

Brouwer, Andrew, Deputy Clerk, Town of Markham, Personal communication, August 31, 2009.

California Secretary of State Bill Jones. 2000. *California Internet Voting Task Force: A Report on the Feasibility of Internet Voting*, www.sos.ca.gov/elections/ivote/final_report.pdf.

Caltech/MIT Voting Technology Project. 2001. *Voting: What Is, What Could Be*, www.vote.caltech.edu/Reports/july01/July01_VTP_%20Voting_Report_Entire.pdf.

CANARIE Inc. 2004. "Canada's First Study on Internet Voting Proves Voters Want e-Democracy." News Release, February 2.

Chevallier, Michel, Michel Warynski, and Alain Sandoz. 2006. "Success Factors of Geneva's E-Voting System." *The Electronic Journal of e-Government* 4,2:55–62.

Chevallier, Michel, Secrétaire général adjoint, Chancellerie d'État, Genève, Personal communication, December 10, 2009.

City of Peterborough. 2005. *Report FACLK05-018. Alternative Voting Methods for the 2006 Municipal Election*. Peterborough: City Council, September 25.

City of Peterborough. 2006. *Report FACLK06-002. Award of P33-05 – Lease of Internet Voting Services and Vote Tabulators – 2006 Municipal Election*. Peterborough: City Council, January 30.

City of Peterborough. "City of Peterborough, Internet Information Guide 2006." *2006 e.lection: Go On-line to Be First in Line*, www.peterboroughvotes.ca (August 21, 2009).

"Countries With e-Voting Projects," *Tiresias.org Making ICT Accessible*, www.tiresias.org/research/guidelines/evoting_projects.htm (July 29, 2009).

Delvinia Interactive. 2007. *Understanding the Digital Voter Experience: The Delvinia Report on Internet Voting in the 2006 Town of Markham Municipal Election*.

Department of Justice Canada. 2000. *Canada Elections Act* (S.C. 2000, c. 9).

Estonian National Electoral Committee. 2009. "Internet Voting in Estonia." www.vvk.ee/index.php?id=11178 (September 19, 2009).

Evans, Lisa T. 2001. "Kiosks: The Interactive Media Solution, or is it?" *SANS Institute InfoSec ReadingRoom*, www.sans.org/reading_room/whitepapers/basics/kiosks_the_interactive_media_solution_or_is_it_521 (August 7, 2009).

Flaherty, Dennis, Manager, Strategic Communications, Town of Markham, Personal interview, August 28, 2009.

Froman, Adam, President, Delvinia Interactive, Personal interview, October 2, 2009.

Froman, Adam, President, Delvinia Interactive, Personal communication, December 8, 2009.

Gallagher, Jason, OSCAR Lead Developer, McMaster University, Personal interview, October 2, 2009.

Grant, Linda, Returning Officer, Regional Municipality of Halifax, Personal interview, August 25, 2009.

Halifax Regional Municipality. 2008. *Halifax Regional Municipality Committee of the Whole Minutes*. January 22.

Hoover, James, Dominion Voting Systems, Personal communication, August 27, 2009.

Intelivote. 2009. "Online Vote Analysis." *Company documents*, August 27, 2009.

Interim Report of the Commission on Electronic Voting on the Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. 2006. www.cev.ie/htm/report/V02.pdf.

International IDEA, 2009. *Voter Turnout, Republic of Estonia*, www.idea.int/vt/country_view.cfm?country=EE (September 24, 2009).

Internet Policy Institute. 2001. *Report of the National Workshop of Internet Voting: Issues and Research Agenda*, news.findlaw.com/cnn/docs/voting/nsfe-voterprt.pdf.

Kies, Raphaël, and Alexander H. Trechsel. 2001. "Le contexte socio-politique." In *Voter par Internet? Le projet e-voting dans le canton de Genève dans une perspective socio-politique et juridique*, Andreas Auer, and Alexander H. Trechsel (Eds.). Bâle, Genève, Munich: Helbing & Lichtenhahn.

Kitcat, Jason. 2007. "Electronic Voting: A Challenge to Democracy?" *Open Rights Group*, www.openrightsgroup.org/uploads/org-evoting-briefing-pack-final.pdf (October 3, 2009).

KPMG. 2000. "The Feasibility of Electronic Voting in Canada: A Summary of the 1998 KPMG/Sussex Circle Report." *Electoral Insight* 2,1:2–5.

LeDuc, Lawrence, and Jon H. Pammett. 2006. "Voter Turnout in 2006: More Than Just the Weather." In *The Canadian Federal Election of 2006*, Jon H. Pammett, and Christopher Dornan (Eds.). Toronto: Dundurn.

Liptrott, Mark. 2006. "E-Voting in the UK: A Work in Progress." *The Electronic Journal of e-Government* 4,2: 71–78.

Local Government Association. 2002. *The Implementation of Electronic Voting in the UK: Research Summary*. London: LGA Publications, www.communities.gov.uk/documents/localgovernment/pdf/133544.pdf.

Lumi, Rasmus, Chargé d'Affaires, Estonian Embassy, Personal interview, September 19, 2009.

Maaten, Epp. 2004. "Towards Remote E-Voting: Estonian Case." In *Electronic Voting in Europe – Technology, Law, Politics and Society: Workshop of the ESF TED Program Together With GI and OCG*, Alexander Prosser and Robert Krimmer (Eds.). Bonn: Köllen Druck & Verlag GmbH.

MacCárthaigh, Colm. 2009. "Electronic Voting in Ireland." Irish Citizens for Trustworthy E-voting, www.stdlib.net/~colmmacc/e-voting-ireland.pdf (October 2, 2009).

MacDonald, Andrea. 2006. "A Cheaper Way to Vote: Dartmouth Company Creates Electronic Voting System That Replaces Traditional Ballot Box." *The Daily News*, November 22.

Madise, Ülle, and Tarvi Martens. 2006. "E-voting in Estonia 2005. The First Practice of Country-wide Binding Internet Voting in the World." In *Electronic Voting 2006, GI Lecture Notes in Informatics*, Robert Krimmer (Ed.). P–86, Bonn.

Mellett, Cathy, A/Manager, Office of the Municipal Clerk, Regional Municipality of Halifax, Personal communication, September 11, 2009.

Mellett, Cathy, A/Manager, Office of the Municipal Clerk, Regional Municipality of Halifax, Personal communication, September 29, 2009.

Mellett, Cathy, A/Manager, Office of the Municipal Clerk, Regional Municipality of Halifax, Personal communication, November 25, 2009.

Mercurio, Bryan. 2004. "Democracy in Decline: Can Internet Voting Save the Electoral Process?" *John Marshall Journal of Computer and Information Law* 12,2: 101–143.

Mohen, Joe, and Julia Glidden. 2001. "The Case for Internet Voting." *Communications of the ACM* 44,1:72–85.

Nicholson, Frank, Director, Legislative Services & Government Relations, the Association of Municipal Managers, Clerks & Treasurers of Ontario, Personal interview, September 23, 2009.

Norris, Pippa. 2005. "E-voting as the Magic Bullet for European Parliamentary Elections?" In *The European Union and E-voting*, Alexander Trechsel and Fernando Mendez (Eds.). London: Routledge.

Open Rights Group: Protecting Your Rights in the Digital Age. 2007. "ElectronicVoting: A challenge to democracy." *E-Voting Briefing Pack*, January.

Organisation for Economic Co-operation and Development, Stat Extracts. 2009. "Country Statistical Profiles 2009: Canada." http://stats.oecd.org/wbos/viewhtml.aspx?queryname=18148&querytype=view&lang=en (September 6, 2009).

Putnam, Robert. 2000. *Bowling Alone: The Collapse and Revival of American Community*. New York: Simon & Schuster.

République et Canton de Genève. 2009. *E-Voting: The Geneva Internet Voting System*, www.geneve.ch/evoting/english/presentation_projet.asp (August 16, 2009).

République et Canton de Genève. 2003. *Information and documentation: The Geneva Internet Voting System*, www.geneve.ch/chancellerie/E-Goverment/e-voting.html (August, 16, 2009).

Sawatzky, Jennifer, Deputy Division Registrar, City of Peterborough, Personal communication, December 9, 2009.

Sibley, Kathleen. 2003. "Markham Voters Go From in Line to Online." *itbusiness.ca*, November 12.

Slashdot. 2007. *Dutch Commission Deals Blow to Electronic Voting*, http://politics.slashdot.org/politics/07/09/28/1216207.shtml (translated from official government Web site: www.minbzk.nl/actueel?ActItmIdt=108604) (November 9, 2009).

Smith, Dean, President, Intelivote. Personal interview, August 26, 2009.

The Electoral Commission. 2003. "Britain Launches Largest Trial of Electronic Voting in Europe." News Release, April 24, www.electoralcommission.org.uk/news-and-media/news-releases/electoral-commission-media-centre/news-releases-campaigns/britain-launches-largest-trial-of-electronic-voting-in-europe (October 5, 2009).

The Electoral Commission. 2007. *Scottish Elections 2007: The Independent Review of the Scottish Parliamentary and Local Government Elections.* http://news.bbc.co.uk/2/shared/bsp/hi/pdfs/23_10_07_votereport.pdf (December 9, 2009).

Tiresias.org, Making IT Accessible. 2009. *Countries With e-Voting Projects*. www.tiresias.org/research/guidelines/evoting_projects.htm (July 22, 2009).

Town of Markham. 2005. *Town of Markham General Committee: 2006 Election*. Markham: City Council, September 12.

Town of Markham. 2007. "2003–2006 Election Cost Rebate and Election."

Trechsel, Alexander. "Report for the Council of Europe: Internet Voting in the March 2007 Parliamentary Elections in Estonia." *Council of Europe*. http://votingtechnologyproject.org/drupal/files/report/internet_voting_estonia_2007.pdf (August 4, 2009).

Wright-Laking, Nancy, Clerk, City of Peterborough, Personal interview, October 1, 2009.

Wright-Laking, Nancy, Clerk, City of Peterborough, Personal communication, November 23, 2009.

Xenakis, Alexandros, and Ann Macintosh. 2004. "The UK Deployment of the e-Electoral Register." Paper presented at the Workshop of the ESF TED Programme together with GI and OCG, Bregenz, Lake of Constance, Austria.

Zetter, Kim. 2003. "Aussies Do It Right: E-Voting." *Wired.com*, www.wired.com/techbiz/media/news/2003/11/61045, November 3.

ACE – The Electoral Knowledge Network
Source: http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b4

Internet Voting

The explosion of the Internet and the World Wide Web in the late 1990s led many individuals both inside and outside of the electoral administrations field to speculate about the possibility of using this new public resource to improve the efficiency, effectiveness, and legitimacy of democratic elections. Following on this discussion, several studies and experiments were developed, in independent jurisdictions and with mixed results. The overwhelming consensus which emerged from these studies is that Internet Voting presents numerous risks which need to be properly addressed before widespread deployment can take place.

Why Consider Internet Voting?

The most obvious advantage of internet voting is convenience for the voter. Regardless of how well polling places are designed and distributed, there could be no more convenient place to vote than from the comfort of one's home. By making electoral participation as easy as logging in to a website, checking a few boxes on a form, and clicking the "Vote" button, it is likely that voter turnout, and hence the overall legitimacy of the results, may be improved significantly. It could also allow significant cost-savings in the deployment and operation of physical polling stations, if the "adoption rate" of internet voting is at a sufficient level. The counting and tabulating of electronic ballots is potentially much faster and easier than counting traditional paper-based or even optical-scan or punch-card ballots, which may represent significant cost savings as well.

It is possible to distinguish three different forms of internet voting:

- Polling Site Internet Voting - in which voters cast their ballots via the internet from client machines physically situated in official polling places, in which both the hardware and software of the client is controlled by election officials, and the authentication of the voters may take place by traditional means.
- Kiosk Internet Voting - in which voters cast their ballots via client machines, in which the hardware and software are controlled by

election officials, but distributed in public places (shopping malls etc.) in which the physical environment and voter authentication are not directly under official control.

- Remote Internet Voting - in which neither the client machines nor the physical environment are under the control of election officials. Whereas the first two methods are potentially much more secure, they also present few advantages over more traditional voting methods. The "allure" of internet voting is only fully encapsulated in systems in which users are able to authenticate themselves and cast their ballots at their convenience, via home, workplace, or public internet terminals. Unfortunately, it is this method which presents the most serious and intractable security risks.

Security Implications of Remote Internet Voting

The possible benefits of internet voting must be weighed against the risks to which this polling method is exposed. As has been emphasized elsewhere, but bears repeating, every election conducted by whatever means should comply faithfully with the same basic principles of secrecy and anonymity, fairness, accuracy, and transparency.

Every polling system, whether it uses pencil and paper, punch cards, touch-screen (DRE), or any other method, must assure that voters are identified accurately and that their votes are counted accurately. In most cases this must be done without allowing any means to associate a particular vote with a particular voter. It is also essential that the citizenry have confidence in the results; in other words, that the system chosen not only comforms to these basic requirements, but that it does so in a manner that is clear and well understood by all participants. Every polling method should be as secret and anonymous, fair, accurate, and transparent as a well-managed paper-and-pencil balloting system:

"Indeed, if perfect clerks would conduct an election using paper-ballots, this would provide the best model we have for a public election. Such an election would be, for example: anonymous (avoiding collusion, coercion), secret (all cast votes are unknown until the election ends) and yet correct (all votes are counted) and honest (no one can vote twice or change the vote of another), oftentimes also complete (all voters must either vote or justify absence). In such a system, if we know the voter (e.g., in voter registration) we cannot

know the vote and if we know the vote (e.g., in tallying) we cannot know the voter. After an election, all votes and all voters are publicly known – but their connection is both unprovable and unknown."

SafeVote Inc., Voting System Requirements, The Bell, Feb. 2001

Any purely electronic voting system must take into account the necessity of safeguarding the accuracy of the vote count, in the absence of a physical representation of the ballot. For a complete discussion of this issue, see Direct Recording Electronic Systems . In addition to these concerns, Internet voting is subject to other potential risks due to the inherent insecurity of both the user's machine and the network connection by which it connects to the central server or tabulator.

At the present time, over 90% of home computers use a version of the Microsoft Windows operating system. As this operating system was never intended for highly sensitive "mission critical" applications, its primary goal is to be as easy as possible for a novice or casual user to operate. As such, little effort has been made to "compartmentalize" the operating system to prevent "rogue" applications from performing unwanted actions or making unwanted changes to the overall operation and configuration of the computer. This fundamentally insecure environment, along with the widespread deployment of "macro languages" in applications like Word or Outlook, has provided a fertile breeding ground for many different forms of computer viruses, "worms", "spyware", or "trojan horse" applications. Despite the widespread use of firewalls and anti-virus software, it has been estimated that 20% of all personal computers are infected with some type of "malware" (see Your PC May Be Less Secure Than You Think). In other words, there is no way at present for designers of internet voting systems to ensure that the voters' home computers have not been compromised in such a way as to call into question the reliability of the voting process.

Securing the connection between the voter's home computer and the central server is also problematic, but in this area at least the correct use of public-key cryptography allows a degree of confidence in the integrity of this communication channel. Specifically, the SSL (Secure Sockets Layer) and TLS (Transport Layer Security) protocols used by web browsers and servers to create secure channels for e-commerce and internet banking, for example, were designed to prevent the so-called "man in the middle" attack

whereby a network transmission is hijacked by an attacker who has managed to control the channel through which the two end-points of the transaction communicate with one another. SSL uses signed encryption keys which have been verified by a trusted "Certificate Authority" to make it impossible for such an attacker to modify the contents of this communication, without revealing that the attack has taken place. Unfortunately, even if this technology is used correctly, it is still vulnerable to other types of attack, which may be characterised as either "denial of service" attacks or "spoofing" attacks. A denial of service attack is said to take place when the attacker, even if unable to alter or interfere with the substance of a communication, is able to prevent the communication from taking place, typically by overloading one or the other endpoint of the communication. A spoofing attack is said to occur when one of the communicating parties is tricked into opening a secure connection to a site controlled by an attacker. A variety of spoofing attack, popularly known as "phishing", has become extremely widespread in recent years, typically involving an email containing an obfuscated link to a site which has been created to perfectly mimic a particular target website (eg. that of a financial institution,) along with an urgent request to "re-enter" sensitive personal information (credit card numbers, passwords, etc.) This is related to a more general form of attack commonly referred to as "social engineering"; that is, bypassing technical security measures by targetting the users of the system, who often have a poor understanding of these security measures. For an informed discussion of the false sense of security created by the widespread deployment of SSL/TLS, see The Maginot Web .

Despite the widespread deployment and use of the internet for banking and other sensitive transactions, it must be emphasised that guaranteeing the security of voting via the internet is a fundamentally more difficult problem, for two important reasons. First, unlike financial transactions, in most constituencies no connection may be made between the voter and his or her vote; record-keeping and auditing capabilities which are standard in the financial world are therefore not applicable to online polling systems. Secondly, discovery of anomolies or errors in the transmission or recording of votes cannot feasibly result in a correction of these results after the fact. At best, such discovery can only result in the invalidation of any votes so

affected; at worst, in the invalidation of the election itself. Needless to say such an outcome could have disastrous effects in terms of public confidence in the legitimacy of the entire process.

For a more complete discussion of the security implications of Internet voting in general, see Security Considerations for Remote Electronic Voting over the Internet by Dr. Avi Rubin of Johns Hopkins University.

Real-world Deployment of Internet Voting

The State of Geneva in Switzerland is perhaps the first constituency in the world to deploy internet voting in any widespread fashion. Beginning in 2003 citizens of Geneva have had the option to cast their ballots online. The motivations behind this deployment, as well as the strategies for overcoming the sorts of security issues outlined above, relate at least partly to circumstances particular to Geneva, which may reduce the applicability of this experiment to other constituencies.

Geneva differs significantly from many localities in that citizens are asked to vote much more frequently, typically 4 to 6 times per year rather than once every 2 or more years, as is the norm elsewhere, due to a "direct democracy" system in which any parliamentary vote may be subject to ratification or refusal by the citizenry. As a consequence of this, electoral authorities in Geneva are under greater pressure than their counterparts elsewhere to make the voting process as simple and convenient as possible. In response to this pressure, in 1995 election officials in Geneva implemented a remote voting system based on postal voting, which quickly became the most popular method of voting, and which is credited with increasing voter turnout by 20%. Accepting the viability of postal voting has the effect of "lowering the bar" somewhat in terms of the security and public acceptance issues facing other forms of remote voting; any new system would only need to achieve the same level of security and acceptance as postal voting. For example, registered voters in Geneva already receive voting cards by mail which contains information allowing them to cast their ballots by return post. Internet voting is simply seen as an extension of this well-established service; as such, system designers have simply not addressed potential problems such as vote-buying or coercion by any

technical security measures whatsoever, relying instead on socio-cultural norms and legal mechanisms to provide protection against this possibility.

For an overview of Geneva's experiences with internet voting, see the State of Geneva's E-Voting web site ; for a detailed account of security risks and countermeasures considered by the implementors of Geneva's internet voting system, see Addressing the Secure Platform Problem for Remote Internet Voting in Geneva .

Another significant experiment in internet voting, with a more negative outcome, was conducted by the U.S. Military for use by overseas active-duty military personnel. An initial pilot project was conducted during the general election in November 2000 in which a mere 84 military voters participated, despite a cost of 6.2 million dollars, and which was widely considered to have failed to address key security issues. (See Internet Voting Project Cost Pentagon $73,809 Per Vote)

Despite these misgivings, the project was further developed, under the administration of the Federal Voting Assistance Program (FVAP), as the Secure Electronic Registration and Voting Experiment (SERVE), for broader deployment in the general election of November 2004. In advance of this planned deployment, a group of computer security experts produced a detailed study of the system, which concluded that

> "The real barrier to success is not a lack of vision, skill, resources, or dedication; it is the fact that, given the current Internet and PC security technology, and the goal of a secure, all-electronic remote voting system, the FVAP has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough. The SERVE project is thus too far ahead of its time, and should not be reconsidered until there is a much improved security infrastructure to build upon."

A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)

In the aftermath of this report, in February 2004 U.S. Defence Secretary Paul Wolfowitz accounced the cancellation the project, citing these unresolved security issues as the primary reason. (See Pentagon halts Internet voting system)

Conclusions

While it is likely, perhaps even inevitable, that voting via the internet will one day become commonplace, for reasons outlined above it is clear that designers and implementors of internet voting systems face major difficulties which must be overcome before it will be suitable for broad deployment. The most important consideration is the degree to which many crucial elements of any internet voting scheme are completely outside the control of election authorities, with the result that it will be difficult to have any degree of confidence in such voting systems until the architecture of both the personal computer and the internet itself have evolved to a state far beyond that which is currently in place.

Dr. David Jefferson of Lawrence Livermore National Laboratories in Berkeley California, one of the authors of the SERVE Report, has stated that

> "Internet voting systems are vulnerable to denial of service attacks, spoofing attacks, malicious code attacks, spyware attacks, remote management attacks, and automated vote selling schemes. These attacks are powerful enough compromise large numbers of votes, either disenfranchizing voters, spying on their votes, changing their votes, or buying votes. These attacks can often succeed, possibly changing the results of an election, and yet go completely undetected. And they can be launched by anyone in the world, from a disturbed teenager to a foreign government. These vulnerabilities are quite fundamental. They cannot be designed around or fixed with the current generation of PC hardware and software and the current Internet protocols. Until such time as the security architectures of the Internet and the PC have been completely redesigned and the new designs widely deployed, which is probably at least a decade away, Internet voting in public elections must remain out of the question."
>
> David Jefferson, The Inherent Security Vulnerabilities with Internet Voting (Abstract)

And according to American computer security and cryptography expert Bruce Schneier, referring specifically to the American context,

> "Building a secure Internet-based voting system is a very hard problem, harder than all the other computer security problems we've attempted and failed at. I believe that the risks to democracy are too great to attempt it."
>
> Bruce Schneier, Crypto-Gram February 15, 2001

Virginia State Board of Elections

Advanced UOCAVA Solutions Research Project

Discussion of the Secure Electronic Return of Election Material for Voters Specified in §24.2-700 (2) and Military Voters with Disabilities or Injuries

---

Discussion provided by
Scytl USA
Election Systems and Software

1 Executive Summary

As of 2008, estimates indicate that there are between six and seven million Americans who are overseas, in the Armed Forces, or dependents of Armed Forces members residing away from their voting jurisdiction of record. Specifically, the GAO reports that the Uniformed and Overseas Absentee Voting Act (UOCAVA) covers more than 6.5 million people, including approximately 3.7 million overseas citizens not affiliated with the government (about 2 million of which are of voting age), 1.4 million military service members, and 1.3 million military dependents of voting age. As of January 2012, Virginia has 3,000 UOCAVA voters and protects these voters under the Code of Virginia § 24.2-700 (2). These American citizens include soldiers stationed in places such as Iraq and Afghanistan, who are currently fighting the war against terrorism; missionaries working in remote regions of the world; younger Americans studying abroad; and Americans who work overseas, building economic opportunities in the global economy.[1] In addition to voting from remote locations, many military service members are further challenged with physical and mental impairments as a result of their service.

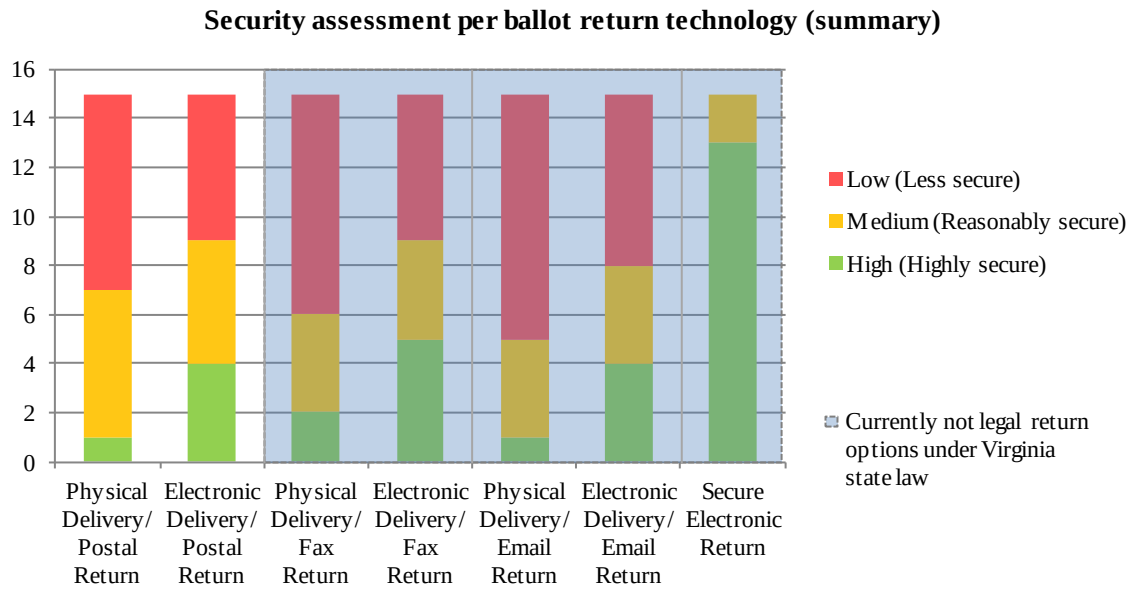
As chronicled in *No Time to Vote*[2] – a study by the Pew Charitable Trusts - these voters have traditionally had difficulty with full participation in the electoral process. Most notably, military and overseas voters tend to experience difficulties with receiving and returning their ballots in a timely and reliable manner. Technology of varying sorts presents possible improvements to the process and assistance to UOCAVA voters who experience these difficulties. Two of the most important questions being raised about these technologies are 1) whether they are a secure alternative to the traditional absentee ballot system and 2) whether they can also assist those voters who have suffered physical and mental wounds from their service. This discussion paper will introduce some of the technologies available for improving UOCAVA voting and work through an assessment of how each ballot return technology addresses security risks and provides accessibility assistance to these voters. The discussion will remain at a high-level and is meant to provide insight into which of these technologies offer the most potential.

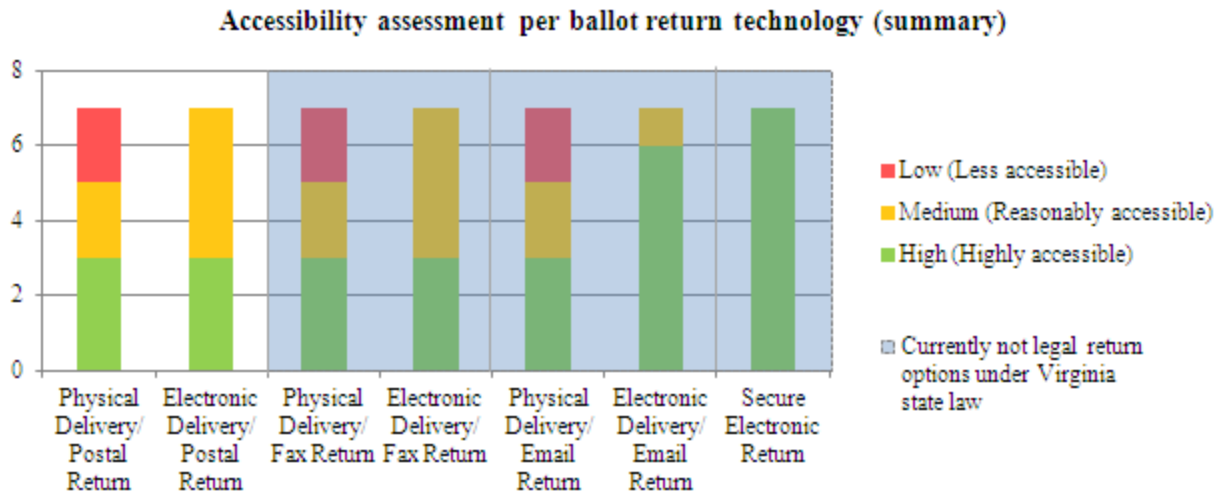
The organization of this document is the following:

- Section 1 explains the objectives of this discussion and the outcome of the assessment.
- Section 2 describes the voting return channels to be assessed and the methodology used to assess them.
- Sections 3 to 6 provide evaluations of the different voting return channels.
- Section 7 contains the conclusions of this discussion paper.
- Section 8 includes additional resources or referents.

The discussion and assessment in this paper concludes that the secure electronic return option holds the most potential for addressing the traditional UOCAVA voting difficulties while providing an accessible platform for those voters with disabilities. It provides the same – often times better – security protections as that of postal voting while greatly increasing the ability for voters with disabilities to vote in an independent and private manner. The following charts provide a synopsis of the discussion.

[1] Thad Hall. UOCAVA: A State of Research.
[2] Pew Charitable Trusts, No Time to Vote.





Note: Above charts summarize the ratings assigned in the following sections. The assessment methodology and categories are described in section 2. Tables summarizing these values can be found in Appendix A: Summary assessment tables.

What is the Advanced UOCAVA Solutions Research Project?

The Advanced UOCAVA Solutions Research Project is designed to further the body of knowledge and strengthen the concepts and technology of advanced UOCAVA solutions. These solutions offer great potential for improving the opportunities and reliability for overseas military and civilians to vote in our elections. This project will be targeted at specific technology enhancements in the context of Virginia requirements but will consider application to other similar jurisdictions. Advanced solutions will be examined and piloted in the following technology categories for their significance, sustainability, impact, and scalability – remote voting accessibility, secure electronic return, and mobile voting stations.

2 Comparing UOCAVA Absentee Voting Technologies

The following is a comparison of various absentee ballot return technologies (or return channels) which are currently available to UOCAVA voters to return their ballots:

1. ***Postal return.*** Postal voting is the use of the postal ballot as a comprehensive alternative to attendance voting. Instead of having a day on which voters attend polling booths to cast their votes, they receive a ballot paper by postal mail and then have a period in which to return their vote by mail before Election Day.
2. ***Fax return.*** Fax voting consists of transmitting the ballot by fax to a pre-assigned number. This channel is mainly supported as a contingency measure in case voters cannot cast their votes on time.
3. ***Email return.*** This channel requires voters to send an email with a scanned version of their ballot (PDF formatted) attached. This email is sent to the local election official's email address. If the ballot is accepted, the emailed vote (PDF) is printed by the election official and put into an envelope to keep it safe until it is counted.
4. ***Secure electronic return.*** This channel is defined as an election system using electronic ballots to allow voters to transmit their voted ballot to election officials over the Internet.

The comparison looks at how each return technology addresses the need to provide a secure and accessible return channel. The level of security will be measured by how well the technology addresses the security risks associated with absentee voting. The level of accessibility then will be measured by the availability of personal assistive devices for common voter disabilities.

Each return technology will be given a rating based on how well it has addressed each security risk and the availability of personal assistive devices for each disability type. The rating categories will be the following:

- ***High (or highly secure).*** The requirement is totally fulfilled and the residual risk level is low, considered an acceptable risk for any existing risk level tolerance.
- ***Medium (or reasonably secure).*** The requirement is partially fulfilled and the residual risk level is medium, considered as moderate.
- ***Low (or less secure).*** The requirement is not fulfilled and the residual risk level is high, as there are no effective countermeasures to reduce it.

2.1 Assessing Security

The following security requirements and related risks will be assessed for each ballot delivery technology option:

- ✓ ***Speed of delivery/ballot replacement.*** This requirement captures the ability of the delivery channel to deliver the ballot in a timely manner to the voter, taking into consideration the procedures for approval and preparation of the response package, and to deliver a new ballot if the previous delivered one was incorrect, destroyed during transport or otherwise subject to replacement.
- ✓ ***Provide correct ballots.*** The delivery channel should provide the correct documents to each voter (ballots and additional information related to each eligible voter and its jurisdiction/precinct).
- ✓ ***Prevent ballot tampering.*** The delivery channel should put mechanisms in place to avoid manipulation of the documents sent to the voter.
- ✓ ***Prevent ballot spoofing.*** The documents sent by the delivery channel should incorporate a mechanism to validate the authenticity of the documents sent, avoiding the chance of a third party sending illegitimate ballots to the voter.
- ✓ ***Ensure proper delivery.*** The delivery channel should guarantee an accurate delivery of the ballots, taking into consideration the actual location of the voter.

The follow security requirements and related risks will be assessed for each ballot return technology.

- ✓ ***Eligibility***. Only authorized voters should be able to vote. This means that the channel must provide a robust way to identify voters and only allow those so identified to vote. One of the main issues of absentee voting is that voters cannot be identified in person, leaving the opportunity for individuals to impersonate

eligible voters. This discussion distinguishes impersonation in two different categories: voluntary and involuntary. Involuntary impersonation is related to the impersonation of the voter without his/her knowledge (e.g., the theft of the voter credentials required to cast a vote). Voluntary impersonation requires the participation of the voter, who cooperates with the person that will impersonate such voter by providing his/her voting credentials. With the aim to simplify the comparison, we considered the risks of voluntary impersonation in the coercion and vote buying resistance security requirement. Therefore we only evaluated the risks of involuntary impersonation in this eligibility requirement.

- ✓ ***Privacy***. The voting system has to protect voter privacy, concealing the relationship between voter and his/her cast vote, and ensuring that the voter's choice will remain anonymous. This requirement must be fulfilled once the voter has cast his/her vote and must be preserved during the counting process.
- ✓ ***Integrity***. A voting system has to protect the vote against manipulation once it is cast and until it is counted. Therefore the channel must to provide measures to prevent and/or detect any attempt to change the voter's intent once the vote has been cast.
- ✓ ***Voter verifiability – cast as intended***. In this discussion, voter verifiability has been divided as: "cast as intended verification" and "counted as cast verification". In cast as intended, voter must have the possibility to check that his/her vote has been accurately recorded. In the case of absentee voting, this implies the availability to confirm that the ballot received by the election officials and stored in the remote Ballot Box (in a physical or electronic manner) is the same as cast by the voter. It is important to note that this requirement cannot conflict with the others ones (i.e., coercion and vote buying).
- ✓ ***Voter verifiability - counted as cast***. In the counted as cast verification, voters must have the possibility to verify the inclusion of his/her vote in the final tally. This is not a requirement currently included in traditional voting methods.
- ✓ ***Prevention of intermediate results***. It is important to prevent the disclosure of intermediate results before the election is closed. This measure ensures that all the voters have the same information during the voting stage.
- ✓ ***Ballot box accuracy***. Protection of the ballot box against the addition of illegitimate ballots or the elimination of legitimate ballots is required.
- ✓ ***Coercion and vote buying resistance***. As introduced before, one of the main concerns of remote voting channels are that they facilitate voter coercion or vote buying. Therefore it is important to assess if the channel facilitates these practices or includes countermeasures to prevent them. The voting channel must mitigate the risks of voluntary impersonation, in which eligible voters cooperate with the coercer or buyer to access the voting system, and involuntary coercion – where the voter is forced to disclose their voting credentials.
- ✓ ***Channel reliability***. This requirement captures the ability for the return channel to provide a consistent, dependable, and time sensitive return channel. This requirement also includes the ability for voters to determine if their vote has been received by the electoral authority on time to be tallied. Other factors, such as the risk of denial of service attacks, influence the availability of the channel. Therefore in this criterion we will balance the ability to detect such delays in an appropriate timeframe (e.g., the detection of a denial of service) and the ability to react to them (e.g., use a contingency channel to cast the vote).
- ✓ ***Auditing of the election results***. Voting channels must provide means for facilitating the audit of the election to ensure its correct execution. This means that it must allow the verification of the accuracy of the election results and provide the means to resolve any dispute.

2.2 Assessing Accessibility

From an accessibility point of view, the main requirement is to ensure that impaired voters are provided independent means to vote with total privacy, without the need of assistance from third parties. Additionally, the following requirements are also analyzed: Prevention of voting errors (the voting channel has to prevent involuntary voting errors by voters when casting their votes – e.g., under-voting, over-voting) and Ease of Use (the voting channel must be easy to use by average voters and by impaired voters as well). The accessibility assessment will be considered per the disability categories below:

- ✓ ***Blindness.*** Major symptom is the loss of all visual acuity.
- ✓ ***Partial visual loss/visual dysfunction.*** Major symptoms are altered light perception, loss of sight in one hemisphere, loss of some visual acuity, double vision, blurring, problems focusing, and sensitivity to light.
- ✓ ***Deafness.*** Major symptoms are complete hearing loss.
- ✓ ***Partial hearing loss/tinnitus.*** Major symptoms are some hearing loss, dizziness, noise sensitivity, concentration problems, ringing or other noise in ears, irritability, fatigue, concentration problems.
- ✓ ***Dexterity (amputation/loss of limb of upper extremities).*** Major symptoms are loss of one or more fingers, hands, or arms. This category also includes paralysis/spinal cord injuries such as quadriplegic which result in a partial or total motor and sensory loss of all limbs and torso, other orthopedic injury limiting voluntary movement and severe burns (thermal injury to skin).
- ✓ ***Mobility (amputation/loss of limb of lower extremities).*** Major symptoms are loss of one or more toes, feet, legs. This category also includes paralysis/spinal cord injuries such as paraplegic which result in an impairment in motor or sensory function of the lower extremities or quadriplegic.
- ✓ ***Cognition (behavioral health/TBI).*** Major symptoms are:
    - Be*havioral health – PTSD:* flashbacks, intrusive thoughts, nightmares, hyper-arousal, irritability, memory & concentration problems, emotional withdrawal.
    - *Behavioral health – depression:* depressed mood, loss of interest in daily activities, fatigue, feelings of worthlessness, impaired ability to concentrate & make decisions, suicidal ideation.
    - *TBI – mild:* headache, fatigue, memory & concentration problems, irritability.
    - *TBI – moderate/severe:* significant memory & concentration problems, irritability, motor weakness, balance problems, speech deficits, seizures, chronic pain.

Moreover, this discussion on accessibility makes the following assumptions:

- The standard is a private voting session; no assistance from another person should be required.
- Personal assistive devices are assistive technologies which are not cost prohibitive and it is reasonable to assume the voter has access to or could gain access to device easily and knows how to operate them.

3 Postal Return of Ballots

The standard vote-by-mail (VBM) model is the most common absentee balloting method in use today to meet UOCAVA requirements. It involves three key steps: 1) ballot request by the voter, 2) delivery of the absentee ballot, and 3) return of the ballot via postal service. Within the vote-by-mail model, there are two delivery methods of the ballot to the voter – physical or electronic delivery.

Physical delivery most commonly involves use of a postal service to transmit the ballot from the jurisdiction to the voter. (For brevity, this discussion is also going to consider facsimile delivery to be equivalent to physical delivery as the security and accessibility considerations are very similar).

Electronic delivery to the voter may be accommodated by an internet portal service where the voter authenticates their identity in order to receive an electronic copy of their ballot, or through direct email transmission of a ballot document from the jurisdiction to the voter. The former is quickly becoming the most widely used electronic delivery mechanism due to the success of the Federal Voting Assistance Program (FVAP) Electronic Voting Support Wizard and Electronic Absentee Systems for Elections projects in 2010 and 2011 respectively. Additionally, the latter (email delivery of the ballot) offers inferior levels of security and traceability. For this discussion, therefore, electronic delivery is assumed to be a secure internal portal service which makes full use of the technological security controls available (i.e. encryption, digital signatures, strong authentication, etc).

The distinguishing feature of the traditional vote-by-mail (postal return) method remains that the physical ballot must be returned via a postal service to the originating jurisdiction. This is most often accomplished through what is termed the two-envelope system where the voter inserts the ballot inside an interior envelope, signs the voter statement, and inserts the interior envelope with the voter statement into an outside mailing envelope. Upon receipt at the local jurisdiction, the identity of the voter is then authenticated through signature verification before the ballot is separated from the voter's identify and set aside for tabulation. This process protects the privacy of the ballot without compromising the need to determine voter eligibility. Some jurisdictions utilize technologies for voter signature verification that can serve to mitigate the heavy workload of this process. This is most commonly encountered in jurisdictions with large vote-by-mail returns (e.g. the State of Washington). However, this task is traditionally performed through a manual signature comparison of the absentee ballot materials to the voter registration system. Postal return of the absentee ballot may also be required by the jurisdiction as a "backup" or means of verification for absentee voters who utilize one of the other ballot return methods.

3.1 UOCAVA Vote-by-mail (VBM) Security

For each key step in the VBM model, there are inherent risks, subject to current and future attempts to mitigate them. Since the first key step (ballot request by voter) is common and is not dependent on the ballot return method, we will focus on the risks of the second (ballot delivery) and third (ballot return) phases of the VBM model by comparing the postal delivery, electronic delivery, and postal return of ballots.

Table 3-1. Postal Return Channel - Security requirements assessment

Security Factor		Physical Delivery/Postal Return	Electronic Delivery/Postal Return
BALLOT DELIVERY	**Speed of Delivery/Ballot Replacement**	Low (Less secure) Lengthy processing time – delivering the physical documents to the voter may take a lengthy period depending on distance and which postal service is utilized, in addition to the lengthy manual process involved in approving and packaging the absentee ballot request. Replacement is difficult – if the ballot is incorrect, destroyed in transport, or otherwise subject to replacement, the manual processes involved must be repeated.	High (Highly Secure) With electronic delivery, ballots are posted by the local election jurisdiction and pulled from the secure website. As soon as the ballots are posted by the jurisdiction, the voter can login and download the ballot. For replacements, the voter may return and repeat the process.

Security Factor		Physical Delivery/Postal Return	Electronic Delivery/Postal Return
	Provide Correct Ballots	Medium (Reasonably secure) Incorrect documents provided – since the selection of the correct physical ballot is a manual process, it carries increased risk that the jurisdiction may provide an incorrect ballot to the voter or omit key components of the absentee package.	Medium (Reasonably secure) Reliant on incorrect data – electronic delivery is reliant on voter and ballot information accuracy as stored in the local voter registration and election management systems. If this data is not correct when provided to the ballot delivery system, voters may not receive the correct ballots.
	Prevent Ballot Tampering	Medium (Reasonably secure) Physical security of key documents – the security of the VBM process is dependent on the secure transport of the physical documents via postal service, public or private, to the voter.	High (Highly Secure) With electronic delivery, ballots are available from a secure website, which establishes a secure channel between the voter and the server that does not allow tampering of the ballot sent.
	Prevent Ballot Spoofing	High (Highly Secure) Ballots are sent inside official mailing envelopes and may contain an official seal on the ballot to represent its authenticity.	High (Highly Secure) With websites, the ballot spoofing concerns are based on illegitimate websites presenting themselves as official. However, secure websites have multiple ways to present proof of authenticity to voters. First, the use of a digitally signed certificate will authenticate the web server to the voter's web browser. Second, the web portal can implement a security image which should be verified by the voter when logging in.
	Ensure proper delivery	Low (Less secure) Address changes – postal delivery relies on the election official having the most recent physical address of the voter in order to send the ballot to the correct location. When this is not the case, the voter may never receive the ballot and/or the ballot may go to an unqualified voter.	High (Highly Secure) Electronic delivery is not restricted based on the voter's physical location. Instead, voters can access their ballots from nearly anywhere. Authentication is typically based on something the voters knows or has with them so this also does not pose a restriction on the delivery to the voter.
BALLOT RETURN	**Eligibility**	Low (Less secure) Easy involuntary impersonation to cast a vote. Handwritten signatures are difficult to validate accurately or not always validated. With physical delivery, it is also very difficult to assure that the correct voter received the ballot. This is mitigated when using electronic delivery because the voter is authenticated in order to download the ballot.	
	Privacy	Medium (Reasonably secure) Voter Privacy – the voter's right to a private ballot is limited to the physical security of the postal service used to transport the ballot to the original jurisdiction and to the procedures followed by the local jurisdiction to open and tabulate the voter's ballot in a manner which preserves the voter's privacy.	
	Integrity	Low (Less secure) Physical security of key documents – the integrity of the voted ballot is subject to the physical security of the means used to transport the ballot to the original jurisdiction. There is no way	

Security Factor		Physical Delivery/Postal Return	Electronic Delivery/Postal Return
		to prove that the cast vote stays unaltered during the election process.	
	Voter verifiability - cast as intended	Low (Less secure) Although there are tools to track a vote sent by mail (counted as cast), there is no guarantee that the envelope received by the election officials contains the same vote cast by the voter, as the voter cannot verify if the ballot contents are the same selected by him/her.	
	Voter verifiability - counted as cast	Medium (Reasonably secure) The voter can verify that his/her ballot is present during the tallying process through a ballot tracker, which is a system updated by the local election jurisdiction when receiving the ballot.	
	Prevent intermediate results	Medium (Reasonably secure) Intermediate results – the physical ballot may be intercepted by a third party in order to ascertain early results.	
	Ballot box accuracy	Medium (Reasonably secure) It is possible to add bogus ballots without detection. Votes can also be eliminated during transportation. However, handwritten signatures can be verified to detect massive fraud.	
	Coercion and vote buying resistance	Low (Less secure) Voter coercion – third parties with access to the voter and the physical ballot may influence the marking of the ballot.	
	Channel reliability	Low (Less secure) Lengthy return time – returning the physical documents to the jurisdiction may take a lengthy period of time, subject to the same constraints as the delivery of materials to the voter. Incorrect documents returned – successful return of the ballot is dependent on the voters' inclusion of all required materials to the jurisdiction; omission of items may delay the processing of or invalidate the absentee ballot altogether. This voting channel depends on the reliability of the postal system in the country from which votes are cast. It is not unusual to receive votes after the closing date and voters cannot do anything.	
	Auditability	Low (Less secure) Limited auditability – the physical ballot does not provide means for the jurisdiction to detect the alteration or deletion of voter marks that may have occurred in transit.	

3.2 UOCAVA Vote-by-mail Accessibility

Voters who utilize the vote by mail absentee balloting method where ballots are delivered by postal mail are not afforded any personal assistive devices other than those available for reading and marking standard paper. The only widely availability technology for reading printed documents is based on Optical Character Recognition (OCR) which requires specific hardware to scan and process the printed document. While the OCR technology is becoming more reliable, it often has difficulty with special characters and complex layouts which are common with ballots.

For voters who receive their ballots electronically through an electronic ballot delivery (EBD) system, there are many more personal assistive devices available to read and mark their ballot through the use of their personal computer. These voters are still forced to print out and submit the ballots via postal mail. This introduces a gap between the time the ballot is printed and placed into the postal system where there are little to no personal assistive

devices which will assist a voter with a disability in properly returning the ballot. A table providing the personal assistive devices available for the postal return channel is presented below.

Table 3-2. Postal Return Channel – Accessibility assessment

Impairment Type	Physical Delivery/Postal Return	Electronic Delivery/Postal Return
Blindness	Low (Less secure) Few assistive devices are available for reading a paper ballot much less marking and returning it. For reading the ballot, there are technologies available to convert the type font on the paper to auditory sounds. This technology requires a scanner and optical character recognition software in order to transcribe the text into audible words. However, in the case of ballots with several races and complex layout, it may be complicated to reproduce the ballot without introducing errors into audible words. In a remote voting environment, there is no assistive device for marking a paper ballot, reviewing the marks, and returning it.	Medium (Reasonably secure) The following are assistive devices which are widely available for remote voters with blindness to read, mark, and review their ballots on a computer. • Screen reader (interprets the page's HTML code and reproduces its content as speech correctly for the voter). • Headphones with adjustable volume. • Standard keyboard – the website supports keyboard-based navigation and selection (i.e. no mouse required). • Reduced keyboard (numeric keyboard) with access to all voting functionalities. • Keyboard with Braille embossed – keyboards can be equipped with braille stickers to indicate each key for navigation and selection on the website. The voter must still print his or her ballot, sign the voter statement, and return the ballot via postal mail.
Partial visual loss / visual dysfunction	Medium (Reasonably secure) There are traditional and computer enhanced magnifiers to assist with reading, marking, reviewing, and returning the ballot. There is no ability, however, to adjust the contrast ratio of the printed ballot.	Medium (Reasonably secure) The same personal assistive devices are available for electronic delivery as those referenced above for blindness plus the ability to adjust the contrast ratio of the images and text on the website and use an independent screen magnifier (adjustable entire screen contrasts, color and font sizes). The voter must still print and sign the voter statement before inserting the ballot into the return envelope for postal return.
Deafness	High (Highly Secure) There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot.	High (Highly Secure) There is no auditory requirement for reading, marking, reviewing, or returning an electronically delivered paper ballot.
Partial hearing loss / tinnitus	High (Highly Secure) There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot.	High (Highly Secure) There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot.
Dexterity (amputation/loss of limb of upper extremities)	Low (Less secure) There are no widely available personal assistive devices to assist voters with dexterity impairments in physically marking the paper ballots. It is also difficult for these voters to sign the voter statement and enclose their ballot properly for return.	Medium (Reasonably secure) The following are assistive devices which are widely available for remote voters with dexterity impairments to use to read, mark, and review their ballots on a computer. • Sip and puff device (simple and effective way to control mouse button clicking/mouse movement). • Head mouse (mouse controlled with the head). • Screen/virtual keyboard.

Impairment Type	Physical Delivery/Postal Return	Electronic Delivery/Postal Return
		• External devices emulating mouse and keyboard. The voter must still print his or her ballot, sign the voter statement, and return the ballot via postal mail.
Mobility (amputation/loss of limb of lower extremities)	High (Highly Secure) There are no mobility requirements for reading, marking, reviewing, and returning an absentee paper ballot which was delivered to the voter's location.	High (Highly Secure) There are no mobility requirements for reading, marking, reviewing, and returning an absentee paper ballot which was downloaded to the voter's personal computer.
Cognition (behavioral health / TBI)	Medium (Reasonably secure) Paper ballots are well understood because of their pervasiveness but they do not provide much assistance to voters with cognitive impairments. The use of clear, brief instructions and a simple ballot layout is the best approach.	Medium (Reasonably secure) Electronic delivery of ballots has a number of mechanisms it can use to assist those voters with cognitive impairments. Beyond what can be done on the electronic ballot delivery service, the voter will still have to print and assemble the return envelopes according to the standard instructions in order to properly return the ballot. A few examples are included below: • Use of common images to help recognize instructions and ballot content. • Use of common colors and font types to represent important concepts. • Use of common sounds and signals to signify the completion of an event. • Use of simple written instructions. • Use of simple verbal instructions. • Use of step by step processes (i.e. break down complex ballot marking into smaller steps). • Provide longer explanations for tasks, as necessary. • Provide warnings for common voter mistakes, such as under-voting and over-voting.

4 Fax Return of Ballots

Note: Although this is not currently a legal return option under Virginia state law, various other states do support this return method for UOCAVA voters. Therefore, the discussion paper assumes its legality solely for purpose of comparison

Another method of returning an absentee ballot utilizes facsimile transmission of the physical ballot from the voter to the originating jurisdiction. This method improves upon the time constraints of the traditional VBM process since receipt of the voted ballot is no longer limited by the speed of the postal service(s) involved. Rather, the image of the voted ballot is captured and sent to the jurisdiction using machines that transmit over traditional analog phone-lines or digital facsimile service.

4.1 UOCAVA Fax Return Security

Typically, if this method is allowed by a jurisdiction, it requires that the voter submit additional documentation, primarily an agreement that their right to a secret ballot has been waived. Since the ballot is transmitted in the clear, unlike the traditional postal channel where the secrecy of the voted ballot is preserved, alongside the voter's identification, there is no longer a reasonable expectation that their votes can be kept independent of their identity at the time when the ballot is received. After confirmation of the voter's registration, however, the ballot is sealed and set aside for tabulation. The voter may also be required by the jurisdiction to transmit the original physical ballot to the jurisdiction by postal service as an additional step. The following table details the security afforded to facsimile return. Refer to Table 3-1 for the security assessment for the physical and electronic delivery.

Table 4-1. Fax Return Channel – Security requirements assessment

Security Factor	Fax Return (physical delivery or electronic delivery)
Eligibility	Low (Less secure) Easy involuntary impersonation to cast a vote. Handwritten signatures are digitized and therefore easy to tamper with. With physical delivery, it is also very difficult to assure that the correct voter received the ballot. This is mitigated when using electronic delivery because the voter is authenticated prior to downloading the ballot.
Privacy	Low (Less secure) Votes are received without any privacy protection. Voters are required to sign a secrecy waiver. The voter's right to a private ballot is lost since the facsimile transmission method cannot separate the ballot from the registration information.
Integrity	Low (Less secure) There is no way to prove that the cast vote stays unaltered during the election process.
Voter verifiability - cast as intended	Low (Less secure) There is no guarantee that the fax vote is received at the destination as it was cast by the voter and there are no mechanisms for the voter to verify if the received ballot contents are the same selected by him/her.
Voter verifiability - counted as cast	Medium (Reasonably secure) The voter can verify that his/her ballot is present during the tallying process through a ballot tracker, which is a system updated by the local election jurisdiction when the ballot is accepted.
Prevent intermediate results	Low (Less secure)

Security Factor	Fax Return (physical delivery or electronic delivery)
	Vote contents could be accessed during the transmission. The vote contents are always accessible upon reception.
Ballot box accuracy	Medium (Reasonably secure) It is possible to add bogus ballots without detection. However, the fax numbers of the voters can be audited in order to detect mass fraud.
Coercion and vote buying resistance	Low (Less secure) Voters can show the selected voting options to third parties before casting their votes, making coercion and vote selling possible.
Channel reliability	High (Highly Secure) Voters realize if their fax vote has not reached the election authority. Therefore contingency measures (e.g., try later or use another voting channel) can be used to prevent the loss of their votes. Incorrect documents returned – mitigated in part through the shorter delivery time; this allows the voter to more easily rectify the missing or incorrect documentation.
Auditability	Low (Less secure) Voting channel (land phone) is difficult to audit and does not generate enough trails to solve any dispute and to audit the entirety of the election process to ensure its correct execution. Moreover, the facsimile ballot image does not provide means to detect the alteration or deletion of voter marks on the ballot.

4.2 UOCAVA Fax Return Accessibility

If a voter chooses to return their voted ballot by fax, he or she is going to be afforded nearly identical accessibility assistance as a voter who is returning their ballot by postal mail. There is one notable exception to this, however, if the voter is receiving the ballot electronically. There are programs available which would allow the voter to fax his ballot without ever having to print the ballot PDF. There are numerous security concerns with this, but no more so than returning the ballot by traditional fax. By keeping the ballot completely digitized, this vastly increases the number of personal assistive devices which the voter can utilize. The voter would still have to return other statements with his or her ballot which would require the voter's signature. So long as digital signatures are not accepted, the voter would have to print out, sign the voter statement, and scan it into the computer in order to fax it along with the ballot. As one can see, there are some possible improvements to accessibility with the fax return channel but none which represent a definitively better alternative for voters. Therefore, the discussion concludes that the same accessibility scores will be given to the fax return channel as with postal return (reference

Table 3-2 for this analysis).

5 Email Return of Ballots

Note: Although this is not currently a legal return option under Virginia state law, various other states do support this return method for UOCAVA voters. Therefore, the discussion paper assumes its legality solely for purpose of comparison

Another technologically available method for the return of an absentee ballot is via email service over public email exchanges. As with postal and facsimile returns, the ballot may be initially delivered to the voter through physical or electronic means. The email return process itself may take two slightly different forms: email transmission of a scanned image of the original ballot or email transmission of an electronic ballot document (e.g. a .PDF image of the ballot). If the ballot is provided to the voter via postal service, conversion into an electronic copy presents an additional hurdle to the voter because it will have to be scanned into the computer. However, the presence of a physical copy does allow for the voter to return the original ballot document as a supplement to their electronic return. If the voter marks and downloads the ballot from an electronic delivery service, the voter can attach the ballot directly to an email. It is important to mention that the voter will likely still be required to sign, scan and attach the voter statement to the email as well. This will require the voter to use a printer and scanner. Unfortunately, this impacts the overall appeal of the email option as detailed in the security and accessibility analysis below.

5.1 Email Return Security

The security of the ballot delivery options was discussed previously and detailed in Table 3-1. Therefore, this section will focus on the security controls afforded to ballots using email as the return channel.

In this discussion of email return, the use of an encryption client is not being considered because, in order for it to be securely used, the voter and election official have to share a cryptographic key or the election official has to setup a PKI (public key infrastructure). This is a difficult implementation and is prone to error, even with expert assistance. Furthermore, the discussion concludes that if the encryption system is strong enough, it will likely resemble a secure electronic return option and will no longer be considered email return. The assessment for standard email return security is below.

Table 5-1. Email Return Channel – Security requirements assessment

Security Factor	Email Return (physical delivery or electronic delivery)
Eligibility	Low (Less secure) Easy involuntary impersonation to cast a vote. Handwritten signatures are digitized and therefore easy to tamper with. With physical delivery, it is also very difficult to assure that the correct voter received the ballot. This is mitigated when using electronic delivery because the voter is authenticated in order to download the ballot.
Privacy	Low (Less secure) Votes are received without any privacy protection. Voters are required to sign a secrecy waiver. The voter's right to a private ballot is lost since the email transmission method cannot separate the ballot from the registration information.
Integrity	Low (Less secure) There is no way to prove that the cast vote stays unaltered during the election process.
Voter verifiability - cast as intended	Low (Less secure) The voter does not have any means to individually verify that the email vote is received at the destination as it was cast by the voter and there are no mechanisms for the voter to verify if the received ballot contents are the same as those selected by him/her.
Voter verifiability -	Medium (Reasonably secure)

Security Factor	Email Return (physical delivery or electronic delivery)
counted as cast	The voter can verify that his/her ballot is present during the tallying process through a ballot tracker, which is a system updated by the local election jurisdiction when the ballot is accepted.
Prevent intermediate results	Low (Less secure) Vote contents could be accessed during the transmission. The vote contents are always accessible upon reception.
Ballot box accuracy	Low (Less secure) It is possible to add bogus ballots. Email addresses can be impersonated. Emails can be eliminated during transmission.
Coercion and vote buying resistance	Low (Less secure) Voters can show the selected voting options to third parties before casting their votes, making coercion and vote selling possible.
Channel reliability	Medium (Reasonably secure) E-mail reception confirmation can be sent to the voter. However the e-mail transmission can be delayed. Incorrect documents returned – mitigated in part through the shorter delivery time; this allows the voter to more easily rectify the missing or incorrect documentation.
Auditability	Low (Less secure) Voting channel (mailers, DNS servers, etc.) is difficult to audit and does not generate enough trails to solve any dispute and to audit the entirety of the election process to ensure its correct execution.

5.2 Email Return Accessibility

The email return of ballots requires that the voter return the ballot in a digital form. This increases the chances that a voter with disabilities will have access to one or more personal assistive devices which may assist him or her with reading, reviewing, and returning the ballot. Whether the ballot is physically delivered or electronically delivered, the chances are that the voter will interact with the ballot at some point when it is in Portable Document Format (PDF). This is the most common file exchange format and the most common program for viewing a PDF is Adobe Reader. Fortunately, Adobe Reader offers the ability for screen readers and other personal assistive technologies to work with the PDFs. That said, Adobe and other PDF readers are often limited in the accessibility support depending on how the PDF file was created. This is actually quite important for this discussion because a downloaded PDF document will be substantially more accessible than ones which are created from a scanned paper document. This consideration and others are discussed in further detail in the table below.

Table 5-2. Email Return channel – Accessibility assessment

Impairment Type	Physical Delivery/Email Return	Electronic Delivery/Email Return
Blindness	Low (Less secure) There is nothing inherent in the email return option which affords the voter any more assistance than if returning the paper ballot by mail. If the voter wishes to have the ballot contents read aloud, the voter will still need to scan the ballot into a computer with optical character recognition abilities. This will convert the	High (Highly Secure) The following are assistive devices which are widely available for remote voters with blindness to use to read, mark, review, and return their ballots on a computer. With email return, the ballot does not have to be printed and the voter can therefore review the ballot in PDF form prior to returning it via email. • Screen reader (interprets the page's HTML code

Impairment Type	Physical Delivery/Email Return	Electronic Delivery/Email Return
	printed text into digital words and sentences. This will have some success at reading the ballot contents but the success rates vary and become lower the more complex the original document is. In any case, the OCR technology will not be able to verbally indicate a marked or unmarked oval/square to the voter so there is no way for the voter to confirm his or her selections prior to sending the email.	and the PDF and reproduces its content as speech correctly for the voter). In this case, the screen reader clearly indicates whether each race is marked or unmarked. • Headphones with adjustable volume. • Standard keyboard – the website supports keyboard-based navigation and selection (i.e. no mouse required). • Reduced keyboard (numeric keyboard) with access to all voting functionalities. • Keyboard with Braille embossed – keyboards can be equipped with Braille stickers to indicate each key for navigation and selection on the website.
Partial visual loss / visual dysfunction	<u>Medium (Reasonably secure)</u> Prior to scanning the ballot into the computer, there are traditional and computer enhanced magnifiers to assist with reading, marking, and reviewing the ballot. Once the ballot is scanned in, the voter can use a screen magnifier to review the ballot, attach it to an email, and send the email. There are still very few assistive technologies in regards to marking the ballot. For example, there is no alternative to a pen/pencil to mark the ballot, such as one that uses Braille or large icons.	<u>High (Highly Secure)</u> The same personal assistive devices are available for electronic delivery as those referenced above for blindness plus the ability to adjust the contrast ratio of the images and text on the website and use an independent screen magnifier (adjustable entire screen contrasts, color and font sizes). Since the ballot will be returned by email, the voter will be able to use these technologies throughout the entire process. The only drawback here is that the voter will have to move the ballot from one application (the electronic ballot delivery website) to the email client. This will most likely use PDF to transfer the ballot which will have separate accessibility provisions than the EBD website.
Deafness	<u>High (Highly Secure)</u> There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot by email.	<u>High (Highly Secure)</u> There is no auditory requirement for reading, marking, reviewing, or returning an emailed ballot.
Partial hearing loss / tinnitus	<u>High (Highly Secure)</u> There is no auditory requirement for reading, marking, reviewing, or returning a paper ballot by email.	<u>High (Highly Secure)</u> There is no auditory requirement for reading, marking, reviewing, or returning an emailed ballot.
Dexterity (amputation/loss of limb of upper extremities)	<u>Low (Less secure)</u> There are no widely available personal assistive devices to assist voters with dexterity impairments in physically marking the paper ballots or scanning it into the computer to email.	<u>High (Highly Secure)</u> The following are assistive devices which are widely available for remote voters with dexterity impairments to use to read, mark, and review their ballots on a computer. The voter should be able to use these devices to download the PDF from the electronic delivery website and attach it to an email. It may require more steps than preferred (switching applications) but it will be possible with these assistive devices: • Sip and puff device (simple and effective way to control mouse button clicking/mouse movement). • Head mouse (mouse controlled with the head). • Screen/virtual keyboard. • External devices emulating mouse and keyboard

Impairment Type	Physical Delivery/Email Return	Electronic Delivery/Email Return
Mobility (amputation/loss of limb of lower extremities)	High (Highly Secure) There are no mobility restrictions for reading, marking, reviewing, and returning an absentee paper ballot which was delivered to the voter's location and is being returned via email.	High (Highly Secure) There are no mobility restrictions for reading, marking, reviewing, and returning an absentee paper ballot which was downloaded to the voter's personal computer and returned via email.
Cognition (behavioral health / TBI)	Medium (Reasonably secure) Paper ballots are well understood because of their pervasiveness but they do not provide much assistance to voters with cognitive impairments. This is exacerbated by the use of email clients and the scanners required to convert the ballot to a digital image.	Medium (Reasonably secure) Electronic delivery of ballots has a number of mechanisms it can use to assist those voters with cognitive impairments. Beyond what can be done on the electronic ballot delivery service, the voter will still have to attach the ballot to an email and follow other instructions in order to properly return the ballot. A few examples are included below: • Use of common images to help recognize instructions and ballot content. • Use of common colors and font types to represent important concepts. • Use of common sounds and signals to signify the completion of an event. • Use of simple written instructions. • Use of simple verbal instructions. • Use of step by step processes (i.e. break down complex ballot marking into smaller steps). • Provide longer explanations for tasks, as necessary. • Provide warnings for common voter mistakes, such as under-voting and over-voting.

6 Secure Electronic Return

Note: Although this is not currently a legal return option under Virginia state law, various other states allow for and are pursuing this return method for UOCAVA voters. Therefore, the discussion paper assumes its legality solely for purpose of comparison

Secure electronic return is a return channel that uses electronic ballots and allows voters to transmit the voted ballot to election officials over the internet. This option has been used in various locations in the United States and across the world to aid overseas voters in completing the absentee voting process in a quick, accessible, and secure manner. This return channel relies on electronically delivery of ballots through a secure online system. These ballots are marked by the voter then subsequently encrypted and digitally signed for secure transmission. There are many variants of how secure electronic return can be implemented. Each variant represents a unique cost, usability, and security balance. The analysis below will assume the most advanced implementation which is known as a Remote End-To-End Verifiable eVoting System.

6.1 Secure Electronic Return Channel Security

Secure Electronic Return technology is often based on the use of advanced cryptography to achieve the unique security requirements of voting from a remote location. Many of the technologies employ the use of proven cryptographic primitives such as hash functions, digital signatures, and public key cryptography. The most recent and revolutionary techniques utilize homomorphic properties present in certain cryptosystems to achieve end-to-end verifiability. This concept provides both voters and universal auditors with the ability to verify the accuracy of an electronic return system without violating any other requirements, such as voter privacy. These advances in secure electronic return technology are considered below in this assessment.

The security of the ballot delivery options was discussed previously and detailed in Table 3-1. Therefore, this section will focus on the security controls afforded to ballots using secure electronic return as the return channel.

Table 6-1. Secure Electronic Return Channel – Security requirements assessment

Security Factor	Secure Electronic Return
Eligibility	High (Highly Secure) The use of strong authentication such as digital certificates prevents the involuntary impersonation of voters.
Privacy	High (Highly Secure) Votes are encrypted before being cast. Cryptographic measures, such as random mixing processes, can be implemented to break any connection between vote and voter. Additionally, voters can protect their PC's against malware or use secure voting kiosks, but it is a voter's choice.
Integrity	High (Highly Secure) Votes can be digitally signed, preventing any manipulation. Furthermore, when using voting receipts, any attempt to delete a vote could be detected by the voter when verifying the receipt. Additionally, voters can protect their PC's against malware or use secure voting kiosks
Voter verifiability - cast as intended	High (Highly Secure) A verification process can be implemented as an independent process from the vote selection process in the voting terminal, which allows the voters to check if the vote received by the election officials and stored in the remote Ballot Box is the same as cast by the voter. Votes are protected by cryptographic means after being cast.
Voter verifiability - counted as cast	High (Highly Secure) A voting receipt can be generated from the digital signature of the encrypted ballot, which allows voters to individually verify that their votes are present in the tallying process.

Security Factor	Secure Electronic Return
Prevent intermediate results	High (Highly Secure) Votes are encrypted before they are cast. Only the authorized officials of the jurisdiction can decrypt them at the end of the election.
Ballot box accuracy	High (Highly Secure) Each encrypted vote can be digitally signed using a unique voter digital certificate to prevent the addition of bogus votes. Additionally, voting receipts can be provided to voters to allow them to detect the elimination of their votes.
Coercion and vote buying resistance	Medium (Reasonably secure) By providing a mechanism that allows voters to self-spoil their ballots and cast replacements, the risk of voter coercion is severely diminished. Voter coercion and voting buying schemes are highly dependent on forcing the voter to provide "proof" of the contents of the final ballot or forcing the use of a premarked ballot on the voter. Self-spoiling eliminates this possibility.
Channel reliability	High (Highly Secure) Voters realize if their vote has not reached the election authority if an error arises when casting the vote. Therefore contingency measures (e.g., try later or use another voting channel) can be used to prevent the lost of their votes.
Auditability	High (Highly Secure) Voters can individually check the accuracy of the election with their voting receipts. Auditors can audit the voting application using independent calculation of homomorphic proofs.

6.2 Secure Electronic Return Channel Accessibility

Because the use of a secure electronic return channel is most securely accomplished using a unified system, the voter can interact with a single entirely electronic interface to receive, read, mark, and return their ballot. This provides great benefits for using personal assistive devices throughout the voting process. First, all of the operations are conducted through a web browser. Therefore, so long as the voting application is compliant with Section 508 of the US Rehabilitation Act, the entire interface can be read by a screen reader. Furthermore, the voter can use the keyboard, voice commands, a head-mouse, and other alternative input devices to make selections and navigate the ballot. When finished, the voter can have the ballot as marked read back to him/her and with the click of a button, submit their ballot or modify it (if changes are required after the ballot review). This presents a tremendous ease-of-use advantage over having to download, print and attach the ballot to an email. Below is the analysis of the accessibility options available with secure electronic return.

Table 6-2. Secure Electronic Return Channel – Accessibility assessment

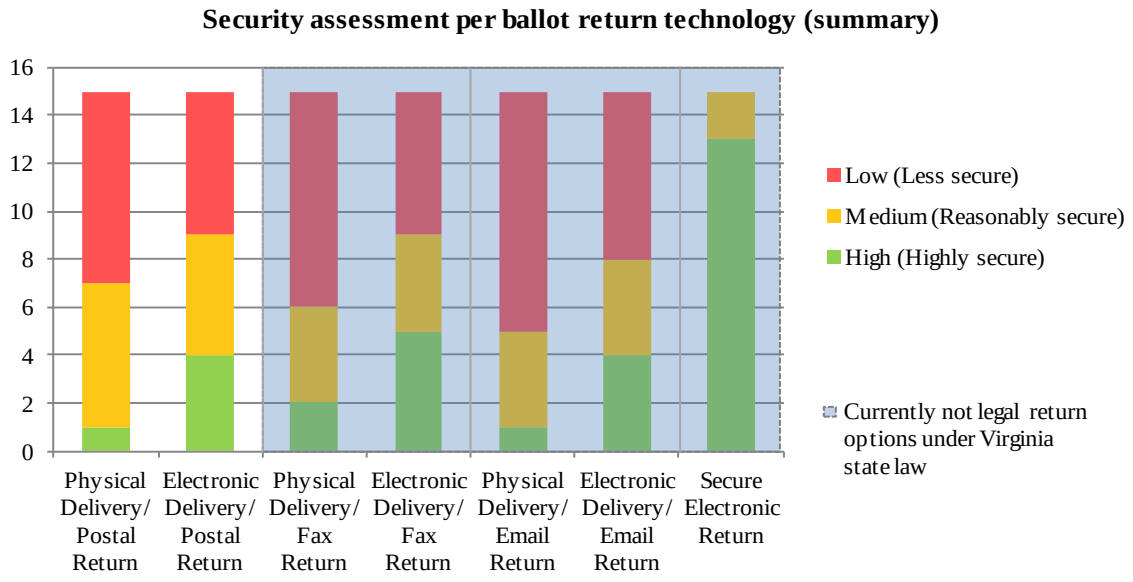
Impairment Type	Secure Electronic Return
Blindness	High (Highly Secure) The following are assistive devices which are widely available for remote voters with blindness to use to read, mark, review, and return their ballots on a computer. With secure electronic return, the ballot does not have to be printed and the voter can review the ballot by having the screen reader read the review screen. As opposed to reading a PDF, the review screen of an electronic ballot delivery/return system can be specially tailored to the voting context. • Screen reader (interprets the page's HTML code and reproduces its content as speech correctly for the voter) • Headphones with adjustable volume

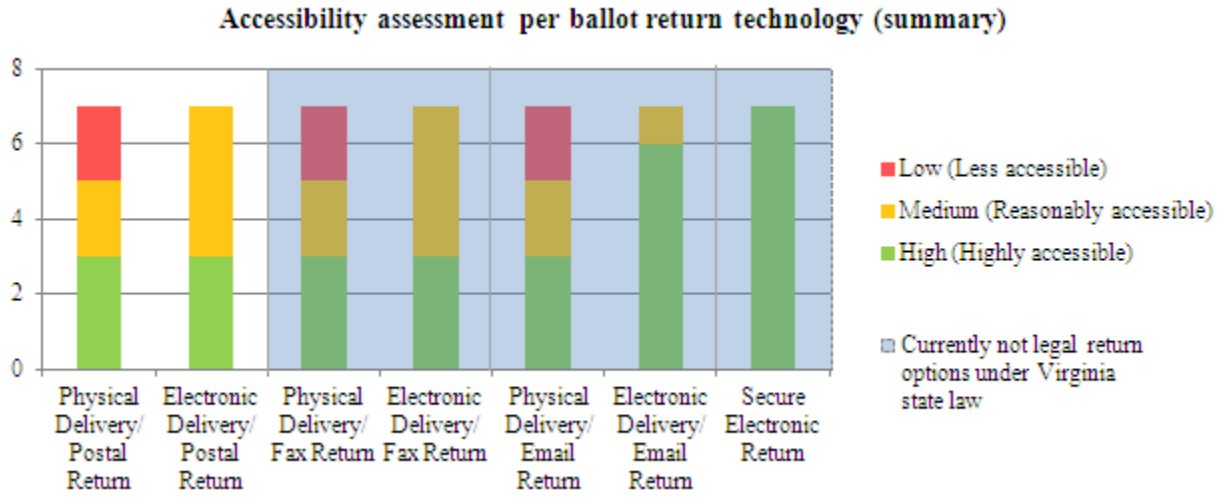
Impairment Type	Secure Electronic Return
	• Standard keyboard – the website supports keyboard-based navigation and selection (i.e. no mouse required). • Reduced keyboard (numeric keyboard) with access to all voting functionalities. • Keyboard with Braille embossed – keyboards can be equipped with Braille stickers to indicate each key for navigation and selection on the website.
Partial visual loss / visual dysfunction	High (Highly Secure) The same personal assistive devices are available for electronic delivery and secure return as those referenced above for blindness plus the ability to adjust the contrast ratio of the images and text on the website and use an independent screen magnifier (adjustable entire screen contrasts, color and font sizes). Since the entire voting process uses the same system, the voter will be able to use these technologies throughout the entire process.
Deafness	High (Highly Secure) There is no auditory requirement for reading, marking, reviewing, or returning an electronic ballot.
Partial hearing loss / tinnitus	High (Highly Secure) There is no auditory requirement for reading, marking, reviewing, or returning an electronic ballot.
Dexterity (amputation/loss of limb of upper extremities)	High (Highly Secure) The following are assistive devices which are widely available for remote voters with dexterity impairments to use to read, mark, and review their ballots on a computer. The voter will be able to operate these devices to complete the entire voting system on the secure electronic system. This includes receiving, reading, marking, and returning the ballot. • Sip and puff device (simple and effective way to control mouse button clicking/mouse movement). • Head mouse (mouse controlled with the head). • Screen/virtual keyboard. • External devices emulating mouse and keyboard.
Mobility (amputation/loss of limb of lower extremities)	High (Highly Secure) There are no mobility restrictions for reading, marking, reviewing, and returning an electronic ballot.
Cognition (behavioral health / TBI)	High (Highly Secure) Electronic delivery of ballots has a number of mechanisms it can use to assist those voters with cognitive impairments. Because the voter will be using the secure electronic system for each step in the voting process, the entire process can use these cognitive assistance techniques to help the voter. • Use of common images to help recognize instructions and ballot content. • Use of common colors and font types to represent important concepts. • Use of common sounds and signals to signify the completion of an event. • Use of simple written instructions. • Use of simple verbal instructions. • Use of step by step processes (i.e. break down complex ballot marking into smaller steps). • Provide longer explanations for tasks, as necessary. • Provide warnings for common voter mistakes, such as under-voting and over-voting.

7 Concluding Thoughts

There is a general concern that the use of remote electronic voting channels generates more security issues than postal voting. However, after comparing the different channels used in the United States, we have seen that the secure electronic return voting channel concerns have similar implications as the postal voting ones. Furthermore, secure electronic return allows the implementation of additional security measures (such as cryptographic voting schemes) that can mitigate or, in some cases, eliminate common security risks of the remote voting methods currently accepted in the United States. That does not mean that the secure electronic return channel is free of security risks, but it does provide a better framework for managing those risks (as the residual risk level is low for almost all requirements). Furthermore, it is clear that secure electronic return provides the most access to personal assistive devices to help those voters with disabilities.

Regarding fax and email electronic voting channels, they can pose additional concerns relative to a secure electronic return. The nature of these channels (e.g., the use of unsecured land telephone networks or public email relays) does not effectively serve to enhance the security or accessibility of the voting process beyond that of traditional postal voting. As detailed earlier, in certain cases, these alternate channels may serve only to offset relief in one risk category with increased risk in another.





Note: Above charts summarize the ratings assigned in the previous sections. Tables summarizing these values can be found in Appendix A: Summary assessment tables.

8 Additional Resources

The following additional resources provide more in depth analysis of the return channels security and accessibility provisions.

http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/PUIGGALI_SecurityPractices_UOCAVA.pdf

http://csrc.nist.gov/groups/ST/UOCAVA/2010/PositionPapers/PUIGGALI_BestPracticesInternetVoting.pdf

http://csrc.nist.gov/groups/ST/UOCAVA/2010/Presentations/KING_UOCAVA_Vote_by_Mail.pdf

http://www.scytl.com/images/upload/home/PNYXCOREWhitePaper.pdf

Appendix A: Summary assessment tables

Appendix A.1: Security assessment table

	Requirement	Postal Return		Fax Return		Email return		Secure Electronic Return
		Physical Delivery	Electronic Delivery	Physical Delivery	Electronic Delivery	Physical Delivery	Electronic Delivery	
BALLOT DELIVERY	Speed of delivery/ballot replacement	Low	High	Low	High	Low	High	High
	Provide correct ballots	Medium	Medium	Medium	Medium	Medium	Medium	Medium
	Prevent ballot tampering	Medium	High	Medium	High	Medium	High	High
	Prevent ballot spoofing	High	High	High	High	High	High	High
	Ensure proper delivery	Low	High	Low	High	Low	High	High
BALLOT RETURN	Eligibility	Low	Low	Low	Medium	Low	Medium	High
	Privacy	Medium	Medium	Low	Low	Low	Low	High
	Integrity	Low	Low	Low	Low	Low	Low	High
	Voter verifiability - cast as intended	Low	Low	Low	Low	Low	Low	High
	Voter verifiability - counted as cast	Medium	Medium	Medium	Medium	Medium	Medium	High
	Prevent intermediate results	Medium	Medium	Low	Low	Low	Low	High
	Ballot box accuracy	Medium	Medium	Medium	Medium	Low	Low	High
	Coercion and vote buying resistance	Low	Low	Low	Low	Low	Low	Medium
	Channel reliability	Low	Low	High	High	Medium	Medium	High
	Auditability	Low	Low	Low	Low	Low	Low	High

Appendix A.2: Accessibility assessment table

Requirement	Postal Return		Fax Return		Email return		Secure Electronic Return
	Physical Delivery	Electronic Delivery	Physical Delivery	Electronic Delivery	Physical Delivery	Electronic Delivery	
Blindness	Low	Medium	Low	Medium	Low	High	High
Partial visual loss / visual dysfunction	Medium	Medium	Medium	Medium	Medium	High	High
Deafness	High	High	High	High	High	High	High
Partial hearing loss / tinnitus	High	High	High	High	High	High	High
Dexterity (amputation/loss of limb of upper extremities)	Low	Medium	Low	Medium	Low	High	High
Mobility (amputation/loss of limb of lower extremities)	High	High	High	High	High	High	High
Cognition (behavioral health / TBI)	Medium	Medium	Medium	Medium	Medium	Medium	High

STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System

Susan Bell, Office of the Travis County Clerk
Josh Benaloh, Microsoft Research
Michael D. Byrne, Rice University
Dana DeBeauvoir, Office of the Travis County Clerk
Bryce Eakin, independent researcher
Gail Fisher, Office of the Travis County Clerk
Philip Kortum, Rice University
Neal McBurnett, ElectionAudits
Julian Montoya, Office of the Travis County Clerk
Michelle Parker, Office of the Travis County Clerk
Olivier Pereira, Université catholique de Louvain
Philip B. Stark, University of California, Berkeley
Dan S. Wallach, Rice University
Michael Winn, Office of the Travis County Clerk

STAR-Vote is a collaboration between a number of academics and the Travis County (Austin), Texas elections office, which currently uses a DRE voting system and previously used an optical scan voting system. STAR-Vote represents a rare opportunity for a variety of sophisticated technologies, such as end-to-end cryptography and risk limiting audits, to be designed into a new voting system, from scratch, with a variety of real world constraints, such as election-day vote centers that must support thousands of ballot styles and run all day in the event of a power failure. This paper describes the current design of STAR-Vote which is now largely settled and whose development will soon begin.

1. INTRODUCTION

A decade ago, DRE voting systems promised to improve many aspects of voting. By having a computer mediating the user's voting experience, they could ostensibly improve usability through summary screens and a variety of accessibility features including enlarged text, audio output, and specialized input devices. They also promised to improve the life of the election administrator, yielding quick, accurate tallies without any of the ambiguities that come along with hand-marked paper ballots. And, of course, they were promised to be secure and reliable, tested and certified. In practice, DRE systems had problems in all these areas.

Many current DRE voting systems experienced their biggest sales volume after the failures of punch card voting systems in Florida in the 2000 presidential election. The subsequent Help America Vote Act provided a one-time injection of funds that made these purchases possible. Now, a decade later, these machines are near the end of their service lifetimes.

Last year, the Travis County election administration, having used Hart InterCivic's eSlate DRE system for over a decade, concluded that no system on the market—DRE or optical scan—met their future needs. They prefer to avoid hand-marked paper ballots because they open the door to ambiguous voter intent, a source of frustration in their previous centrally-tabulated optical scan system. They didn't want to go back.

Travis County's needs and preferences impose several significant constraints on the design of STAR-Vote:

DRE-style UI. Hand-marked ballots are not to be used, for the reason above. DRE-style systems were also preferred for their ability to offer facilities for voters with disabilities.

Printed paper ballot summaries. While the DRE-style UI was desired for entering selections, printed ballots were desired for their security benefits, verifiability by voters, and redundancy against failures in the electronic system. In order to save on paper and paper management, the county wished to only print a list of each voter's selections, analogous to the summary screens on many current-generation DRE systems.

All-day battery life. Power failures happen. Current-generation DRE systems have batteries that can last for hours. The new system must also be able to operate for hours without external power.

Early voting and election-day vote centers. Travis County supports two weeks of early voting, where any voter may vote in any of more than 20 locations. Also, on Election Day, any voter may go to any local polling place. Our county's voters informally report their appreciation of these benefits.

COTS hardware. Current DRE systems are surprisingly expensive. Travis County wants to use commercially available, off-the-shelf equipment, whenever possible, to reduce costs and shorten upgrade cycles. That is, "office equipment" rather than "election equipment" should be used where possible.

Long ballots. While voters in many countries only select a candidate for member of parliament, in the U.S., voters regularly face 100 or more contests for federal, state, and regional offices; judges; propositions; and constitutional amendments. STAR-Vote must support very long ballots as well as long list of contestants in each race.

These constraints interact in surprising ways. Even if the county did not have a strong preference for a DRE-like UI, pre-printed paper ballots are inefficient for vote centers, which may need to support hundreds or thousands of distinct ballot styles. Likewise, the requirement to run all-day on battery backup eliminates the possibility of using laser printers for ballot-on-demand printing, which consume far too much power.[1] We note that counties that face fewer constraints may choose to adopt quite different architectures. For example, a county without election-day vote centers might instead use pre-printed ballots and electronic ballot marking devices.

These constraints likewise eliminate prior-fielded e2e systems like Scantegrity [Carback et al. 2010; Chaum et al. 2008], and Prêt à Voter [Ryan and Peacock 2006; Burton et al. 2012], which rely on hand-marked paper, and Helios [Adida et al. 2009; Adida 2008], which is meant for use in web browsers, not traditional polling locations. Wombat [Ben-Nun et al. 2012] has a paper trail, but it's only designed for single-issue ballots. VoteBox [Sandler et al. 2008] has a DRE-like interface, but it's an entirely paperless system. Instead, to satisfy our constraints, we must build something new, or at least extend an existing system to satisfy our constraints.

We were charged with using the latest advances in human factors, end-to-end cryptography, and statistical auditing techniques, while keeping costs down and satisfying many challenging constraints. We want to generate quick, verifiable tallies when the election is over, yet incorporate a variety of audit mechanisms (some voter-verifiable, others facilitated by auditors with additional privileges).

We notably have chosen to design STAR-Vote without explicitly worrying about the constraints of State or Federal certification. Of course, for STAR-Vote to go into production, these challenges need to be addressed, but at least for now, our focus has been on designing the best possible voting system given our constraints.

2. VOTER FLOW

Figure 1 shows how STAR-Vote works from the perspective of a voter. The STAR-Vote voting system bears a resemblance to the Hart InterCivic eSlate system and to VoteBox [Sandler et al. 2008], in that the voting machines are networked together, simplifying the movement of data. Like eSlate, our design contains a networked group of voting machines that share a common judge's station with a computer like Hart InterCivic's "Judge Booth Controller" (JBC) that manages everything.

(1) *Registration (pollbook).* The first step for the voter is to check-in with a poll worker. This is where voter registration is verified and the voter's precinct and ballot style are determined. The

[1] A laser printer might consume 1000 watts or more while printing. A reasonably good UPS, weighing 26 kg, can provide that much power for only ten minutes. Since a printer must warm up for each page when printed one-off (perhaps 10 seconds per page), the battery might be exhausted by printing as few as 60 ballots.

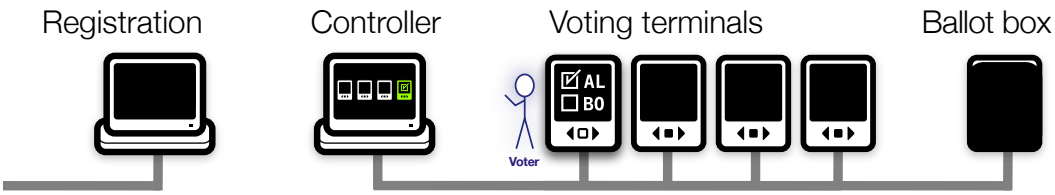


Fig. 1. The design of the STAR-Vote system. The voter registration system (left) is connected to the Internet but not to the internal LAN. Voters move left to right. First, the voter's registration is validated, and a thermal printout indicates the proper ballot style. This moves to the controller, which scans it and issues the voter a PIN, again printed on thermal paper. The voter proceeds to any open voting terminal, enters the PIN, and is given the proper ballot style. The ballot summary is printed, and deposited into the ballot box (right).

registration system, via cellular modem, notifies a centralized database of the voter's change in status, to eliminate any risk of double-voting.

The registration system will use a thermal label printer to generate a sticker with the voter's name, precinct and ballot style indicated. The precinct and ballot style are also indicated with a 1-D barcode. This sticker goes into a poll book which the voter signs, providing a backup to the online database. The barcode can also be read by an off-the-shelf scanner connected to the controller. This represents the only data flow from the outside world into the internal voting network, and helps avoid data entry errors that might come from human transcription. Nothing in the barcode is secret nor is it unique to the voter. Consequently, the flow of this information does not compromise the voter's privacy, so long as the voter is not the only voter with the same precinct and ballot style to vote at that polling location.

Provisional voters will be indicated with a suitable prefix to their precinct code, allowing the voting system to suitably distinguish their ballots from regular ones. (Provisional votes are cast by voters who, for whatever reason, do not appear in the voter registration database, and believe this to be in error. They are only tabulated after the voter's registration status is verified, typically not until at least a few days after the end of voting.)

(2) *Controller.* The controller scans the barcode on the sticker to identify the voter's precinct and ballot style. The controller then prints a 5-digit code, unique for the remainder of the election in this polling place. Holding this printout, the voter can then approach any open voting terminal, enter the code, and be presented with the correct ballot style. (There will probably need to be a special alternative for ADA compliance as not all voters can see or handle paper. One possible solution is that a poll worker could enter the relevant code, then depart before the voter begins voting.)

There are only ever a small number of 5-digit codes active at any one time, reducing the odds of a voter successfully guessing an active code and casting multiple ballots. We note that there will be no record binding the 5-digit code to the voter, helping ensure voter anonymity. We also note that these codes reduce the attack surface, relative to other voting systems that use smartcards or other active electronic devices to initialize a voting machine for each voter.

(3) *Voting terminals.* The voter makes selections with the GUI (for sighted voters) or auditory UI (for non-sighted voters). There is a review screen (or the auditory equivalent) so that the voter can confirm all selections before producing a paper record.

(4) *Print.* When the voter has finished making selections, the voting terminal prints two (possibly joined) items: (1) a paper ballot which includes a human-readable summary of the voter's selections and a random (non-sequential) serial number, and (2) a take-home receipt that identifies the voting terminal used, the time of the vote, and a short (16-20 character) hash code that serves as a commitment to the vote but does not reveal its contents.[2] The voting terminal also sends

[2] A secondary hash code with as many as 16-20 additional characters may be included for additional assurance.

data about the vote and receipt to the judge's station. (See Section 6 for the exact cryptographic design.)

(5) *Review printed record.* The voter may then review the printed record to confirm the indicated selections. There will be at least one offline station available that can scan the paper record and read it back to the voter for those who cannot visually read the paper record.

(6) *Option: Cast or challenge/spoil.* After reviewing the ballot, the voter has a choice: Cast the ballot or spoil it. A voter might spoil the ballot because of an error (or change of heart) or because the voter wishes to challenge the voting terminal, demanding it to show that the voter's selections were correctly recorded and committed to. This process represents a novel variant on Benaloh challenges [Benaloh 2006; 2007]; rather than asking the voter a "cast or challenge" question, the voter either deposits the ballot in the box or not. This represents a potentially significant usability gain over prior variants of the Benaloh challenge.

The two procedures are described below. Note also that there is a special procedure for provisional ballots.

Regardless, the voter may keep the take-home paper receipt. We note that most thermal printers include a cutting device that leaves a small paper connection between the two sides of the cut. It is therefore a simple matter for the voting terminal to print a single sheet that the voter can easily separate into the ballot summary and the take-home receipt. We also note that "privacy sleeves" (i.e., simple paper folders) can protect the privacy of these printed ballots as voters carry them from the voting machine either to the ballot box to be cast, or to the judge's station to be spoiled.

(a) *Ballot box: cast ballot.* A voter who wishes to cast the ballot takes the paper ballot summary to the ballot box. The ballot box has a simple scanner that can read the serial number from the ballot (the serial number might also be represented as a one-dimensional barcode for reliability) and communicate this to the controller, allowing the controller to keep a record of which ballots have found their way to the ballot box, and thus, which ballots should be tabulated. *An electronic ballot record is not considered complete and should not be included in the tally unless and until its corresponding paper ballot summary has been deposited in the ballot box.*

(b) *Spoil ballot.* If the paper record is to be spoiled, the voter returns to a poll worker. The ballot serial number is scanned so that the controller can record that the ballot is to be spoiled. This informs the controller that the corresponding encrypted ballot record should not be included in contest results. Instead, it should be decrypted and published as such after the election is over. The original printed paper ballot thus corresponds to a *commitment* by the voting machine, before it ever "knew" it might be challenged. If the voting machine cannot produce a suitable proof that the ballot encryption matches the plaintext, then it has been caught cheating. Voters who don't care about verification can simply restart the process. For voters who may feel uncomfortable with this process, as it might reveal their intent to a poll worker, we note that voters could deliberately spoil ballots that misstate their true intent. We note that dedicated election monitors could be allowed to use voting machines, producing printed ballots that they would be forbidden from placing in the ballot box, but which would be spoiled and then the corresponding ciphertext would be decrypted. In effect, election monitors can conduct *parallel testing in the field* on any voting machine at any time during the live election.

(c) *Provisional ballot.* In the case of a provisional ballot, the voter must return the printed ballot to a poll worker. The voter can choose to spoil the ballot and re-vote or to cast the ballot provisionally by having it placed—under an identifying seal—into a distinct provisional ballot box. The voter may retain the receipt to see if the ballot ends up being counted. Because the ballot box is connected to the controller over the LAN, it can also query the controller as to whether the ballot is provisional. In the event that a voter accidentally puts a provisional ballot into the ballot box, the scanner can detect this and reject the printed ballot. (Provisional ballots need to go into dedicated envelopes that are processed after the voting has ended.)

(7) *At home (optional): Voter checks crypto.* The encrypted votes will be posted on a public "bulletin board" (i.e., a web site maintained by the county). The voter receipt corresponds to a cryptographic hash of the encrypted vote. A voter should be able to easily verify that this vote is present on the bulletin board. If a voter spoiled a ballot, that should also be visible on the bulletin board together with its decrypted selections. This allows independent observers to know which ballots to include in the tally and allows independent verifiers to check that all spoiled ballots are correctly decrypted. Individual voters can check, without any mathematics, that the decryptions of their own spoiled ballots match their expectations.

While this process is more cumbersome than a traditional DRE voting system, it has several advantages. By having the paper elements, this system not only benefits from sophisticated end-to-end cryptographic techniques (described in Section 6), it also can be audited post-election, by hand, using a risk-limiting audit (see Section 5). Voters also have the confidence that comes from holding, verifying, and casting a tangible record of their votes, whether or not they trust the computers.

3. DESIGN

From the perspective of voters, the process of registration and poll-station sign-in is unchanged from current practice. Once authorized, voters proceed to a voting terminal where they use a rich interface that prevents overvotes, warns of undervotes, and supports alternative input/output media for disabled and impaired voters. The printed ballot summary and the corresponding electronic ballot record both include a variety of cryptographic features, which we now describe.

3.1. Crypto Overview

From the perspective of election officials, the first new element in the election regimen is to generate the cryptographic keys. A set of election trustees is designated as key holders and a threshold number is fixed. The functional effect is that if there are n election trustees and the threshold value is k, then any k of the n trustees can complete the election, even if the remaining $n-k$ are unavailable. This threshold mechanism provides robustness while preventing any fewer than k of the trustees from performing election functions that might compromise voter privacy. Threshold cryptosystems are straightforward extensions of traditional public-key cryptosystems [Desmedt and Frankel 1989].

The trustees each generate a key pair consisting of a private key and a public key; they publish their public keys. A standard public procedure is then used to compute a single public key from the n trustee public keys such that decryptions can be performed by any k of the trustees. This single election public key K is published and provided to all voting terminals together with all necessary ballot style information to be used in the election. A start value z_0, which is unpredictable and unique to the election, is also chosen and distributed to each voting terminal for reasons discussed below.

During the election, voters use voting terminals to make their selections. Once selections are completed, the voting terminal produces paper printouts of two items. The first is the paper ballot summary which consists of the selections made by the voter and also includes a random (non-sequential) serial number. The second is a receipt that consists of an identification number for the voting terminal, the date and time of the vote, and a short hash of the encryption of the voter's selections together with the previous hash value. Specifically, if the voter's selections are denoted by v, the ith hash value produced by a particular voting terminal m in an election is computed as

$$z_i = H(E_K(v), m, z_{i-1})$$

where H denotes the hash function and E denotes encryption. This separation of the ballots into two parts makes sure that the ballot summary does not contain any voter-related information, while the take-home receipt does not leak any information about the voter choices. Furthermore, since we only store votes in an encrypted form, and since the decryption keys are kept out of the system, there is no problem with storing the votes with timestamps: they could only allow linking a voter to a ciphertext that will never be decrypted, which is harmless.

The voting terminal should retain both the encrypted ballots and the current hash value. At the conclusion of the election (if not sooner), the encrypted ballots should be posted on a publicly-accessible web page and digitally signed by the election office using a simple signature key (not the key generated by the trustees). The posting of each encrypted ballot should also include a non-interactive zero-knowledge (NIZK) proof that the ballot is well-formed. Once they receive their ballot summaries and take-home receipts, voters may either deposit their ballot summaries into a ballot box or take them to a poll-worker and have them spoiled. Ballot summaries deposited in a ballot box have their serial numbers scanned and recorded. The electronically stored encrypted vote is not considered complete (and not included in the tally) unless and until its corresponding serial number has been recorded in the ballot box.

Any electronically stored encrypted ballots for which no corresponding serial number has been scanned and recorded are deemed spoiled. The published election record should include all spoiled ballots as well as all cast ballots, but for each spoiled ballot the published record should also include a verifiable decryption of the ballot's contents. Voters should be able to easily look up digitally-signed records for any receipts they hold and verify their presence and, for spoiled receipts, the ballot contents.

A voter who takes a completed paper ballot summary to a poll worker can request that the poll worker spoil the ballot and give the voter an opportunity to re-vote. The poll worker marks both the take-home receipt and the paper ballot summary as spoiled (including removing or marking the serial number so that it will not be recorded if subsequently placed in the ballot box) and returns the spoiled ballot summary to the voter.

Upon completion of the election, the election office homomorphically combines the cast ballots into an aggregate encryption of the election tally (this can be as simple as a multiplication of the public encrypted ballots). At least k of the election trustees then each perform their share of the decryption of the aggregate as well as individual decryptions of each of the spoiled ballots. The trustees also post data necessary to allow observers to verify the accuracy of the decryptions.

A privacy-preserving risk-limiting audit is then performed by randomly selecting paper ballot summaries and matching each selected ballot with a corresponding encrypted ballot to demonstrate the correct matching and provide software-independent evidence of the outcome [Rivest and Wack 2006; Lindeman and Stark 2012; Stark and Wagner 2012].

3.2. Triple Assurance

Three lines of evidence are produced to support each election outcome [Stark and Wagner 2012]. The homomorphic tallying process proves that the announced tally corresponds to the posted encrypted ballot records. The ballot challenge and receipt checking processes allow voters to check that these encrypted ballot records correctly reflect their selections. The risk-limiting audit process serves to verify the correspondence between the paper records and the electronic records. In addition, the paper records remain available in case of systemic failure of the electronic records or if a manual count is ever desired. The paper and electronic records are conveyed to the local election office separately, providing additional physical security of the redundant audit trail.

The design of the election system ensures that all three of these checks should be perfectly consistent. There is sufficient information in the records so that if any discrepancies arise (for instance because of loss of some of the electronic or paper records), the discrepancies can be isolated to individual ballots that are mismatched or counted differently.

Why combine e2e with risk-limiting auditing? Each provides different guarantees and they support each other's strengths. E2e techniques, for example, provide cryptographically strong evidence that a voter's receipt corresponds to a ballot, on the bulletin board, which has been included correctly in the final tally—a guarantee that risk-limiting audits alone cannot accomplish. However, if there's a discrepancy, e2e techniques cannot necessarily identify where things went wrong. Risk-limiting audits provide a backstop to prevent cryptographic failures from ruining the election outcome. They also provide a secondary check against machines that might be producing paper and electronic records that disagree, even if voters aren't bothering to conduct e2e challenge audits.

3.3. Software and Hardware Engineering

An important criteria for STAR-Vote is that it should leverage commodity components whenever feasible. This reduces cost and simplifies the ability for an election administrator to replace aging hardware by sourcing it from multiple vendors. While this paper isn't intended to cover certification issues, the separation of hardware and software allows for the possibility of *commercial off-the-shelf* (COTS) hardware, which *could* be subject to a lower bar for certification than the software.

Ideally, the voting terminals and the judge station could use identical hardware. In particular, we believe that a reasonable target might be "point of sale" terminals. These are used in restaurants worldwide. They are used in relatively demanding environments and, on the inside, are ordinary PCs, sometimes built from low-power laptop-class parts. The only missing hardware from a COTS point of sale terminal, relative to our needs for STAR-Vote, are a printer and a battery.

If you want a reliable, low-power printer, without having to worry about consumable ink or toner, there's only one choice: thermal printers. They come in a variety of widths, up to US Letter size. Thermal paper, particularly higher cost thermal paper, can last for years in an air-conditioned warehouse, although some experimentation would be required to see whether it can survive an un-air-conditioned trip in a hot car in the summer. Every shipping label from major online vendors like Amazon is printed thermally, lending some credence to its survivability in tough conditions.

Specifying a battery is more complicated. We could require that the voting terminal have an internal (and removable) battery, but this eliminates COTS point of sale terminals. Tablet computers come with built-in batteries that, at least in some cases, can last all day. Tablet computers have smaller screens than we might prefer, but they don't have hardware Ethernet ports or enough USB ports to support accessibility devices and printers[3]. Also, we would prefer to use wired networks, rather than the wireless networks built into most tablets. We note that a number of vendors are now releasing touchscreen-enabled laptops and larger touchscreen desktop models to support Windows 8. This new hardware is likely to provide good options for running STAR.

For the software layer, we see no need for anything other than a commodity operating system, like Linux, which can be stripped of unessential features to reduce the attack surface. For example, we don't need a full-blown window system or 3D graphics pipeline. All we need are basic pre-rendered ballots, as in pVote [Yee et al. 2006; Yee 2007] or VoteBox [Sandler et al. 2008]. We would specify that the voting system software be engineered in a type-safe language like Java or C# (eliminating buffer overflow vulnerabilities, among other problems) and we would also specify that the software be engineered with *privilege separation* [Provos et al. 2003], running separate parts of the voting software as distinct applications, with distinct Unix user-ids, and with suitably reduced privileges. For example, the storage subsystem can maintain append-only storage for ballots. The voter-facing UI would then have no direct access to ballot storage, or the network, and could be "rebooted" for every voter. Consequently, a software compromise that impacts the UI application could impact at most one voter. A tablet that includes a Trusted Platform Module (TPM) can provide additional assurance that the correct software — and only the correct software — is running on the device.

A separation architecture like this also provides some degree of protection over sensitive cryptographic key materials, e.g., if we want every voting terminal to have a unique private key to compute digital signatures over ballots, then we must restrict the ability for compromised software to extract the private keys. DStar [Zeldovich et al. 2008], for example, used this technique to protect the key material in an SSL/TLS web server.

4. USABILITY

4.1. Design Considerations

In designing this reference voting system it was important to maximize the usability of the system within the framework of enhanced security and administrative expediency. The overall design of the

[3]While a single USB port can connect to a USB hub, which would then have more expandability, a *powered* USB hub might be necessary to drive some devices like a USB Ethernet adapter, complicating our requirement to keep STAR running even when on battery power.

system was strongly influenced by usability concerns. For example, a proposal was put forth to have all voters electronically review the paper record on a second station; this was rejected on usability grounds. ISO 9241 Part 11 [ISO] specifies the three metrics of usability as effectiveness, efficiency, and satisfaction, and these are the parameters we attempt to maximize in this design. Effectiveness of the system means that users should be able to reliably accomplish their task, as they see it. In voting, this means completing a ballot that correctly records the candidate selections of their choice, whether that be though individual candidate selection by race, straight party voting, or candidate write-ins. Efficiency measures the ability of a voter to complete the task with a minimum of effort, as measured through time on task or number of discrete operations required to complete a task. Efficiency is important because users want to complete the voting task quickly and voting officials are concerned about voter throughput. Reduced efficiency means longer lines for waiting voters, more time in the polling booth, and higher equipment costs for election officials. Satisfaction describes a user's subjective assessment of the overall experience. While satisfaction does not directly impact a voter's ability to cast a vote in the current election, it can have direct impact on their willingness to engage in the process of voting at all, so low satisfaction might disenfranchise voters even if they can cast their ballots effectively and efficiently. How does this design seek to maximize these usability metrics? For voting systems, the system must generally be assumed to be walk-up-and-use. Voting is an infrequent activity for most, so the system must be intuitive enough that little to no instruction is required to use. The system should minimize the cognitive load on voters, so that they can focus on making candidate selections and not on system navigation or operation. The system should also mitigate the kinds of error that humans are known to make, and support the easy identification and simple correction of those errors before the ballot is cast.

Why not paper?. Paper ballots (bubble ballots in particular) have many characteristics that make them highly usable [Everett et al. 2006; Byrne et al. 2007]. Users are familiar with paper, and most have had some experience with bubble-type item selection schemes. Voting for write-in candidates can be relatively simple and intuitive. Unlike electric voting machines, paper is nearly 100% reliable and is immune from issues of power interruption. Further, paper leaves an auditable trail, and wholesale tampering is extremely difficult. However, paper is not a perfect solution. Voters actually show higher satisfaction with electronic voting methods than they do with paper [Everett et al. 2008] and paper has significant weaknesses that computers can overcome more easily. First, the ambiguity that can be caused by partial marks leads to substantial problems in counting, recounting, and re-interpreting paper ballots. Second, voting by individuals with disabilities can be more easily accommodated using electronic voting methods (e.g., screen readers, jelly switches). Third, electronic voting can significantly aid in the reduction of error (e.g. undervotes, overvotes, stray marks) by the user in the voting process. Fourth, electronic voting can more easily support users whose first language is not English, since additional ballots for every possible language request do not have to be printed, distributed and maintained at every polling location. This advantage is also evident in early voting and vote center administration; rather than having to print, transport, secure, and administer every possible ballot for every precinct, the correct ballot can simply be displayed for each voter. Computers also facilitate sophisticated security and cryptography measures that are more difficult to implement in a pure paper format. Finally, administration of the ballots can be easier with electronic formats, since vote counting and transportation of the results are more efficient. We have taken a hybrid approach in this design, by using both paper and electronic voting methods in order to create a voting system that retains the benefits of each medium while minimizing their weaknesses.

Usability vs Security. Usability and security are often at odds with each other. Password design is a perfect example of this tension. A system that requires a user have a 32-character password with upper and lower case letters, digits, and symbols with no identifiable words embedded might be highly secure, but it would have significant usability issues. Further, security might actually be *compromised* since users are likely to write such a difficult password down and leave it in an insecure location (e.g., stuck to the computer monitor). For voting systems, we must strive for maximum usability while not sacrificing the security of the system (our security colleagues might argue that

we need to maximize security while not sacrificing usability). In our implementation, many of the security mechanisms are invisible to the user. Those that are not invisible are designed in such a way that only those users who choose to exercise the enhanced security/verifiability of the voting process are required to navigate additional tasks (e.g., ballot challenge, post-voting verification).

Accessibility vs Security. STAR-Vote makes strategic use of paper to enhance the overall security and auditability of the voting process. From an auditability standpoint, the presence of the paper ballot allows matching of the paper and electronic records and preserves a separate physical copy apart from the electronic tally. From a security standpoint, it allows a voter to verify that the choices selected on the electronic voting terminal (DRE) have been faithfully recorded on the paper ballot (although this voter verification is not a robust as one might hope [Everett 2007]), and challenge their vote if they choose to do so. However, the added benefits provided by the inclusion of paper come at a cost to the accessibility of the system. Visually impaired voters must now be given a way to verify the contents of printed material and be guided in the handling of that paper into the scanners and ballot boxes. Voters with mobility impairments must now handle these paper ballots with moderate dexterity in order to feed them into the scanning ballot boxes as well. Solutions to this tradeoff are still under evaluation. Many obvious solutions, such as giving voters with disabilities the option to simply cast an electronic ballot without a paper record, seriously compromise the overall security and auditability of the voting system, and also present significant privacy concerns, since voters who opt out the main flow might be easily identified. Simple but non-optimal solutions are being considered (test-to-speech scanning stations, ballot privacy sleeves and increased poll worker involvement), but we continue to investigate more elegant solutions that involve automatic paper handling mechanisms. A final design has still not been identified.

Error reduction. The use of computers in combination with paper is anticipated to reduce errors committed by voters. Because voters will fill out the ballot on electronic voting terminals, certain classes of errors are completely eliminated. For example, it will be impossible to over vote or make stray ballot marks, as the interface will preclude the selection of more than a single candidate per race. Under voting will be minimized by employing sequential race presentation, forcing the voter to make a conscious choice to skip a race [Greene 2008]. Undervotes will also be highlighted in color on the review screen, providing further opportunity for users to correct accidental undervotes. This review screen will also employ a novel party identification marker (see below) that will allow a voter to easily discern the party for which they cast a vote in each race. The use of the paper ballot (printed when the voter signals completion) provides the voter with a final chance to review all choices before casting the final ballot.

4.2. User Interface Design Specification

The basic design for the UI is a standard touchscreen DRE with auditory interface for visually impaired voters and support for voter-supplied hardware controls for physical impairments (e.g., jelly switches).

The VVSG. The starting point for UI specifications is the 2012 draft version 1.1 of the Voluntary Voting System Guidelines (VVSG). These guidelines specify many of the critical properties required for a high-quality voting system user interface, from simple visual properties such as font size and display contrast to more subtle properties such as ballot layout. They also require that interfaces meet certain usability benchmarks in terms of error rates and ballot completion time. We believe that no extant commercial voting UI meets these requirements, and that any new system that could meet them would be a marked improvement in terms of usability. That said, there are some additional requirements that we believe should be met.

Accessibility. While the VVSG includes many guidelines regarding accessibility, more recent research aimed at meeting the needs of visually-impaired voters [Piner and Byrne 2011] has produced some additional recommendations that should be followed. These include:

— In order to capitalize on user preference, a synthesized male voice should be used.
— Navigation should allow users to skip through sections of speech that are not important to them as well as allowing them to replay any parts they may have missed or not comprehended the first time.
— At the end of the voting process, a review of the ballot must be included, but should not be required for the voter.

Review Screens. Another area where the VVSG can be augmented concerns review screens. Voter detection of errors (or possible malfeasance) on review screens is poor [Everett 2007], but there is some evidence that UI manipulations can improve detection in some cases [Campbell and Byrne 2009a]. Thus, STAR-Vote requires the following in addition to the requirements listed in the VVSG:

— Full names of contests and candidates should be displayed on the review screen; that is, names should be text-wrapped rather than truncated. Party affiliation should also be displayed.
— Undervotes should be highlighted using an orange-colored background.
— Activating (that is, touching on the visual screen or selecting the relevant option in the auditory interface) should return the voter to the full UI for the selected contest.
— In addition to party affiliation in text form, graphic markings should be used to indicate the state of each race: voted Republican, voted Democratic, voted Green, etc.—with a distinctive graphic for "not voted" as well. These graphic markings should be highly distinguishable from each other so that a rapid visual scan quickly reveals the state of each race, while taking note of potential usability issues with graphics symbols [Smith et al. 2009]. Exact graphic symbols for STAR-Vote have not yet been determined.

Paper Record. The VVSG has few recommendations for the paper record. For usability, the paper record should meet VVSG guidelines for font size and should contain full names for office and candidate. To facilitate scanner-based retabulations, the font should be OCR-friendly. Contest names should be left-justified while candidate names should be right-justified to a margin that allows for printing of the same graphic symbols used in the review screen to facilitate rapid scanning of ballots for anomalies. Candidate names should not be placed on the same line of text as the contest name and a thin horizontal dividing line should appear between each office and the next in order to minimize possible visual confusion.

4.3. Issues that still need to be addressed

There are still several issues that need to be addressed in order to make the system have the highest usability. The first of these is straight party voting (SPV). SPV can be quite difficult for a voter to understand and accomplish without error, particularly if voters intend to cross-vote in one or more races [Campbell and Byrne 2009b]. Both paper and electronic methods suffer from these difficulties, and the optimum method of implementation will require additional research. Races in which voters are required to select more than one candidate (k of n races) also create some unique user difficulties, and solutions to those problems are not yet well understood.

5. AUDIT

The E2E feature of STAR-Vote enables individual voters to confirm that their votes were included in the tabulation, and that the encrypted votes were added correctly. The challenge feature, if used by enough voters, assures that the encryption was honest and that substantially all the votes are included in the tabulation. But there might not be many voters who challenge the system; the voters who do are hardly representative of the voting public; and some problems may go unnoticed. Moreover, the anonymized form of E2E used here does not allow a voter to confirm that *others'* ballots were included in the tabulation, only that those ballots that were included were included correctly.

The paper audit trail enables an entirely independent check that the votes were included and tabulated accurately, that the visible trace of voter intent as reflected in the ballot agrees with the encryption, and, importantly, that the winners reported by the voting system are the winners that a

full hand count of the audit trail would reveal. The key is to perform a compliance audit to ensure that the audit trail of paper ballots is adequately intact to determine the outcomes, and then to perform a risk-limiting audit of the machine interpretation against a manual interpretation of the paper ballots. For the risk-limiting audit, STAR-Vote uses SOBA [Benaloh et al. 2011] with improvements given by [Lindeman and Stark 2012].

A risk-limiting audit guarantees a large minimum chance of a full hand count of the audit trail if the reported outcome (i.e., the set of winners) disagrees with the outcome that the full hand count would reveal. The full hand count then sets the record straight, correcting the outcome before it becomes official. Risk-limiting audits are widely considered best practice for election audits [Lindeman et al. 2008; Bretschneider et al. 2012].

The most efficient risk-limiting audits, ballot-level comparison audits, rely on comparing the machine interpretation of individual ballots (cast vote records or CVRs) against a hand interpretation of the same ballots [Stark 2010; Benaloh et al. 2011; Lindeman and Stark 2012]. Current federally certified voting systems do not report cast vote records, so they cannot be audited using the most efficient techniques [Lindeman and Stark 2012; Stark and Wagner 2012]. This necessitates expensive work-arounds.[4] The preamble to conducting a ballot-level comparison audit using currently deployed voting systems can annihilate the efficiency advantage of ballot-level comparison audits [Stark and Wagner 2012].

A big advantage of STAR-Vote is that it records and stores individual cast vote records in a way that *can* be linked to the paper ballot each purports to represent, through encrypted identifiers of the ballot corresponding to each voter's selections, separately for each contest. This makes ballot-level comparison audits extremely simple and efficient. It also reduces the vulnerability of the audit to human error, such as accidental changes to the order of the physical ballots.[5]

A comparison audit can be thought of as consisting of two parts: Checking the addition of the data,[6] and randomly spot-checking the accuracy of the data added, to confirm that they are accurate enough for their tabulation to give the correct electoral outcome. The data are the votes as reported by the voting system. For the audit to be meaningful, the election official must commit to the vote data before the spot-checking begins. Moreover, for the public to verify readily that the reported votes sum to the reported contest totals, it helps to publish the individual reported votes. However, if these votes were published ballot by ballot, pattern voting could be used to signal voter identity, opening a communication channel that might enable widespread wholesale coercion [Rescorla 2009; Benaloh et al. 2011].

The SOBA risk-limiting protocol [Benaloh et al. 2011] solves both of these problems: It allows the election official to commit cryptographically and publicly to the vote data; it publishes the vote data in plain text but "unbundled" into separate contests so that pattern voting cannot be used to signal. Moreover, the computations that SOBA requires are extremely simple (they are simplified even further by [Lindeman and Stark 2012]). The simplicity increases transparency, because observers can confirm that the calculations were done correctly with a pencil and paper or a hand calculator.

The encrypted ballot/contest identifiers on the ballot that STAR-Vote produces allow the electronic cast vote records for each contest to be linked to the paper they purport to represent. This simplifies SOBA procedures because it eliminates the need to store ballots in a rigid order. Moreover, because the voting terminal generates both the electronic vote data and the paper ballot, the audit should find very few if any discrepancies between them.

---

[4]For instance, a *transitive audit* might require marking the ballots with unique identifiers or keeping them in a prescribed order, re-scanning all the ballots to make digital images, and processing those images with software that can construct CVRs from the images and associate the CVRs with the ballots. That software in turn needs to be programmed with the all the ballot definitions in the contest, which itself entails a great deal of error-prone handwork.

[5]For instance, we have seen groups of ballots dropped on the floor accidentally; even though none was lost, restoring them to their original order was impossible.

[6]This presupposes that the contest under audit is a plurality, majority, super-majority, or vote-for-k contest. The operation that must be checked to audit an instant-runoff contest is not addition, but the same principle applies.

But since voters and election workers will handle the ballots in transit from the voting terminal to the scanner to the audit, voters might make marks on their ballots. Depending on the rules in place for ascertaining voter intent from the ballot, those marks might be interpreted as expressing voter intent different from the machine-printed selections, in which case the SOBA audit might find discrepancies.

It could also happen that a ballot enters the ballot box but its serial number is not picked up, so the electronic vote data ends up in the "untallied but unspoiled" group. This should be detectable by a compliance audit [Benaloh et al. 2011; Lindeman and Stark 2012; Stark and Wagner 2012] as a mismatch between the number of recorded votes and the number of pieces of paper, providing an opportunity to resolve the problem before the audit begins.

If such cases remain and turn up in the audit sample, SOBA would count them as discrepancies and the sample might need to expand, either until there is strong evidence that the electoral outcomes are correct despite any errors the audit uncovers, or until there has been a complete hand count.

The random selection of ballots for the SOBA audit should involve public participation in generating many bits of entropy to seed a high-quality, public, pseudo-random number generator (PRNG), which is then used to select a sequence of ballots to inspect manually [Lindeman and Stark 2012]. (For instance, audit observers might roll 10-sided dice repeatedly to generate a 20-digit number.) Publishing the PRNG algorithm adds transparency by allowing observers to verify that the selection of ballots was fair.

6. THE CRYPTOGRAPHIC WORKFLOW

The core elements. At its core, the cryptographic workflow of STAR-Vote follows the approach of Cramer, Gennaro and Schoenmakers [Cramer et al. 1997], also used in Helios [Adida et al. 2009] and VoteBox[Sandler et al. 2008], among others. Cryptographic analyzes of this approach can be found in [Bernhard et al. 2012; Cortier et al. 2013]. We then augment this approach in various ways in order to ease the detection of and recovery from potential problem.

STAR-Vote keeps an electronic record of all the votes encrypted with a threshold cryptosystem (so that decryption capabilities are distributed to protect voter privacy) that has an additive homomorphic property (to allow individual encrypted ballots to be combined into an aggregate encryption of the tally). The common exponential version of the Elgamal cryptosystem [ElGamal 1985] satisfies the required properties, and stronger security is obtained by using PPATS encryption [Cuvelier et al. 2013], in particular against key manipulation errors by the trustees and long-term security. The encryption scheme comes with an extraction function Ext that, from a ciphertext, extracts a commitment on the encrypted value. In the case of Elgamal, this commitment is be the ciphertext itself, while in the case of PPATS, it is a perfectly hiding homomorphic commitment.

Cryptographic key generation can be accomplished in one of two ways, depending on the availability of the election trustees and the desired amount of robustness. The preferred process offers general threshold key generation requires multiple rounds (see [Gennaro et al. 2007] for Elgamal and PPATS), but can be simplified into a single-round solution if redundancy is eliminated (as in Helios for instance [Adida et al. 2009]). At the end of the key generation procedure, the trustees each hold a private key share that does not contain any information on the full private key, and the unique public key K corresponding to those shares is published.

During the polling phase, the ballot marking devices encrypt the votes of each voter using the public key K. This encryption procedure is randomized in order to make sure that two votes for the same candidates result in ciphertexts that look independent to any observer.

Following Benaloh [Benaloh 2006], a cryptographic hash value of the commitment extracted from each ciphertext (and of a few more data, as discussed below) is also computed, fingerprinting the ballot to a 256 bit string. An abridged form of which is provided to the voter in a human readable form as part of the take-home receipt. All the hashes and commitments are computed and posted on a publicly accessible web page, as soon as the polls are closed. This web page is digitally signed by the election office using a traditional signature key (as performed by [Adida et al. 2009]). This signature operation makes it infeasible to consistently modify the content of the web page without

the help of the signer, and provides evidence against a malicious signer who would try to sign various versions of the bulletin board.

The posting of all the hashes gives all voters the ability to verify that their ballots have been recorded properly. The commitments can also be checked for consistency with the hashes and used to confirm the homomorphic aggregation of the individual ballots into a single encryption of the sum of the ballots, which constitutes an encryption of the election tallies.

At the end of the election, any set of trustees that achieve the pre-set quorum threshold use their respective private keys to decrypt the derived aggregate tally encryption. This procedure is simple and efficient and can be completed locally without interaction between the trustees. We note that the individual encrypted ballots, from which the aggregate encryption of the tallies is formed, are never individually decrypted. However, each spoiled ballot *is* individually decrypted using exactly the same process that is used to decrypt the aggregate tally encryption.

The elements we just described make the core of the workflow and are sufficient to compute an election tally while preserving the privacy of the votes. We now explain various ways in which this simple workflow is hardened in order to make sure that the tally is also correct. All the techniques that follow enable the verification of different aspects of the ballot preparation and casting.

Hardening encryption. Since the tally does not involve the decryption of any individual ballot, and since the audit procedure relies on the fact that all counted ballots are properly formed, it is crucial to make sure that all the encrypted ballots that are added correspond to valid votes [Benaloh and Fischer 1985]. This is achieved by requiring the ballot marking devices to compute, together with the encryption of the votes, a non-interactive zero-knowledge (NIZK) proof that each ballot is well-formed. Such a proof guarantees that each ciphertext encrypts a valid vote and does not leak any other information about the content of the vote. As a side benefit, this proof can be designed to make the ballots non-malleable, which provides an easy technique to prevent the replay of old ballots (i.e., reject duplicates). Traditional sigma proofs provide the required security properties and are described and analyzed in [Bernhard et al. 2012].

We note that, if malicious software were to get into the voting system, it could use the randomness inherent in the encryption process to encode a subliminal message to an external observer. This sort of threat, along with the threat of a malicious voting machine that simply records every vote cast, in plaintext, in internal memory, is something that cryptography cannot address. (More discussion on this appears in Section 3.3.)

Hardening decryption. Making sure that the encrypted ballots are valid is not enough: we also need to make sure that the tally is correctly decrypted as a function of those encrypted ballots: otherwise, malicious trustees (or trustees using corrupted devices) could publish an outcome that does not correspond to these ballots. As a result, we require the trustees to provide evidence of the correctness of the decryption operations that they perform. This can also be accomplished with sigma proofs in the case of Elgamal or more simply by publishing commitment openings in the case of PPATS.

Hardening the timeline. The procedures described above prevent malfunctioning or corrupted voting terminals or trustees to falsify individual ballots or decryption operations.

The detection of manipulation of encrypted ballots can be more effective by linking ballots with each other, using hash chaining [Sandler and Wallach 2007; Benaloh and Lazarus 2011]. For this purpose, each ballot marking device is seeded, at the beginning of the election, with a public start value z_0 that includes a unique identifier for the election. This unique identifier is chosen at random shortly before the election, either in a central way or by the poll workers themselves at the beginning of election day.

From this seed, all election events are chain hashed, with z_{i+1} being computed as a hash of z_i concatenated to the id of the machine on which the event happens and to the event content. Two such chains are maintained and properly separated. One is internal and contains the full election data, including the encryption of the votes, the casting time of each paper ballot, and information

on machines being added or removed. The second is public and chains the commitment extracted from all encrypted votes, together with time and identifiers for the election and voting machine. The public hash is the one actually printed on the take-home receipt. When the polls close, the final value of the hash chains are digitally signed, and the public chain is made public together with all the information needed for its reconstruction.

As a result of this procedure, any removed ballot will invalidate the hash chain which is committed to at the close of the election and whose constituents appear on the voter take-home receipts.

Hardening the link between the paper and electronic election outcome. As described in Section 5, STAR-Vote includes a risk limiting audit (RLA) based on the human-readable versions of each ballot summary printed by the voting terminals and inspected for correctness by voters. This RLA comes in addition to the cast or challenge procedure discussed above, and the production of the inputs for the RLA is an original contribution of STAR-Vote.

The requirement for running the RLA is to commit on a full electronic record including a 1-to-1 mapping and evidence that this electronic record leads to the announced outcome. This is achieved as follows.

(1) For each ballot, the ballot marking device selects a random ballot id sequence number *bid*. This *bid* is printed on the ballots as a barcode. Furthermore, for each race r to which the voter participates, an encryption of $H(bid\|r)$ is also computed and appended to the encryption of the choices.
(2) At the end of the day, and before decryption of the tallies, the trustees (or their delegates) shuffle and rerandomize all encrypted votes, race by race. This shuffle does not need to be verifiable, even though a verifiable shuffle would improve accountability by making it possible to verify that the shufflers did not cheat if it happens that a discrepancy is detected during the RLA. However, in the case of a non verifiable shuffle, the shufflers must save their permutation and randomness until the end of the election audit. The non-verifiable solution is preferred for its simplicity (verifiable shuffles are particularly challenging to implement properly) and for its efficiency (permutations and reencryption factors can be precomputed, leaving only one multiplication to perform per ciphertext in the online phase, which is convenient when millions of ciphertexts have to be shuffled).
(3) When the trustees decrypt the homomorphically added votes, they also decrypt the output of this shuffle. For each race, this provides a list of elements of the form $H(bid\|r)$ and the corresponding cleartext choices.
(4) Now, auditors can sample the paper ballots, read the *bid* printed on them, recompute the value of $H(bid\|r)$ for all races present on the paper ballot, and compare to the electronic record (as well as check many other things, as prescribed for the risk-limiting audit).

The use of hashed *bid*'s has the important benefit of making sure that someone who does not know a *bid* value cannot, by looking at the electronic record, link the selections made for the different races on a single ballot, which protects from pattern voting attacks. There is no need for such a protection from someone who can access the paper ballots, since that person can already link all races just by looking at the paper.

The full cryptographic protocol. The resulting cryptographic workflow is as follows.

(1) The trustees jointly generate a threshold public key/private key encryption pair. The encryption key K is published.
(2) Each voting terminal is initialized with the ballot and election parameters, the public key K and seeds z_0^p and z_0^i that are computed by hashing all election parameters and a public random salt z_0.
(3) When a voter completes the ballot marking process selection to produce a ballot v, the voting terminal performs the following operations:
    (a) It selects a unique and unpredictable ballot identifier *bid*, as well as a unique (but possibly predictable) ballot casting identifier *bcid*.

(b) It computes an encryption $c_v = E_K(v)$ of the vote, as well as a NIZK proof p_v that c_v is an encryption of a valid ballot. This proof is written in such a way that it can be verified from $Ext(c_v)$ only.
(c) For each race $r_1, \ldots, r_n$ to which the voter takes part, it computes an encryption $c_{bid} = E_K(bid\|r_1)\|\cdots\|E_K(bid\|r_n)$.
(d) It computes a public hash code $z_i^p = H(bcid\|Ext(c_v)\|p_v\|m\|z_{i-1}^p)$, where m is the voting terminal unique identifier, as well as an internal hash $z_i^i = H(bcid\|c_v\|p_v\|c_{bid}\|\|m\|z_{i-1}^i)$
(e) It prints a paper ballot in two parts. The first contains v in a human readable format as well as c_{bid} and $bcid$ in a robust machine readable format (e.g., as barcodes). The second is a voter take-home receipt that includes, the voting terminal identifier m, the date and time, and the hash code z_i^p (or a truncation thereof), all in a human-readable format.
(f) It transmits $(bcid, c_v, p_v, c_{bid}, m, z_i^p, z_i^i)$ to the judge's station.

(4) When a ballot is cast, the ballot casting id $bcid$ is scanned and sent to the judge's station. The judge's station then marks the associated ballot as cast and ready to be included in the tally. This information is also broadcast and added in the two hash chains.
(5) When the polls are closed, the tally is computed: the product of all cast encrypted votes is computed and verifiably decrypted, providing an election result.
(6) The data needed for the risk limiting audit is computed, as described above.

All the data included in the public hash chain are eventually digitally signed and published by the local authority. Those audit data are considered to be valid if the hash chain checks, if all cryptographic proofs check, that is, if the ballot validity proofs check, if the homomorphic aggregation of the committed votes is computed and opened correctly, and if all spoiled ballots are decrypted correctly.

Write-in votes. So far, we have not described how our cryptographic construction can support write-in voting. Support for write-in votes is required in many states. To be general-purpose, STAR-Vote adopts the vector-ballot approach [Kiayias and Yung 2004], wherein there is a separate homomorphic counter for the write-in slot plus an encryption of the string in the write-in. If there are enough write-in votes to influence the election outcome, then the write-in slots, across the whole election, will be mixed and tallied (together with the corresponding counters).

We note that, at least for elections in our state, write-in candidates must be registered in advance. It's conceivable that we could simply allocate a separate homomorphic counter for each registered candidate and have the STAR-Vote terminal help the voter select the desired "write-in" candidate. Such an approach could have significant usability benefits but is expected to require some update of regulations.

7. THREATS

To evaluate the design and engineering of STAR-Vote, it's helpful to have a threat model in mind. The obvious place to start would be VoteBox [Sandler et al. 2008], which is closely related to STAR-Vote. The original VoteBox authors did not state a concise threat model, but considered several kinds of threats and security design goals:

Software independence. STAR-Vote, like VoteBox, should be able to produce a proof of the correctness of an election that does not require any statement about the correctness of the software used in STAR-Vote. VoteBox achieved this through end-to-end cryptographic means. STAR-Vote uses similar cryptography and adds a risk-limiting audit that can verify the correspondence between STAR-Vote printed ballot records and their electronic counterparts, adding a degree of flexibility if the cryptography cannot prove an exact correspondence to determine exactly what went wrong.

Reduced trusted computing base. STAR-Vote, like VoteBox or any other software artifact, would benefit from having simpler code and less of it. This makes it easier to verify and less likely to have bugs. Software independence means that STAR-Vote's software is not required for *cor-*

rectness of the election outcome, but it does help defeat attacks which could disable the system, destroy records, or otherwise cause grief to election officials running STAR-Vote. VoteBox specifies that it uses pre-rendered user interfaces [Yee 2007; Yee et al. 2006]. STAR-Vote should probably use this technique as well.

Robustness against data loss. STAR-Vote, like VoteBox, specifies that vote records be stored on every voting terminal in the local polling place, using tamper-evident logging techniques. STAR-Vote adds a printed ballot record, stored in a ballot box. VoteBox went a step further by considering the real-time one-way transfer of vote records out of the polling place, across the Internet, to a central election headquarters. While STAR-Vote could add this in the future, it's not part of the initial design.

Mega attacks. In the VoteBox paper, the authors considered a variety of attacks with highly capable attackers. Such attackers might run a concurrent election on parallel equipment, in an attempt to substitute the results for genuine votes. Other attackers might mount a "booth capture" attack, wherein armed gunmen take over a polling place and cast votes as fast as possible until the police arrive. These attacks, needless to say, are well within the ability of STAR-Vote's cryptographic and risk-limiting infrastructure to detect. The best such attackers can hope to do is, in effect, mount a denial of service attack against the election. Attackers with that as their goal can arrive at much simpler approaches and STAR-Vote has relatively little it can offer beyond any other election system in this regard.

A full consideration of threats to STAR-Vote and their corresponding countermeasures or mitigations would be far too long to fit in this paper. Instead, we focus on several areas where STAR-Vote differs from other e2e voting systems in the literature.

7.1. Coercion

In designing STAR-Vote, we made several explicit decisions regarding how much to complicate the protocol and impede the voter experience in order to mitigate known coercion threats. Specifically, one known threat is that a voter is instructed to create a ballot in a particular way but to then execute a decision to cast or spoil the ballot according to some stimulus received after the ballot has been completed and the receipt has been generated. The stimulus could come, for example, from subtle motions by a coercer in the poll site, the vibration of a cell phone in silent mode, or some of the (unpredictable) data that is printed on the voter's receipt. Some prior protocols have required that the receipt, although committed to by the voting device, not be visible to the voter until after a cast or spoil decision has been made (perhaps by printing the receipt face down behind a glass barrier) and configuring poll sites so that voters cannot see or be seen by members of the public until after they have completed all steps. We could insist on similar measures here, but in an era where cell phones with video recording capabilities are ubiquitous and eyeglasses with embedded video cameras can easily be purchased, it seems unwise to *require* elaborate measures which mitigate some coercion threats but leave others unaddressed.

7.1.1. Chain voting. A similar threat of "chain voting" is possible with this system wherein a voter early in the day is instructed to neither cast nor spoil a ballot but to instead leave the poll site with a printed ballot completed in a specified way. This completed ballot is delivered to a coercer who will then give this ballot to the next voter with instructions to cast the ballot and return with a new printed ballot—again completed as specified. Chain voting can be mitigated by instituting timeouts which automatically spoil ballots that have not been cast within a fixed period after having been printed. We also expect to have procedures in place to prevent voters from accidentally leaving poll sites with printed ballots. We note that the timeout period need only cover the time we expect will be required for a voter to cross the room with a printed ballot and place it in the box, allowing for a relatively tight time bound, probably less than 5 minutes, although we'd need to run this in practice to understand the distribution of times that might happen in the real world.

(We note that traditional paper ballots sometimes include a perforated header section which includes a serial number. A poll worker keeps one copy of this number and verifies that the ballot a

voter wishes to cast matches the expected serial number. If so, the serial number is then detached from the ballot and deposited in the box. STAR-Vote could support this, but we believe it would damage STAR-Vote's usability. The timeout mechanism seems like an adequate mitigation.)

We do, however, take measures to prevent wholesale coercion attacks such as those that may be enabled by pattern voting. For instance, The SOBA audit process is explicitly designed to prevent pattern-voting attacks; and the high assurances in the accuracy of the tally are acheived without ever publishing the full set of raw ballots.

An interesting concern is that our paper ballots have data on them to connect them to electronic ballot records from the voting terminals and judge's console. The very data that links a paper ballot to an electronic, encrypted ballot creates a potential vulnerability. Since some individual paper ballot summaries will be selected for post-election audit and made public at that time, we are careful to not include any data on the voter's take-home receipt which can be associated with the corresonding paper ballot summary.

7.1.2. Absentee and provisional ballots. There are several methods available for incorporating ballots which are not cast within the STAR-Vote system, such as absentee and provisional ballots. The simplest approach is to completely segregate votes and tallies, but this has several disadvantages, including a reduction in voter privacy and much lower assurance of the accuracy of the combined tally.

It may be possible to eliminate all "external" votes by providing electronic means for capturing provisional and remote ballots. However, for the initial design of the STAR-Vote system, we have chosen to avoid this complexity. Instead, we ask that voting officials receive external votes and enter them into the STAR-Vote system as a proxy for voters. While this still does not allow remote voters to audit their own ballots, the privacy-preserving risk-limiting audit step is still able to detect any substantive deviations between the paper records of external voters and their electronically recorded ballots. This provides more supporting evidence of the veracity of the outcome without reducing voter privacy.

7.2. Further analysis

If we wished to conduct a more in-depth threat modeling exercise, one place to begin would be the threat model developed by the California Top To Bottom Review's source code audit teams (see, e.g., [Inguva et al. 2007]). They considered different levels of attacker access, ranging from voters to election officials. They also considered different attacker motives (disrupt elections, steal votes, coerce voters) and different attack outcomes (detectable vs. undetectable, recoverable vs. unrecoverable, prevention vs. detection, wholesale vs. retail, and casual vs. sophisticated). A complete consideration of STAR-Vote against all these criteria would take far more space than is available in this venue. Instead, we now focus on where STAR-Vote advances the state of the art in these areas.

Most notably, STAR-Vote's combination of end-to-end cryptography with risk-limiting audits of paper ballots is a game changer, in terms of thwarting attackers who might want to disrupt elections. Unlike paperless systems, STAR-Vote has the ability to fall back to the paper records, with efficient processes to detect when inconsistencies exist that would require this. This radically improves STAR-Vote's recoverability from extreme failures.

Similarly, while STAR-Vote is "software independent," we must concern ourselves with software tampering that does not change any of the cryptographic computations, but instead causes the STAR-Vote machines to silently record everything the voter does. This threat cannot be mitigated by better cryptography or ballot auditing. The only likely solution is some sort of trusted platform management (TPM), where the hardware will refused to run third-party code (more discussion on this appears in Section 3.3).

Lastly, we consider a threat that only arises in e2e systems: presentation of a fraudulent voting receipt. Consider the case where a voter may spoil her ballot and take it home to verify against the public bulletin board. A malicious voter with access to similar printers could produce a seemingly legitimate ballot for which there is no correspondence on the public bulletin board, thus "proving"

that the election system lost a record. Similar defaming attacks could be made by forging the receipt that a voter can take home after casting a ballot. For STAR-Vote, we have considered a number of mitigations against these attacks, ranging from cryptographic (having the voting terminals compute a digital signature, with protected key material) to procedural (e.g., watermarking the paper or having poll workers physically sign spoiled ballots). Real STAR-Vote deployments will inevitably use one or more of these mitigations.

8. CONCLUSIONS AND FUTURE WORK

In many ways, STAR-Vote is a straightforward evolution from existing commercial voting systems, like the Hart InterCivic eSlate, mixing in advanced cryptography, software engineering, usability, and auditing techniques from the research literature in a way that will go largely unnoticed by most voters, but that have huge impact on the reliability, accuracy, fraud-resistance, and transparency of elections. Of course, we can also take this opportunity to improve more pragmatic features, such as offering better support for the election administration's desired workflow. Clearly, we're long overdue for election systems engineered with all the knowledge we now have available.

STAR-Vote also opens the door to a variety of interesting future directions. For example, while STAR-Vote is intended to service any given county as an island unto itself, there's no reason why it cannot also support *remote voting*, where ballot definitions could be transmitted to a remote supervised kiosk, which securely returns the electronic and paper records. By virtue of STAR-Vote's cryptographic mechanisms, such a remote vote is really no different than a local provisional vote and can be resolved in a similar fashion, preserving the anonymity of the voter. (A variation on this idea was earlier proposed as the RemoteBox extension [Sandler and Wallach 2008] to VoteBox [Sandler et al. 2008].) This could have important ramifications for overseas and military voters with access to a suitable impromptu polling place, e.g., on a military base or in a consular office.

(We do not want to suggest that STAR-Vote would be suitable for *Internet* voting. Using computers of unknown provenance, with inevitable malware infections, and without any systematic way to prevent voter bribery or coercion, would be a foolhardy way to cast ballots. A STAR-Vote variant, running in a web browser and printing a paper ballot returned through the postal mail, might well be feasible as a replacement for current vote-by-mail practices. A full consideration of this is left for future work.)

STAR-Vote anticipates the possibility that voting machine hardware might be nothing more than commodity computers running custom software. It remains unclear whether off-the-shelf computers can be procured to satisfy all the requirements of voting systems (e.g., long-term storage without necessarily having any climate control, or having enough battery life to last for a full day of usage), but perhaps such configurations might be possible, saving money and improving the voting experience.

ACKNOWLEDGMENTS

Olivier Pereira's work was supported by the Belgian French Community through the SCOOP ARC project and by the European Commission through the HOME/2010/ISEC/AG/INT-011 B-CCENTRE project.

REFERENCES

Ben Adida. 2008. Helios: Web-based Open-Audit Voting. In *17th USENIX Security Symposium*. San Jose, CA.

Ben Adida, Oliver de Marneffe, Oliver Pereira, and Jean-Jaques Quisquater. 2009. Electing a University President using Open-Audit Voting: Analysis of real-world use of Helios. In *Proceedings of the Electronic Voting Technology Workshop / Workshop On Trustworthy Elections (EVT/WOTE 2009)*. Montreal.

Jonathan Ben-Nun, Niko Farhi, Morgan Llewellyn, Ben Riva, Alon Rosen, Amnon Ta-Shma, and Douglas Wikström. 2012. A New Implementation of a Dual (Paper and Cryptographic) Voting System. In *5th International Conference on Electronic Voting (EVOTE 2012)*. Lochau/Bregenz, Austria.

Josh Benaloh. 2006. Simple Verifiable Elections. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '06)*. Vancouver, B.C., Canada. http://www.usenix.org/events/evt06/tech/full_papers/benaloh/benaloh.pdf

Josh Benaloh. 2007. Ballot Casting Assurance via Voter-Initiated Poll Station Auditing. In *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*. Boston, MA.

J. Benaloh and M. Fischer. 1985. A robust and verifiable cryptographically secure election scheme. In *28th IEEE Symposium on Foundations of Computer Science (FOCS)*. Portland, OR, 372–382.

J. Benaloh, D. Jones, E. Lazarus, M. Lindeman, and P.B. Stark. 2011. SOBA: Secrecy-preserving Observable Ballot-level Audits. In *Proceedings of the 2011 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '11)*. USENIX. http://statistics.berkeley.edu/~stark/Preprints/soba11.pdf

Josh Benaloh and Eric Lazarus. 2011. *The Trash Attack: An Attack on Verifiable Voting Systems and a Simple Mitigation*. Technical Report MSR-TR-2011-115. Microsoft Technical Report.

David Bernhard, Olivier Pereira, and Bogdan Warinschi. 2012. How Not to Prove Yourself: Pitfalls of the Fiat-Shamir Heuristic and Applications to Helios. In *ASIACRYPT 2012 (Lecture Notes in Computer Science)*, X. Wang and K. Sako (Eds.), Vol. 7658. Springer, 626–643.

J. Bretschneider, S. Flaherty, S. Goodman, M. Halvorson, R. Johnston, M. Lindeman, R.L. Rivest, P. Smith, and P.B. Stark. 2012. Risk-Limiting Post-Election Audits: Why and How. http://statistics.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf. (2012).

Craig Burton, Chris Culnane, James Heather, Thea Peacock, Peter Y. A. Ryan, Steve Schneider, Sriramkrishnan Srinivasan, Vanessa Teague, Roland Wen, and Zhe Xia. 2012. Using Prêt à Voter in Victorian State elections. In *2012 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '12)*. Bellevue, WA.

M. D. Byrne, K. K. Greene, and S. P. Everett. 2007. Usability of voting systems: Baseline data for paper, punch cards, and lever machines. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems (CHI '07)*. ACM, San Jose, CA, 171–180.

Bryan A. Campbell and Michael D. Byrne. 2009a. Now do voters notice review screen anomalies? A look at voting system usability. In *2009 USENIX/ACCURATE Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE)*. Montreal, Canada.

Bryan A. Campbell and Michael D. Byrne. 2009b. Straight party voting: What do voters think? *IEEE Transactions on Information Forensics and Security* 4, 4 (2009), 718–728.

Richard Carback, David Chaum, Jeremy Clark, Aleksander Essex, Travis Mayberry, Stefan Popoveniuc, Ronald L. Rivest, Emily Shen, Alan T. Sherman, and Poorvi L. Vora. 2010. Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy. In *USENIX Security 2010*. Washington, DC.

David Chaum, Richard Carback, Jeremy Clark, Aleksander Essex, Stefan Popoveniuc, Ronald L. Rivest, Peter Y.A. Ryan, Emily Shen, and Alan T. Sherman. 2008. Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes. In *Electronic Voting Technology Workshop 2008*. San Jose, CA.

Veronique Cortier, David Galindo, Stephane Glondu, and Malika Izabachene. 2013. A generic construction for voting correctness at minimum cost - Application to Helios. Cryptology ePrint Archive, Report 2013/177. (2013). http://eprint.iacr.org/.

R. Cramer, R. Gennaro, and B. Schoenmakers. 1997. A Secure and Optimally Efficient Multi-Authority Election Scheme. In *Advances in Cryptology - EUROCRYPT '97 (LNCS)*, Walter Fumy (Ed.), Vol. 1233. Springer, 103–118.

Edouard Cuvelier, Olivier Pereira, and Thomas Peters. 2013. Election Verifiability or Ballot Privacy: Do We Need to Choose? Cryptology ePrint Archive, Report 2013/216. (2013). http://eprint.iacr.org/.

Yvo Desmedt and Yair Frankel. 1989. Threshold Cryptosystems. In *CRYPTO '89: Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology*. Santa Barbara, CA, 307–315. http://dsns.csie.nctu.edu.tw/research/crypto/HTML/PDF/C89/307.PDF

T. ElGamal. 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory* 31, 4 (1985), 469–472.

Sarah Everett, Kristen Greene, Michael Byrne, Dan Wallach, Kyle Derr, Daniel Sandler, and Ted Torous. 2008. Is Newer Always Better? The Usability of Electronic Voting Machines versus Traditional Methods. In *Proceedings of CHI 2008*. Florence, Italy. http://www.chi2008.org/ap/112.html

Sarah P. Everett. 2007. *The Usability of Electronic Voting Machines and How Votes Can Be Changed Without Detection*. Ph.D. Dissertation. Rice University, Houston, TX.

Sarah P. Everett, Michael D. Byrne, and Kristen K. Greene. 2006. Measuring the usability of paper ballots: Efficiency, effectiveness, and satisfaction. In *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting*. Human Factors and Ergonomics Society, Santa Monica, CA, 2547–2551.

Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin. 2007. Secure Distributed Key Generation for Discrete-Log Based Cryptosystems. *J. Cryptology* 20, 1 (2007), 51–83.

K. K. Greene. 2008. *Usability of New Electronic Voting Systems and Traditional Methods: Comparisons Between Sequential and Direct Access Electronic Voting Interfaces, Paper Ballots, Punch Cards, and Lever Machines*. Master's thesis. Rice University, Houston, TX.

Srinivas Inguva, Eric Rescorla, Hovav Shacham, and Dan S. Wallach. 2007. *Source Code Review of the Hart InterCivic Voting System*. California Sec. of State's "Top to Bottom" Review. http://www.sos.ca.gov/elections/voting_systems/ttbr/Hart-source-public.pdf http://www.sos.ca.gov/elections/voting_systems/ttbr/Hart-source-public.pdf.

ISO. *Ergonomic requirements for office work with visual display terminal (VDT's)–Part 11: Guidance on usability*. ISO, Geneva, Switzerland. ISO 9241-11(E).

Aggelos Kiayias and Moti Yung. 2004. The Vector-Ballot E-Voting Approach. In *8th International Conference on Fianncial Cryptography (FC '04)*. Key West, Florida.

M. Lindeman, M. Halvorson, P. Smith, L. Garland, V. Addona, and D. McCrea. 2008. Principles and Best Practices for Post-Election Audits. www.electionaudits.org/files/best%20practices%20final_0.pdf. (2008). Retrieved April 20, 2011.

Mark Lindeman and Philip B. Stark. 2012. A Gentle Introduction to Risk-Limiting Audits. *IEEE Security and Privacy* 10 (2012), 42–49.

Gillian E. Piner and Michael D. Byrne. 2011. The experience of accessible voting: Results of a survey among legally blind users. In *Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting*. Human Factors and Ergonomics Society, Santa Monica, CA.

Niels Provos, Markus Friedl, and Peter Honeyman. 2003. Preventing Privilege Escalation. In *Proceedings of the 12th USENIX Security Symposium*. Washington, DC.

E. Rescorla. 2009. Understanding the Security Properties of Ballot-Based Verification Techniques. In *Proceedings of the 2010 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '10)*. http://www.usenix.org/event/evtwote09/tech/full_papers/rescorla-ballot.pdf Retrieved March 6, 2011.

Ronald L. Rivest and John P. Wack. 2006. On the Notion of "Software Independence" in Voting Systems. (2006). http://vote.nist.gov/SI-in-voting.pdf.

Peter Y. A. Ryan and T. Peacock. 2006. A Threat Analysis of Prêt à Voter. In *Workshop On Trustworthy Elections (WOTE 2006)*. Cambridge, U.K.

Daniel R. Sandler, Kyle Derr, and Dan S. Wallach. 2008. VoteBox: A tamper-evident, verifiable electronic voting system. In *Proceedings of the 17th USENIX Security Symposium*. San Jose, CA.

Daniel R. Sandler and Dan S. Wallach. 2007. Casting Votes in the Auditorium. In *Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*. Boston, MA. http://accurate-voting.org/wp-content/uploads/2007/08/evt07-sandler.pdf

Daniel R. Sandler and Dan S. Wallach. 2008. The case for networked remote voting precincts. In *Proceedings of the 3rd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'08)*. San Jose, CA.

B. Smith, S. J. Laskowski, and S. Lowry. 2009. Implications of Graphics on Usability and Accessibility for the Voter. In *Proceedings of the Second International Conference on E-Voting and Identity, VOTE-ID 2009*. Luxembourg, 54–74.

P.B. Stark. 2010. Super-Simple Simultaneous Single-Ballot Risk-Limiting Audits. In *Proceedings of the 2010 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '10)*. USENIX. http://www.usenix.org/events/evtwote10/tech/full_papers/Stark.pdf. Retrieved April 20, 2011.

Philip B. Stark and David A. Wagner. 2012. Evidence-Based Elections. *IEEE Security and Privacy* 10 (2012), 33–41.

Ka-Ping Yee. 2007. Extending prerendered-interface voting software to support accessibility and other ballot features. In *USENIX/ACCURATE Electronic Voting Technology Workshop 2007*. Boston, MA. http://pvote.org/docs/evt2007/paper.pdf

Ka-Ping Yee, David Wagner, Marti Hearst, and Steven M. Bellovin. 2006. Prerendered User Interfaces for Higher-Assurance Electronic Voting. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '06)*. Vancouver, B.C., Canada. http://zesty.ca/voting/prui/prui.pdf

Nickolai Zeldovich, Silas Boyd-Wickizer, and David Mazières. 2008. Securing Distributed Systems with Information Flow Control. In *Proceedings of the 5th Symposium on Networked Systems Design and Implementation (NSDI '08)*. San Francisco, CA.

End-to-end verifiability

Josh Benaloh, Microsoft Research. benaloh@microsoft.com

Ronald Rivest, MIT. rivest@mit.edu

Peter Y. A. Ryan, University of Luxembourg. peter.ryan@uni.lu

Philip Stark, UC Berkeley. stark@stat.berkeley.edu

Vanessa Teague, University of Melbourne. vjteague@unimelb.edu.au

Poorvi Vora, George Washington University. poorvi@gwu.edu

February 2nd, 2014.

This pamphlet describes end-to-end election verifiability (E2E-V) for a nontechnical audience: election officials, public policymakers, and anyone else interested in secure, transparent, evidence-based electronic elections.

This work is part of the Overseas Vote Foundation's End-to-End Verifiable Internet Voting: Specification and Feasibility Assessment Study (E2E VIV Project), funded by the Democracy Fund.[1]

Introduction – what is end-to-end verifiability?

Getting the election outcome right isn't good enough. Voters deserve convincing evidence that the outcome is correct.

There are many ways an election can go wrong or be suspect. Perhaps ballots were lost—and known to be lost. Perhaps a memory card failed—and was known to have failed. Perhaps more votes were reported than there were voters. Perhaps the announced outcome is correct but the evidence supporting it is incomplete or unconvincing. Perhaps some people claim to have observed irregularities. ***An election might appear outwardly to have been conducted properly but have an inaccurate outcome due to undetected errors or fraud.***

Well-managed paper-based elections include administrative mitigations to avoid these failures using a combination of human processes and physical evidence. If polling and counting processes are transparent, observers can watch the polling place throughout the election and scrutinize the count afterwards. Rigorous auditing conducted transparently and under observation can reinforce or correct the announced outcome.

Even under ideal circumstances—better than can be expected in real elections—typical voters have no eyes on the process. From their perspective, they cast their votes, go home, and are told the outcome. If they distrust election officials, equipment, or processes, there is little that they can do.

End-to-end verifiable election techniques enable individual voters to check crucial ingredients of election results – without requiring voters to trust election software, hardware, election officials, procedures, or even observers. Voters may check these ingredients themselves, place their trust in others of their choice (e.g. their preferred candidates, news media, and/or interest groups), or accept the outcome produced with the usual administrative safeguards.

[1] Thanks to Judy Murray and Keith Instone for helpful comments on an earlier draft.

Comparison with other software independent voting methods

E2E-V is not the only sensible option for computerized voting. In many cases some other software-independent system might be more appropriate. Software-independent systems, as defined by Rivest and Wack (Rivest 2008), are voting systems where an error in the voting system software will not cause an undetectable error in the election outcome. In such a system, one need not trust the voting system software to be correct in order to accept the election outcome, because there are other chains of evidence that can help check that the software performed its task correctly.

Most jurisdictions in the USA have accepted that electronic records from paperless DREs are not good evidence, motivating a return to permanent paper records. New techniques for risk-limiting audits have convinced most people that a properly conducted random audit is a good (and much cheaper) substitute for a full manual count in many circumstances. But audits still rely on the integrity and completeness of the paper records that are audited—which itself requires evidence. The integrity of the audit trail may be difficult to guarantee. It may be verifiable (for ballots cast in person) or not (for remote voting). Verifiably secure transport and storage of paper records is particularly challenging for remote voting, whether in a supervised or unsupervised polling place.

Any chain of evidence, for any system design, requires some assumptions. Checking that those assumptions hold for the election in question is crucial. Trusting unverifiable hardware or software is generally not reasonable. Trusting processes for secure handling of paper ballots may, or may not, be reasonable, depending on what those processes are and how they can be observed. E2E-V systems are software independent and do not rely on trusted paper processes, instead providing opportunities to verify the election outcome electronically.

Other considerations such as usability, accessibility, resilience, vote privacy and resistance to coercion are also important, but not part of this document.

How to achieve end-to-end verifiability (E2E-V)

End-to-end verifiability is a collection of techniques for replicating, and in some ways exceeding, the standards of evidence provided by an ideal, observed, polling place. This includes two principal components.

1. *Cast As Intended:* voters can verify that their selections (whether indicated electronically, on paper, or by other means) are correctly recorded, and
2. *Tallied As Cast:* any member of the public can verify that every recorded vote is correctly included in the tally.

Consider first a simple way to conduct a verifiable election: the names of voters along with their votes are posted on a public "bulletin board" of some kind. Voters can check the bulletin board to see whether their own votes appear correctly, and everyone can confirm the tally of the listed votes. This election tally is easily verifiable by anyone[2] and requires no trust in election officials, but there is no privacy – all votes are public.

So, let's try a more sophisticated approach: an election authority assigns each voter a pseudonym. After each voter votes, the authority posts the pseudonym next to the vote. Again, voters can individually check that their correct votes appear alongside their respective pseudonyms. This protects ballot privacy somewhat (some voters might accidentally or deliberately reveal their pseudonyms) but it still has problems – for example, voters are susceptible to coercion, and the

[2] Voters must trust that *other* voters are also checking that *their* votes appear correctly.

authority might cheat, for instance by assigning the same pseudonym to voters who are likely to vote the same way.

So, we move to a still more sophisticated approach. Each vote is encrypted before it is cast, meaning that it can be read only by someone (such as the electoral authority) who holds the secret decryption key[3]. The authority posts each encrypted vote on the bulletin board next to its voter's true name. Now of course, to compute the outcome, the authority has to compute the tally from encrypted votes in a way that will preserve ballot privacy, and to check the outcome, voters need to be able to verify that the tally of encrypted votes is correct. In most end-to-end verifiable systems, the two principle requirements described above (*cast as intended* and *tallied as cast*) are achieved in three phases, described here.

1. *Cast As Intended:* voters make their selections and, at the time of vote casting, can get convincing evidence that their encrypted votes accurately reflect their choices;
2. *Recorded As Cast:* voters or their designees can check that their encrypted votes have been correctly included, by finding exactly the encrypted value they cast on a public list of encrypted cast votes; and
3. *Tallied As Recorded:* any member of the public can check that all the published encrypted votes are correctly included in the tally, without knowing how any individual voted.

End-to-end verifiable voting schemes provide ways of performing these tasks. Consider the *cast as intended* step. One solution is to tell voters that they may use the voting device to produce as many encrypted ballots as they like, but choose only one to cast. All the other encrypted ballots serve as "challenges" and are subsequently decrypted to provide evidence that they match what the voters expect. This is often called a "Benaloh" challenge. Checking that the decryption is honest may require assistance, but these need not be burdensome for voters. While voters could expend the effort to use any of a variety of means to check the decryptions in real time, it is simpler for the election authority to post all challenged ballots on a public list (distinct from the list of cast ballots).

It is crucial that the voting device does not know which encryptions will be challenged. If enough voters select randomly and independently which encryptions to challenge, the machine is very likely to be "caught" if any significant portion of its encryptions are faulty. Also importantly, it is not necessary for all voters to challenge encryptions for this detection probability to be large. The crucial assumption is that the voting device cannot predict with confidence that certain voters will not challenge.

The Helios E2E-V Internet voting system (vote.heliosvoting.org) was one of the earliest systems to use this approach. The Wombat voting system, http://www.wombat-voting.com/, and StarVote both combine this sort of challenge mechanism with a paper evidence trail.

Prêt à Voter and Scantegrity II use a related approach, but the encrypted candidate names are generated before voting and printed on paper alongside human-readable candidate names. Each voter marks a selection of those (encrypted) candidate names. Interested voters can challenge printed ballots before they vote, which means checking that they are "correctly constructed" and hence would result in correct encryptions of the vote.

The *recorded as cast* step usually involves giving data about the encrypted ballot to the voter as a "receipt" when the voter casts the ballot. Voters may subsequently check the published list to ensure that the data on their receipts is published correctly.

The *tallied as recorded* step uses cryptographic mathematical proofs, usually in one of two ways. The first method, called "verifiable mixing," disassociates the votes from voters' names by

---

[3] The encryption step also adds some randomness, so that two encryptions of the same vote don't look the same.

"shuffling," then decrypts the votes. This shuffling is performed in a way that allows the authorities to prove that none of the votes have been altered but does not allow the public to trace a given vote to any particular voter. The second method, which uses "homomorphic encryption," makes it possible to tally the encrypted votes without decrypting them and then prove that the tally is correct. Both methods produce a mathematical proof that the announced outcome matches the published encrypted cast votes.

What procedures are necessary to support E2E-V?

End-to-end verifiable systems require unfamiliar (and sometimes complex) procedures, which pollworkers must be trained to follow exactly. If the procedures are not followed to the letter, it may be impossible to give convincing evidence that the announced election result is correct.

What trust assumptions remain?

End-to-end verifiability puts powerful auditing capabilities into the hands of voters, but it adds nothing if these capabilities are not exercised. A verifiable election that nobody bothers to verify does not produce any meaningful evidence, and the evidence can be unconvincing if an insufficient number of voters avail themselves of their new capabilities. Fortunately, in most cases only a tiny fraction of voters need to perform these additional tasks to produce compelling evidence of the correctness of the election outcome. The additional procedures that are available vary among end-to-end verifiable systems, but they can place an extra burden on voters and election officials.

E2E-verification hinges on the unpredictability of voters. If the system makes many errors—either encrypting votes incorrectly or losing encrypted votes before they are published—then it does not take many attempted verifications for there to be a large chance of discovering at least one error, provided voters decide whether to verify the encryption of their votes or the presence of their votes on the bulletin board as if at random, independently. Some verification (such as the voter's opportunity to check that their votes are cast as intended) must be performed on the spot, by the voter, before the election outcome is known. Other kinds, such as correct recording of votes or a universal check of correct tallying, can be performed afterwards, by anyone.

(In contrast, methods such as Risk Limiting Audits use public random auditing to develop statistical evidence about election outcomes. However, this evidence may be convincing to only to voters who observe the audit, or who trust those who observed the audit.)

In current E2E-V systems, much of the verification involves calculations that are beyond the capabilities of humans to perform the checks unassisted. They need software and computers to perform the checks, but this of course raises a further question – how can we trust the checking software? The answer is that anyone can, in principle, write software to perform the checks. Independent organizations (such as interest groups or news media), interested individuals, and even candidates or political parties can provide their own checking software. Voters and observers can choose any source they trust, use several, or even write their own; in principle, that makes it possible to determine whether the checking software is correct. More importantly, as long as *enough* checks are performed with sound code, there will be a large chance of detecting errors. In contrast to traditional systems, where the software is built by vendors behind closed doors and chosen by election officials, with E2E-V systems, the verification process is public and each voter can choose which verification software to trust.

The risk of conflicting results amongst software verifiers is mitigated by public expectations of their results. A verifier that merely asserts that an election tally is incorrect – without offering specific evidence – can be ignored. A reasonable verifier should either assert that a tally is correct or offer evidence of an error that is so specific as to be verifiable by hand. All properly-constructed verifiers should produce the same result. However, if there is disagreement, even a lone verifier that finds an error in the tally is sufficient to overturn a result if it provides specific and independently-confirmable evidence of an error.

It should be noted that within this context, errors are not trifles. Instead what is being verified is that a posted set of ballots corresponds to a claimed tally. Errors at this stage are not caused by misplaced ballots or ambiguous interpretations. An error here is only possible if the tallying software misbehaves, and in such cases the tally produced could be off by a million votes as easily as off by a single vote. Confirmed errors need to be rectified to obtain an accurate tally.

How can you tell whether you've got E2E-V?

Since end-to-end verifiability is recognized as a desirable attribute, some electronic voting software vendors claim they (already) sell it. Claims are easy, but implementing E2E-V methods is not. Having examined many commercial products, we know of none that offers true E2E-V. The crucial properties are the kinds of verification mentioned above, with complete freedom about what software to trust for verification. ***If voters and election observers do not have complete freedom about which software to trust to do the verification, or if only a privileged few are able to verify at all, the system is not truly E2E-V.***

Dispute resolution (accountability, non repudiation, defense against defaming).

Our discussion of verification has so far included only a description of what can be verified. End-to-end verifiability gives voters (collectively) the opportunity to detect errors that might have altered the announced outcome. We have not discussed procedures for dealing with claims that the system erred. Of course, claims may be legitimate, but they might also be false. Hence, we have several closely related questions:

- If voters (or observers) detects that the system erred, how can they prove it?
- What procedures are in place to ensure that credible claims of error are acted on appropriately?
- How can the system (or the authorities) defend against false claims that the system misbehaved?

These questions apply to conventional voting systems too. For example, a voter could claim that a voter-verifiable paper trail has incorrectly recorded a vote, or an observer of a traditional paper count could claim to have observed misbehaviour. Because E2E-V presents new kinds of verification, it also introduces new ways to perform this old attack.

A good E2E-V system should specify what happens if a verification step fails. Authorities and observers should have ways to assess whether a problem is genuine and how much of an election could be affected. This is called "dispute resolution," meaning that when someone complains about a system malfunction, the accuser can bring evidence to a third party who can resolve the dispute by either accepting the evidence of system misbehaviour or exonerating the system.

For example, many end-to-end verifiable systems provide voters with a paper receipt at the time of voting. The voter uses this information later to check whether the associated vote was correctly included in the count. If such receipts are easy to counterfeit, then voters can falsely accuse the system of altering or omitting votes (this is sometimes called a "defaming attack"). Although such attacks cannot manipulate votes undetectably, they can cast doubt on the outcome by creating the impression that someone has manipulated the votes. Prêt à Voter, and variants such as the vVote system, print a digital signature on each receipt. This can make it very difficult to forge a paper receipt. However, a malicious voting system could produce invalid digital signatures on receipts associated with votes that it wishes to discard. Thus, digital signatures are only effective if voters have independent means to validate the validity of the signature within poll sites (perhaps using a trusted application on a personal smart phone to read a QR code or 2D bar code). Even then, a protest is only credible if independent entities can observe that the invalid receipt came directly from the election equipment and not, say, the voter's pocket.

As another example, Scantegrity II provides voters with short return codes (usually two letters) which voters only see after committing to their selections. Voters can later use these codes to prove that their votes should have been included. A voter who attempted to defame a system by falsely accusing it of altering or omitting a vote would need to guess the right return code. This is difficult but not impossible – if there were thousands of false accusations, we would expect a handful of correct guesses "by chance." Because the Scantegrity II paper ballots are printed in advance, incorrect return codes would likely be detected during the ballot verification process.

The STAR-Vote system also provides real-time evidence that can be used for dispute resolution. Voters can spoil ballots produced by the system. Upon spoiling a ballot, a voter is in direct possession of both an encrypted receipt and an associated cleartext ballot summary. These can be shown to observers and the paper can be retained by the voter as forensic evidence.

Without dispute resolution, it may not be possible to distinguish genuine errors or manipulation attempts from efforts to defame the system. Hence it may not be possible to verify whether the outcome was indeed correct. However, even without dispute resolution, voters using an E2E-V system will know whether their votes have been properly counted and will know whether the count of the recorded votes is correct. The uncertainty comes if other voters claim that their votes were not correctly included, and external methods must be employed to assess the veracity of any such claims. This uncertainty can be mitigated if a process of real-time auditing is used wherein systems are randomly tested in public with dummy votes; in contrast with normal voters, dummy voters can be observed and even recorded during the process, and any inconsistences can thereby be publically captured.

Practical deployments of E2E-V

There have been numerous small trials of end-to-end verifiable voting systems. Some interesting polling-place E2E-V systems for binding government elections:

- The use of Scantegrity II (http://en.wikipedia.org/wiki/Scantegrity) in Takoma Park MD is still the only example of true E2E-V to have been used in a binding government election in the U.S. It combined E2E-V with familiar opscan-like paper ballots.
- A version of the Prêt à Voter E2E-V voting system was used for part of the State government election in the Australian state of Victoria, in November 2014.
- The StarVote project, which is expected to be used for binding government elections in Travis County and Dallas County, TX, beginning around 2018, also combines a paper evidence trail with an E2E-V voting system. Methods for facilitating risk-limiting audits of the paper trail are incorporated as well.

Some Internet E2E-V systems:

- Remotegrity was the remote voting solution for Takoma Park MD. Voters received a code sheet by postal mail, which then allowed them to cast their votes over an E2E-V Internet voting system linked to Scantegrity II.
- The Helios E2E-V Internet voting system (vote.heliosvoting.org) has been used in numerous non-government elections.

Non-E2E-V Internet voting systems may permit some verification of some steps. For example:

- Civitas (http://www.cs.cornell.edu/projects/civitas/) is a coercion-resistant Internet voting system that provides openly verifiable evidence that all the votes are correctly included and accurately tallied. However, it does not currently allow voters to verify that their votes are cast as they intended.
- The now-discontinued Norwegian Internet voting system incorporated an elegant code-based system for voters to check that their votes were cast as they intended. It also

provided some evidence to some restricted observers that the outcome was tallied as recorded.

As far as we know, no end-to-end verifiable Internet voting scheme has been used for a large-scale binding government election. There is almost no experience with E2E-V in governmental elections, even in supervised settings.

Conclusion and discussion of remaining issues

End-to-end Verifiable election technologies can be used in paper-based systems and in fully electronic systems, in remote voting systems and in-person poll-site systems, with simple majority counting methods and with many complex preferential schemes. *Any* electoral system can benefit greatly from the inclusion of E2E-V technologies. That said, the most vulnerable systems have the most to gain. There are good safeguards available for an election that is conducted entirely in-person and on hand-counted paper using simple rules. However, without E2E-V technologies, it is much more difficult to mitigate the inherent risks associated with remote and/or electronic systems. In particular, the risks of Internet voting systems are very substantial and they should not be contemplated without the mitigating benefits of E2E-verifiability.

However, while E2E-V appears to be a necessary condition for Internet voting, E2E-V Internet voting does not currently provide the same standards of evidence as E2E-V elections in supervised settings. We do not yet have much experience with E2E-V governmental elections in supervised settings, where procedures and the use of paper and statistical audits can help to address mishaps. The remote setting is far more challenging—especially without the use of a second channel (such as the postal service) —and also much less predictable. The only responsible path forward for Internet voting is to implement polling-place E2E-V voting and gradually experiment with more ambitious deployments without weakening the standard of evidence.

Remaining unsolved challenges include:

- ensuring that enough voters perform the cast-as-intended verification process properly,
- achieving dispute resolution without supervision of the voting process,
- achieving usable cast-as-intended verification without paper or some other similar material that allows the device to commit to an encrypted value.

There are partial solutions in each case. Remotegrity has some dispute resolution, but relies on a paper code sheet sent in conventional mail. Helios allows for cast-as-intended verification without paper, but only if the voter is very careful to record the encrypted votes before they are challenged. Some forms of encouragement for cast-as-intended verification could be performed remotely.

Overall, we are *not* asserting that Internet voting is viable if it is E2E-V, nor that the resulting scheme would achieve the same degree of privacy or verifiability as in-person (attendance) voting.

References

Rivest, R. L. (2008). "On the notion of 'software independence' in voting systems." Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences **366**(1881): 3759-3767.

Estonia gets to vote online. Why can't America?

By Brad Plumer November 6, 2012

http://www.washingtonpost.com/news/wonkblog/wp/2012/11/06/estonians-get-to-vote-online-why-cant-america/

If anecdotal reports are anything to go by, millions of Americans on Tuesday are standing in the cold for hours to vote at their local polling places. But why should they have to? Many Americans can already pay their utilities online and bank online. Why can't we vote over the Internet as well?

That's the question raised by Thad Hall, a political scientist and author of *Electronic Elections*. In theory, he says, allowing Americans to vote online could have all sorts of benefits. We wouldn't have to endure hours outside in the chilly November air waiting to vote. We could do research online while voting for ballot initiatives. Americans overseas could cast ballots more easily. But, he notes, there are big potential downsides too, including the very real risk that the system could get hacked.

Online voting isn't a far-fetched idea. Estonians have been doing it since 2005. While only 2 percent of Estonians took advantage of the system when it first came out, that number rose to 25 percent by 2011. "Surveys have found that Estonians view their system as being very effective," Hall says. "They have high confidence in it. They like it."

What's Estonia's secret? For one, all Estonians are issued a government ID with a scannable chip and a PIN number that gives them a unique online identity — they can use this identity to file their taxes or pay library fines or buy bus passes. That makes Internet voting workable. (The votes are encrypted to preserve anonymity.) What's more, Estonia has a proportional representation voting system, rather than a winner-take-all system like the United States. According to Hall, research has found that electoral fraud

seems to pop up more frequently in winner-take-all systems — since there's more at stake for the candidates.

Indeed, far and away the biggest concern about Internet voting is that such a system would be highly susceptible to fraud or hacking. Over at MIT Technology Review, David Talbot recaps concerns by computer scientists at a recent conference on the topic:

The unsolved problems include the ability of malicious actors to intercept Internet communications, log in as someone else, and hack into servers to rewrite or corrupt code. While these are also big problems in e-commerce, if a hacker steals money, the theft can soon be discovered. A bank or store can decide whether any losses are an acceptable cost of doing business.

Voting is a different and harder problem. Lost votes aren't acceptable. And a voting system is supposed to protect the anonymity of a person's vote—quite unlike a banking or e-commerce transaction—while at the same time validating that it was cast accurately, in a manner that maintains records that a losing candidate will accept as valid and verified.

Hall agrees that those security concerns are legitimate. Still, the fact that online voting would make it much easier for many people to cast a ballot makes it an enticing prospect. Washington D.C., for one, tried to develop an Internet Voting pilot project back in 2010, though computer scientists found that the program was riddled with flaws and easily hacked. After that, it was back to the drawing board.

The other big question, meanwhile, is whether Internet voting would actually expand participation at all. In a paper (pdf) in 2005, MIT's Adam Berensky found that most electoral reform measures mainly benefit voters who were *already* highly motivated to vote. If that's true, then online voting might simply make it easier and more convenient for dedicated voters and partisans

to cast a ballot. It wouldn't necessarily lure in those who aren't voting currently.

Hall agrees that online voting likely might not make a huge difference in overall participation — though there's one huge exception here. His research has found (pdf) that online voting could be a huge boon to Americans with disabilities or those who find it hard to get to their local polling places on Election Day. According to the Census, some 2.3 million Americans didn't vote in 2008 because of an illness or disability. Simply making it easier for those voters would be a big deal.

"You can find a lot of computer experts who will tell you all about the potential problems," Hall says. "But there are a lot of potential benefits too."

Further reading:

--A closer look at why more than 50 million Americans won't vote in this election.

--For more on those potential problems, check out this story from 2010 of how a computer scientist quickly hacked into Washington D.C.'s proposed online voting system.

--Thanks to wolfemi1 in comments, here's a great Slashdot article on the pros and cons of online voting. Privacy is another concern: "Now if you have to go to a voting booth to vote your overbearing [significant other] can't coerce you to vote one way or another. You have plausible deniability. That's kind of hard to do when they're standing behind you watching you vote from the family PC."

Estonia's Online Voting System Is Not Secure, Researchers Say

BY ANTONELLA NAPOLITANO | Wednesday, May 21 2014

http://techpresident.com/news/wegov/25066/estonia-online-voting-system-not-secure

“I gave my e-vote. This is not only convenient, but a vote of confidence to one of the best IT systems in the world, a vote of confidence to the Estonian State,” tweeted Toomas Hendrik Ilves , the president of Estonia on May 15th, marking the start of early voting for the European Parliament (the voting process will end on May 25th.)

While undoubtedly convenient, e-voting in Estonia might not be as safe as President Ilves think.

An independent group of researchers recently tested the Estonian I-voting system used during the last municipal elections, held in October 2013, and concluded that the flaws and lapses in operational security make it vulnerable to manipulations. Therefore, it cannot be considered safe enough.

Last Monday, the Guardian reported on the research, whose results are available in a technical report published on Estoniaevoting.org, a website set up by the researchers, complete with photos and videos.

"These computers could have easily been compromised by criminals or foreign hackers, undermining the security of the whole system," declared Harri Hursti to the British newspaper. Hursti is an independent researcher from Finland with experience in testing e-voting systems.

Estonia: Proudly Voting Online Since 2005

Today, Estonia is the only country that has been significantly and consistently using the e-voting system.

Starting in a 2005 local election, the system has being used in all subsequent elections, including the last European election in 2009; up to a quarter of votes are cast online, notes the Guardian. In the (contested) 2013 municipal elections, about 21 percent of voters used online voting.

In order to cast an online ballot, a voter identifies him/herself with the use of an activated electronic ID card, a system which has been available for several years.

The group of independent researchers recreated the system, using the real source code and the client software and simulated the kind of attacks the system could be subjected to, whether it be home computers or the central system.

“Estonia's Internet voting system is actually quite sophisticated,” says Alex Halderman, one of the researchers in a video detailing the work on the e-voting system. He explains: “The system was built by people who had intimate knowledge of security. They made large parts of the system open source, they documented their procedures and they have videos of almost every step of the process."

But this is not enough, he concludes: the system is still susceptible to being compromised.

Halderman, a professor at the University of Michigan, is a longtime skeptic of online voting.

Back in 2010, he tested a District of Columbia pilot project aimed at allowing overseas and military voters to download and return absentee ballots over the Internet.

“It may someday be possible to build a secure method for submitting ballots over the Internet, but in the meantime, such systems should be presumed to be vulnerable based on the limitations of today’s security technology,” he wrote at the time.

After the article was published by the Guardian last Monday, the Estonian National Electoral Committee (NEC) issued a statement with a preliminary rebuttal to the researchers' critiques. Here are some of their points:

1. The researchers have not discovered any new attack vectors that had not already been accounted for in the design of our system as a whole.
2. It is not feasible to effectively conduct the described attacks to alter the results of the voting.
3. The electoral committee has numerous safeguards and failsafe mechanisms to detect attacks against the elections or manipulated results.
4. The website put up by the security researchers (estoniaevoting.org) contains numerous factual and detail errors, and does not provide technical details on the alleged vulnerabilities in our system.

The NEC also argues that the system has been used in six elections “without a single incident which have influenced the outcome.”

The subsequent response of the researchers points out that there is no way to prove that there has been no interference because of the flaws of the system: “Our research argues that a well resourced attacker, such as a nation-state like Russia, would be able to undetectably steal votes in an election using the Estonian e-voting system. We maintain that the Election Committee cannot, by virtue of the failings in the systems used, irrefutably prove that the six elections thus far conducted were never influenced nor could they prove that for elections using the system in the future based on the current design.”

Security Flaws and Critical Questions Not Asked

This is not the first time that doubts about the security of the Estonian voting system have been raised.

In a 2011 report on Estonian national elections, the Organization for Security and Co-operation in Europe (OSCE) concluded that several parts of the voting process, from software testing to data storing, were exposed to manipulations.

“As in previous elections, and despite the recommendation made by the OSCE/ODIHR in 2007, the time of casting a vote was recorded in a log file by the vote storage server along with the personal identification code of the voter,” the report says. “This could potentially allow checking whether the voter re-cast his/her Internet vote, thus circumventing the safeguards in place to protect the freedom of the vote.”

The software test raised more concerns. According to the report, the NEC carried out a test of the software without formal reporting. The report explains that “the Cyber Defence League (CDL) conducted an exercise in January 2011 to test the software under given threat scenarios, and produced a report for the NEC that was made available to observers but not to the public. […] In a parallel process, a programmer, who was contracted by the NEC, verified the software code. The identity of the programmer and his report to the NEC was kept secret. It was not made available to the OSCE/ODIHR EAM, other observers or political parties.”

While the entire electoral process was conducted in a collaborative environment and no particular issues were detected, the OSCE report expressed concerns that this led to an environment “where critical questions were no longer asked and where detailed protocols of proceedings were too rarely part of the process.”

Another risk is that online elections can't be audited effectively because there's no paper trail, says Margaret MacAlpine, the Post-Election Audit Advisor featured in the video about independent researchers analyzing the voting system.

She later advised the Estonian government to keep working on their excellent e-government system but to take the online voting out of it.

Another round of analysis and counterarguments will likely come after the European elections.

“In my assessment, no country in the world today can do Internet voting safely” concludes Alderman in the video. “It's going to be a decade, if ever, before we're able to solve some of the central security problems at stake.”

Personal Democracy Media is grateful to the Omidyar Network and the UN Foundation for their generous support of techPresident's WeGov section.

E-voting is (too) secure

Anto Veldre writes about yet another attack against Estonian e-elections that started this week: again political, again not technical.

https://www.ria.ee/e-voting-is-too-secure/

14.05.2014

Responsible and irresponsible disclosure

‘Responsible disclosure’ is a standard practice in the information security community – a person who identifies a security issue doesn't rush to abuse it (to rob a bank or extort money) – but contacts the company that created the software and tells them where exactly the vulnerabilities are, what they look like, etc.

This practice is reasonable, as repairing security holes may be very expensive for some companies, which means that hiding the hole for as long as possible may be economically more beneficial for such companies.

Responsible disclosure policy helps against such delays – at first, the author of the faulty software is given time to correct the error (a month or two), but a date is set when the technical description of the error will be made public. This way, the wolves are fed and the sheep stay safe.

The way responsible disclosure usually works in practice is that the experts who detect the security vulnerability send an accurate, passionless and technical description of the error to the author (the manufacturer of the device or software). For example, citizen X reports that such a security hole (followed by a description) was detected in product Z of company Y.

Technical information, network dump and command line examples are added so other parties can reproduce the error and correct it. A competent specialist looks at the description and immediately understands: “Yep, the hole is here!”. Any specialist following the instructions in the initial report can also reproduce the problem.

Without a detailed description, security errors cannot be confirmed, checked or repaired. It’s up to the reporter to produce the description. In contrast, cartoons, political invective or the drum roll of Siberian shamans proclaiming the end of the world are not the proper way to report security problems. Hysterical cries that the bug will bring about the end of the world tomorrow are likewise useless.

PR incidents, on the other hand, are completely different creatures. They appear in another manner: either as newspaper articles, anonymous phone calls or hints given by friends. The claim made in the case of a PR incident usually is that **absolutely everything** is kaput, the security

hole is **the size of the Earth**, but the technical information required for checking the claim is not provided.

Stories about the impending end of the world in media publications keep collecting clicks, but the experts who would like to repair the errors never get to discuss details with the accusers or, even if they manage to do so, get no **substantive** information. But the 'risk assessment' thrown into the media is scary, the 'end of the world' is coming and cannot be stopped!

Yet another attack

On the evening of the second Sunday in May, a website appeared from nowhere claiming that things with the e-elections in Estonia had gone all pear-shaped and that there was going to be a press conference at 11 am on Monday. A project-based claim site had also been prepared about the case.

Although the claim site was not yet up on Sunday, it later became evident that a group of 'independent experts' had audited the Estonian e-voting system, found it to be 'shockingly unsecure' and the voting results 'easy to manipulate', and urged the Republic of Estonia to cancel its online voting.

Quote: "We urgently recommend that Estonia discontinue use of the system." And then: "...use of the Estonian I-voting system should be immediately discontinued."

This was followed by a friendly suggestion: "Estonia has a well organised paper voting system that they should revert to." So, some 'expert' arrives and asks the Republic of Estonia to take down one of its public information systems. Immediately! Of course, the Government of the Republic of Estonia can be the only addressee of this demand, as online voting, which is carried out on the basis of law, simply cannot be cancelled at a lower level.

There is also the promise that information about the errors will be given, but… only after the elections?

Why is it bad that e-elections are so secure? Because manipulating such elections is extremely difficult. This doesn't suit those who are used to achieving what they want by bending the rules. To wit, e-elections don't enable the sort of grotesque 'voting' we saw in Eastern Ukraine last week (and whose more 'civilised' variant people who under Commununism still remember).

Maybe the reason for the attack against e-elections is that one or more political parties operating in Estonia would be pleased about such falsification? The foreign experts who've been 'thrown under the bus' may not even understand that they're here not because of their technical savvy, but their politically suitable (although technically incompetent) message.

Alleged security holes

The first allegation made by the group of experts is that PCs may be infected with malware. Take note – may be! Cyber hygiene in Estonia is relatively high. It is true that there is more malware circulating in Estonia than in Finland, Denmark or Singapore, but we're still far ahead of the other Eastern bloc countries.

About that hole. Item 9.2.4 of the an E-voting security analysis commissioned by the National Elections Committee tells us that the possibility of a voter's computer being exploited was acknowledged back in 2003. What was done with this knowledge?

In a democratic country, it is unthinkable that the State goes to a person's home, even virtually, and starts creating order in voters' computers, e.g. by removing malware. That's why this risk has been acknowledged and marked as an ACCEPTED risk (see the explanations here).

Voters themselves have to keep their computers clean (at least) during the elections! Of course, using smartcard readers with built in PIN-pads really helps, as this way malware on your computer cannot see your PINs. There's nothing that malware can do with the ID card – it is a two factor device, so PINs are always required. Even if the card has been glued into the card reader.

Anyway – we were given the general opinion of some expert that the voter's computer MAY be infected with a virus. It may indeed be. But nice people who care about computer hygiene have no viruses. And if someone is afraid that their computer may be infected, they can always go to the polling station on the day of the elections or use a card reader with a PIN pad. It's up to the person to decide – do they know what's going on in their computer or would they rather go to the polling station.

The other serious allegation is that the DVDs from which the e-voting systems are installed MAY be infected. This is a valid claim, THEORETICALLY. Just like a storm hitting Estonia on the day of the elections and paralysing our energy system, the explosion of a neutron bomb on a train arriving at the Main Railway Station or the Sun transforming into a Supernova.

Alright then. How will a DVD and/or the software on it become infected and infect others? Are we talking about an attack against the file system, compromising the software, screwing up the compiler or what exactly is happening, dear e-election experts?

OK. Let's suppose that there is 'an attack'. Who on the IT team of the elections are the traitors who lie that the image hashes on the discs are a match, although this is not the case when they're compared?

As far as we know, no technical descriptions of the attacks have been given to the Election Committee (EC), to us or to anybody else.

Apparently, the group reviewed last year's e-voting audit videos on Youtube minute by minute and found some interesting events:

1. Debian Linux packages were downloaded from a place that the experts didn't like.
   So they should've been downloaded a distro from a .ru or .su website?
2. The icon of a poker website could be seen on the desktop (was it actually a poker website or 'an icon similar to the icon of a poker website'?).
   Of course, having this icon on the desktop of course discredits the user of that computer, their country and the entire European Union.
3. The RAID controller had a delay recognising a disk.
   The RAID controller was obviously infected with BadBIOS and FOXACID at the same time! In addition to the "Bundestrojaner".
4. The WiFi password of the local guest network could be seen on the wall.
   Oh dear, because the election servers (with the telephones and computers of all guests) are certainly connected to that WiFi network, their ILO ports greedily open.
5. The cameraman who shot the audit filmed an elections observer in such a manner that his password was captured on film.
   We do thank you for this observation – we will improve our cameraman's training – but this is an error of the supporting process (the audit) and not the main process (the elections).
   The fact that the e-elections team in corpore change all of their PINs and passwords after the elections isn't important here.

But… how did these five findings lead to the conclusion that the entire e-election server system has actually been compromised by a foreign country (Russia was explicitly named) and so unsecure that the I-voting must be cancelled?

The experts have not presented descriptions of any repeatable activities that (apart or together) lead to the materialisation of such a scenario.

I remember the meeting in July 2013 where the source code used for the e-voting was made public. During a two-hour meeting, the e-voting team received considerably more constructive feedback from the public than we have now received from the Kitcat team in three days.

US vs Estonia

In North America, the attitude towards any e- or i-voting differs significantly from Estonians'. The first attempts at electronic voting on the other side of the Atlantic were plagued by security holes. Security specialists broke into Diebold's election machines (well, kiosk like devices). We were well aware of all this when we launched e-voting in Estonia. Our attitude towards e-voting has been positive, or at least cautiously neutral, from the very beginning. The attitude of the US towards e-voting is strictly negative. There are entire schools of specialists who are ideologically convinced that e-voting is the devil's playground.

Electronic or online, i.e. i-voting? The Americans only learnt to distinguish between these two in the last couple of years. They couldn't have online voting (which is what we call i-voting), as they don't have anything like our ID card and PKI. The real issue isn't about the physical, plastic ID card, but about a nationally supported PKI system (Public Key Infrastructure), which makes it possible to identify the cardholder remotely by electronic channels and to make sure that the

signature they give is authentic. This service, provided by Estonia's Certificate Authority, is the very 'magic' that allows Estonian banks, the Tax Board or small company websites to identify people electronically.

This difference probably led to several hilarious situations during the events organised by the Estonian Centre Party, where examples of attacks against Diebold voting machines were used to preach "the truth" that Estonian e-voting is the deed of The Satan. But comparing Diebold machines with Estonian e-voting system is as comparing wild boar with a toothbrush – both are hairy!

Estonians' experience with falsifying the paper voting dates back to the Soviet era: The Communist Party always received 97-99% of votes in all polling stations. How? Well, the memories of that voting process could be rather traumatic for "the voters", featuring free vodka, bribery, broken fingers, swollen testicles or event some cold years in Siberia.

Point being, we have very real memories of the practices used to falsify the "paper voting".That's opposed to the fact that it's rather difficult to bribe a computer.

Therefore, the experience over here, in Estonia, is that paper voting is a lot easier to falsify.

Theoretical vs practical security

People in the West probably still believe that verified security solutions (altogether with the back doors) can be created on a drawing board and then used for decades without any changes. This hasn't been the case for a long time. The development of computers has increased the complexity of technology significantly. Try as hard as you want, there is always going to be an error, not to mention intentional traps.

Joanna Rutkowska hit the nail on the head when she wrote that the keyboard, screen and mouse of your computer belong to… whom? No, they don't belong to you, they belong to the software manufacturer. Technically, the manufacturer can take over your identity at any time and do whatever it wants on your behalf. Not a single modern operating system has been designed in consideration of the opposite requirement. Therefore, we can only trust our computer so much. In practice, though, Microsoft and Apple don't interfere with people's lives and we can only guess why.

The same applies to the hardware we use. It's made somewhere in China or South Korea and it is possible that there is a back door somewhere on the motherboard.

These claims sound so horrendous that we should stop using computers altogether!? The reality isn't actually that bad. Despite the OS and hardware risks, it is still possible to build software and procedures on top of these that are owned by the state of Estonia and use the Internet as the communications channel. Every movement that is important for the outcome (of the voting process) is logged and the e-voting process is observed by dozens of IT people (and international IT aware observers are very welcome as well!). Yes, we must keep the threats described above in

mind and evaluate them in our risk assessment formulae as well as in our software development process.

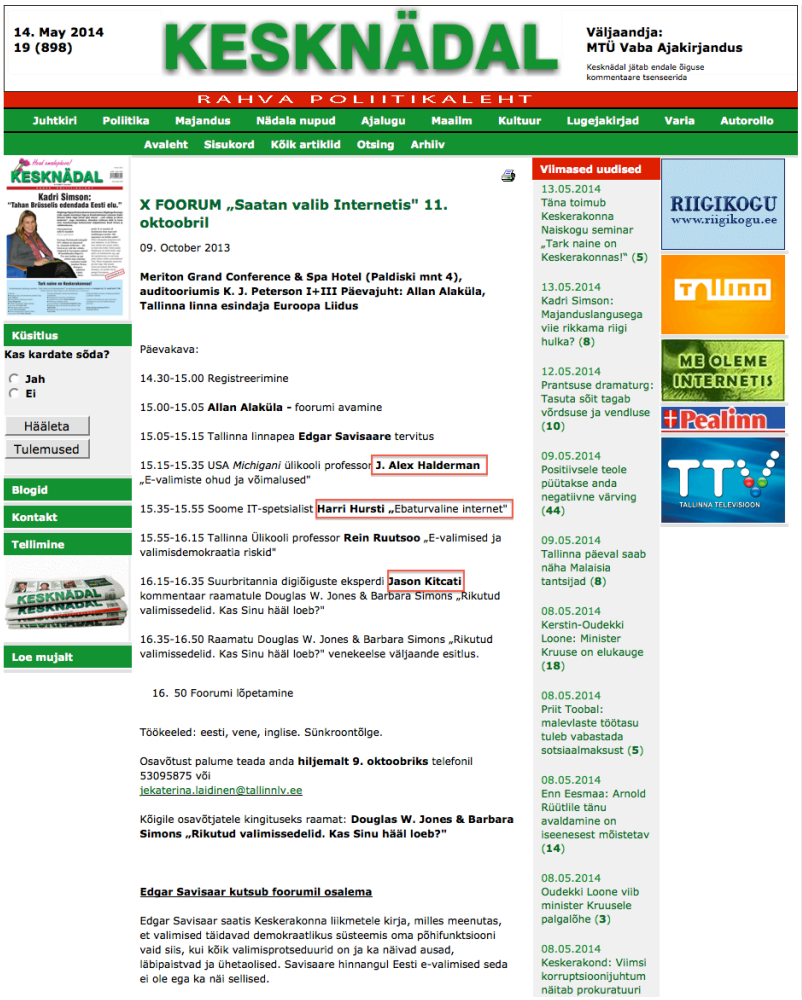
Secure e-voting is impossible in theory (at least that's what they think in America). In practice, computer risks have been eliminated with different measures, from procedures and audits to the 'four eyes principle' of cross checking every step in the process. In Estonia, we've carried out e-voting six times now and haven't had any security incidents yet.

We believe that computer systems are built differently in an e-society. The computer or the software is not trusted; the system that is designed on top of these, the system logs its own operations and is in its turn supervised by people.

Our dear foreign guests also seem to forget this tiny little detail that in the case of e-voting, the network layer, monitoring and logs are under our control and not under the control of an attacker, like it may have seemed in their laboratory.

Research

Harri Hursti introduced himself as **an independent** security expert at the press conference of 12 May. He's not really that independent, is he? He has twice taken part in election events of the Tallinn City Government called "The Devil Votes Online". At the time, the (mostly retirement-age) people who attended the events also failed to understand why the online elections in Estonia are compared to some foreign electronic voting process or why election kiosks are mentioned.



14. May 2014
19 (898)

KESKNÄDAL

Väljaandja:
MTÜ Vaba Ajakirjandus

Kesknädal jätab endale õiguse kommentaare tsenseerida

RAHVA POLIITIKALEHT

Juhtkiri | Poliitika | Majandus | Nädala nupud | Ajalugu | Maailm | Kultuur | Lugejakirjad | Varia | Autorollo

Avaleht | Sisukord | Kõik artiklid | Otsing | Arhiiv

Küsitlus
Kas kardate sõda?
Jah
Ei
Hääleta
Tulemused

Blogid
Kontakt
Tellimine
Loe mujalt

X FOORUM „Saatan valib Internetis" 11. oktoobril

09. October 2013

Meriton Grand Conference & Spa Hotel (Paldiski mnt 4), auditooriumis K. J. Peterson I+III Päevajuht: Allan Alaküla, Tallinna linna esindaja Euroopa Liidus

Päevakava:

14.30-15.00 Registreerimine

15.00-15.05 **Allan Alaküla -** foorumi avamine

15.05-15.15 Tallinna linnapea **Edgar Savisaare** tervitus

15.15-15.35 USA *Michigani* ülikooli professor **J. Alex Halderman** „E-valimiste ohud ja võimalused"

15.35-15.55 Soome IT-spetsialist **Harri Hursti** „Ebaturvaline internet"

15.55-16.15 Tallinna Ülikooli professor **Rein Ruutsoo** „E-valimised ja valimisdemokraatia riskid"

16.15-16.35 Suurbritannia digiõiguste eksperdi **Jason Kitcati** kommentaar raamatule Douglas W. Jones & Barbara Simons „Rikutud valimissedelid. Kas Sinu hääl loeb?"

16.35-16.50 Raamatu Douglas W. Jones & Barbara Simons „Rikutud valimissedelid. Kas Sinu hääl loeb?" venekeelse väljaande esitlus.

16. 50 Foorumi lõpetamine

Töökeeled: eesti, vene, inglise. Sünkroontõlge.

Osavõtust palume teada anda **hiljemalt 9. oktoobriks** telefonil 53095875 või jekaterina.laidinen@tallinnlv.ee

Kõigile osavõtjatele kingituseks raamat: **Douglas W. Jones & Barbara Simons „Rikutud valimissedelid. Kas Sinu hääl loeb?"**

Edgar Savisaar kutsub foorumil osalema

Edgar Savisaar saatis Keskerakonna liikmetele kirja, milles meenutas, et valimised täidavad demokraatlikus süsteemis oma põhifunktsiooni vaid siis, kui kõik valimisprotseduurid on ja ka näivad ausad, läbipaistvad ja ühetaolised. Savisaare hinnangul Eesti e-valimised seda ei ole ega ka näi sellised.

Viimased uudised
13.05.2014 Täna toimub Keskerakonna Naiskogu seminar „Tark naine on Keskerakonnas!" (5)
13.05.2014 Kadri Simson: Majanduslangusega viie rikkama riigi hulka? (8)
12.05.2014 Prantsuse dramaturg: Tasuta sõit tagab võrdsuse ja vendluse (10)
09.05.2014 Positiivsele teole püütakse anda negatiivne värving (44)
09.05.2014 Tallinna päeval saab näha Malaisia tantsijad (8)
08.05.2014 Kerstin-Oudekki Loone: Minister Kruuse on elukauge (18)
08.05.2014 Priit Toobal: malevlaste töötasu tuleb vabastada sotsiaalmaksust (5)
08.05.2014 Enn Eesmaa: Arnold Rüütlile tänu avaldamine on iseenesest mõistetav (14)
08.05.2014 Oudekki Loone viib minister Kruusele palgalõhe (3)
08.05.2014 Keskerakond: Viimsi korruptsioonijuhtum näitab prokuratuuri

TallinnaTV
Esileht | LV Pressikonverentsid | Kava | Arhiiv

Kava E·T·K·N·R·L·P
Kolmapäev 14.05.14
00:10 Poolkuu. Igor Grätzin*
00:40 TeleChat
07:00 Info TV
08:00 TÄNA. Uudised*
08:30 Europarlamendi valimised 2014*
09:00 Draamaseriaal. Keelatud armastus. Otse südamesse 37/142(Verbotene Liebe/Straight to Your Heart)*
09:45 Nädal Pealinnas*
10:00 Gordioni sõim*
10:30 TÄNA. Uudised*
11:00 Heeroldi jutud 2/4*
11:30 Linnaruumi arhiivist. Linnahall
12:00 OTSE: LV Pressikonverents
12:30 Mõtleme taas*
13:00 Poolkuu. Igor Grätzin*
13:30 Europarlamendi valimised 2014*
14:00 Kas tohib? Yana Toom*
14:30 Kinnisvaraveeb
16:15 Nädal Pealinnas*
16:30 Mõtleme taas*
17:00 Poolkuu. Igor Grätzin*
17:30 LV Pressikonverents*
18:00 TÄNA. Uudised

Poliitika õhtukool. Harri Hursti e-valimistest 1. osa - 13.05.2013

Harri Hursti põrmustab e-valimised, tuues välja ohud, millest on seni vaikitud - ohud, mis varitsevad sidekanalites ja operatsioonisüsteemides.

Tweet 0 | Jaga | Lisa video

Jason Kitcat and Alex Halderman are well known for having been against e-, I- and any other non-paper elections for at least five years, if not longer. Back in 2011, Halderman already taught a university course whose message was: society is not yet ready for e-elections. That’s exactly

the case in the US. But this objection cannot be automatically applied to Estonia. We really do understand that the Americans are disappointed in their voting kiosks, we really do understand that they want to fight against kiosk elections in their own country… But perhaps they could have this fight without trampling all over the small country of Estonia in the process, because we have managed to solve this task perfectly for ourselves? True, in slightly different cultural conditions.

The experience has certainly proven to be interesting for the two students in the team: they were able to play with the world's best online voting system in their lab and then get sent on a holiday to that country.

To be honest, the quality of the videos uploaded on Jason's website, as a training material, are ridiculous. If students at the Estonian IT College had created something like this for their homework, they would've received an F.

But about the video: We see something like a server with three sparkling diodes on the table and there are messages in a foreign language (that the students don't understand) running across the screen. There is some activity without any commentary, things are selected from the menus displayed on the screen, some discs are inserted into the server, etc. People in dark appear scurrying around the computers, moving the VGA cable between the projector and the server back and forth so that the projector blinds the camera.

Compare this to the 3-minute lock bumping video on YouTube. Could you open the lock after watching the video? Now watch Kitcat's almost 12-minute video and answer this question: could you break into the Estonian online voting system after this? I'm sure that your answer is "No".

The most important thing is that the promised PDF summary has still not been uploaded on Jason's site. Apparently, it still needs some editing and there're a couple of more things that need to be added and the summary will only be presented after the elections!

Update: Full report was published on May 17 2014.

To me, it looks more like an attempt to rig the elections by scaremongering than a piece of research or responsible disclosure of an actual security hole.

The glad news is that the Estonian online voting system is still secure and we can use it to vote again in a couple of days. We're grateful to our foreign guests for these little crumbs that will help us make the e-voting procedure even better in the future. Those of you who suspect a computer virus at home – do make sure you head your polling station on the day of the elections!

We have the only functioning nationwide e-voting system in the world! Let's be proud!

Anto Veldre

Independent Panel on

Internet Voting

BRITISH COLUMBIA

Recommendations Report to the Legislative Assembly of British Columbia

February 2014

Independent Panel on
Internet Voting
BRITISH COLUMBIA

PO Box 9275 Stn Prov Govt, Victoria, BC, V8W 9J6
Enquiries: 250-387-5305 or Toll-free at 1-800-661-8683
Email: info@internetvotingpanel.ca
Website: internetvotingpanel.ca

February 12, 2014

Honourable Linda Reid
Speaker of the Legislative Assembly
Room 207
Parliament Buildings
Victoria, B.C. V8V 1X4

Dear Madame Speaker:

I have the honour to submit the Recommendations Report to the Legislative Assembly of British Columbia – February 2014.

This report is filed in accordance with section 13(1)(d) of the *Election Act*.

Respectfully submitted,

Keith Archer, Ph.D.
Chief Electoral Officer
British Columbia
Chair, Independent Panel on Internet Voting

Independent Panel on
Internet Voting
BRITISH COLUMBIA

PO Box 9275 Stn Prov Govt, Victoria, BC, V8W 9J6
Enquiries: 250-387-5305 or Toll-free at 1-800-661-8683
Email: info@internetvotingpanel.ca
Website: internetvotingpanel.ca

February 12, 2014

Members of the Legislative Assembly of British Columbia,

Beginning in September 2012, the members of the Independent Panel on Internet Voting reviewed best practices with respect to Internet voting in other jurisdictions and examined issues associated with implementing Internet voting for provincial or local government elections in British Columbia.

A Preliminary Report was made available on the panel's website (internetvotingpanel.ca) for a six-week public comment period from October 23 to December 4, 2013. The panel reviewed the commentary on Internet voting and the Preliminary Report, including additional submissions from experts, academics and vendors in the Internet voting community.

The following *Recommendations Report to the Legislative Assembly of British Columbia – February 2014* expresses the panel's conclusions and recommendations. In developing the report, the panel focused much of its effort on evaluating the benefits and challenges of implementing Internet voting in British Columbia. The report includes a summary of the panel's assessment of those benefits and challenges and a summary of lessons learned from other jurisdictions.

The report also contains a number of appendices, a list of references, and case studies of the experiences with Internet voting in other jurisdictions. A complete bibliography of the materials reviewed and considered is included on the panel's website.

The panel thanks everyone who participated in the public process and for taking the time and effort to engage in the important discussion. All panel members concur with the conclusions and recommendations detailed in this report.

Dr. Keith Archer, Chair

Dr. Konstantin Beznosov

Lee-Ann Crane

Dr. Valerie King

George Morfitt, FCA

CONTENTS

1.0 EXECUTIVE SUMMARY 1
1.1 Conclusions and recommendations 1

2.0 INTRODUCTION 6
2.1 The Independent Panel on Internet Voting 6
2.2 The work of the panel 7
2.3 Voting in local and provincial government elections . . 9

3.0 INTERNET VOTING: DEFINITION AND SCOPE 11

4.0 PERCEIVED AND ACTUAL BENEFITS OF INTERNET VOTING . . 12
4.1 Increase voter turnout 12
4.2 Increase accessibility and convenience 13
4.3 Improve speed and accuracy of results 15
4.4 Cost savings of administering Internet voting over in-person voting 17
4.5 Require fewer resources of parties and candidates . . 19
4.6 Reduce/eliminate errors made by voters when casting ballots . 20
4.7 Maintain relevance by keeping up with other aspects of society . 20
4.8 "Greener" 21

5.0 PERCEIVED AND ACTUAL CHALLENGES TO IMPLEMENTING INTERNET VOTING 22
5.1 Security 22
5.2 Compromised election results 26
5.3 Accessibility, usability and availability 27
5.4 Authentication and ballot anonymity 28
5.5 Secrecy of the ballot 31
5.6 Transparency and auditability 33
5.7 Trust 37
5.8 Stakeholder management 38
5.9 Cost 39

6.0 SUMMARY 41
6.1 Perceived and actual benefits 41
6.2 Perceived and actual challenges 42

7.0 EXPERIENCE WITH INTERNET VOTING IN OTHER JURISDICTIONS . 45
7.1 Lessons learned for B.C. 45

8.0 RECOMMENDATIONS 47

APPENDIX A - CONVENING THE PANEL 50

APPENDIX B - PANEL MEMBERS 54

APPENDIX C - EXPERT PRESENTERS 57

APPENDIX D - QUESTIONS TO INTERNET VOTING VENDORS . . . 58

APPENDIX E - REFERENCE LIST 60

APPENDIX F - EXPERIENCE WITH INTERNET VOTING IN OTHER JURISDICTIONS 73

Canada - Implemented 73

Canada - Investigated and rejected 78

Other jurisdictions - Implemented 82

Other jurisdictions - Investigated and rejected 95

APPENDIX G - GLOSSARY 100

1.0 EXECUTIVE SUMMARY

The Independent Panel on Internet Voting (the panel) was formed by the Chief Electoral Officer on August 9, 2012, following an invitation of the B.C. Attorney General, to examine opportunities and challenges related to the potential implementation of Internet-based voting as a channel of voting for provincial or local government elections in British Columbia. The panel, comprised of the Chief Electoral Officer and four additional members, met 13 times between September 2012 and October 2013. In that time the panel reviewed the existing and evolving literature and spoke to a variety of experts in the fields of technology, Internet security and electoral administration. The panel examined research on both the benefits of and challenges to implementing Internet voting and heard from experts strongly in favour of and strongly opposed to the idea of implementing Internet voting in British Columbia.

A report outlining the panel's preliminary conclusions and recommendations was made available for public comment between October 23, 2013 and December 4, 2013. The panel heard from over 100 individuals and from experts in the field of Internet security, vendors of Internet voting technologies, and groups representing persons with disabilities. At the conclusion of the public input period, the panel met an additional two times to consider the input and produce this report. The public input largely reaffirmed the panel's thinking as expressed in the preliminary report.

This report is intended to provide the Legislative Assembly with a review and assessment of the prospects for Internet voting in British Columbia. It is intended that Members of the Legislative Assembly will use this report to become informed regarding the concepts, principles and arguments made both for and against implementing Internet voting at either the local or provincial government level.

1.1 Conclusions and recommendations

The panel concludes that Internet voting has the potential to provide some benefits for administering local government elections and provincial elections in British Columbia and that the most significant potential benefit of Internet voting is increased accessibility and convenience for B.C. voters. Other presumed benefits, such as increased turnout and lower cost are not typically realized.[1]

The panel also concludes that Internet voting has some significant inherent risks. It is important to understand that although the Internet is used for an increasing number of interactions (such as banking, shopping, dating, planning trips, and the like) with their own risks, voting over the Internet has a set of unique challenges that inevitably introduce a number of additional risks. The extent to which each of these risks can be mitigated or eliminated also depends on the details of the way in which an Internet voting model is implemented. Security at the voter's device,[2] reduced transparency and

1 For more on the potential benefits of implementing Internet voting, see 4.0 Perceived and actual benefits of Internet voting, page 12

2 References in this report to the voter's "device" can be read as any means by which an individual could cast a ballot for Internet voting (e.g., computer, tablet, smartphone)

auditability compared to traditional voting methods, and cost were seen by the panel to be the most significant challenges to implementing Internet voting for either local government or provincial government elections.[3]

While Internet voting has been investigated by various jurisdictions around the world over the past fifteen years, it is still not widely implemented. Internet voting is used in only a limited number of jurisdictions, and only on a limited basis.

Weighing the benefits and challenges to implementing Internet voting in specific circumstances is the role of policy-makers. There is a high level of trust in the current voting processes used at the local and provincial government levels, but there are opportunities for improvement in each. The panel believes that Internet voting has the potential to be an additional voting channel for voters with specific accessibility challenges in future local or provincial government elections, provided that the recommendations outlined in this report are followed and any system implemented complies with the principles established by the panel. The panel believes it is not feasible for this to occur in time for the 2014 local government elections.

To guide members of the Legislative Assembly, and potentially local government officials, in their task of weighing the benefits and risks of Internet voting, the panel sets forth the following recommendations:

1. **Do not implement universal Internet voting for either local government or provincial government elections at this time. However if Internet voting is implemented, it should be limited to those voters with specific accessibility challenges. If Internet voting is implemented on a limited basis, jurisdictions need to recognize that the risks to the accuracy of the voting results remain substantial.**

   The risks of implementing Internet voting in British Columbia outweigh the benefits at this time. Therefore it is premature to implement Internet voting on a universal basis.

   Because of the strengths of Internet voting to provide increased accessibility for certain segments of the population (e.g., remote voters, voters with disabilities and voters who would otherwise need assistance to vote), Internet voting could be used in the future on a limited basis to improve access to the ballot for these groups. There are significant risks to implementing Internet voting that can jeopardize the integrity of an election, no matter the extent of implementation. If Internet voting is to be used in British Columbia in the future, the following three recommendations must be adhered to, including all of the principles outlined in recommendation #4.

3 For more on the challenges to implementing Internet voting, see 5.0 Perceived and actual challenges to implementing Internet voting, page 22

2. **Take a province-wide coordinated approach to Internet voting.**

   If Internet voting is to be implemented at either the local government or provincial government level, election administrators should work with each other and with the provincial government to conduct a more rigorous review of the options, establish a common framework for implementation and retain control and oversight over election administration during implementation.

3. **Establish an independent technical committee to evaluate Internet voting systems and support jurisdictions that wish to implement approved systems.**

   Provincial and local government election administrators do not have the necessary technical expertise in-house to properly evaluate, verify and test high security systems such as Internet voting systems. A technical committee independent from vendors, political parties, and elected representatives, and made up of election administrators and recognized experts in Internet voting, cryptography, and computer security should be established to support the province-wide coordinated approach. The technical committee would be established by, and would report to, the B.C. Chief Electoral Officer. Such a reporting structure would emphasize the technical committee's independence. Such a committee would have to stay abreast of changes in available and emerging technology in order to establish standards and requirements that would have to be met by any Internet voting system to be used in British Columbia. The committee would also be responsible for overseeing a rigorous review of any system being considered for use against those standards and requirements to ensure high security. Only Internet voting systems approved by the technical committee should be authorized for use in B.C. jurisdictions. The technical committee would also be responsible for monitoring the security of the systems while in use and conducting a full audit and evaluation afterwards. The work of the technical committee should be made public to ensure transparency and to build trust in any system implemented.

4. Evaluate any Internet voting system against the principles established by the panel.

While acknowledging that there will be unique factors to consider in each jurisdiction, the panel recognizes the benefit of establishing a common, or at least similar, set of principles that can be used by multiple jurisdictions in Canada to evaluate Internet voting. There is a growing consensus among election administrators of what these principles are. The panel used the eight principles established by Elections Ontario in its Alternative Voting Technologies Report[4] as a starting point from which to develop principles for British Columbia. Many of the principles outlined below share common elements with Elections Ontario's principles, but some have been amended to reflect a B.C. context or for consistency with the language used in this report. These principles must be met in addition to any standards a technical committee would establish.

Accessibility

The Internet voting process must be readily available to, and usable by, all voters eligible to vote by Internet voting, even in the presence of Internet voting-specific threats.

Ballot anonymity

The voting process must prevent at any stage of the election the ability to connect a voter and the ballot(s) cast by the voter.

Individual and independent verifiability

The voting process will provide for the voter to verify that their vote has been counted as cast, and for the tally to be verified by the election administration, political parties and candidate representatives.

Non-reliance on trustworthiness of the voter's device(s)

The security of the Internet voting system and the secrecy of the ballot should not depend on the trustworthiness of the voter's device(s).

One vote per voter

Only one vote per voter is counted for obtaining the election results. This will be fulfilled even in the case where the voter is allowed to cast their vote on multiple occasions (in some systems, people can cast their vote multiple times, with only the last one being counted).

4 Reference #292

Only count votes from eligible voters

The electoral process shall ensure that the votes used in the counting process are the ones cast by eligible voters.

Process validation and transparency

The procedures, technology, source code, design and implementation details, and documentation of the system must be available in their entirety for free and unconstrained evaluation by anyone for testing and review for an appropriate length of time before, during and after the system is to be used. Policies and procedures must be in place to respond to issues that arise. Appropriate oversight and transparency are key to ensuring the integrity of the voting process and facilitating stakeholder trust.

Service availability

The election process and any of its critical components (e.g., voters list information, cast votes, voting channel, etc.) will be available as required to voters, election administrators, observers or any others involved in the process. If Internet voting should become unavailable or compromised, alternative voting opportunities should be available.

Voter authentication and authorization

The electoral process will ensure that before allowing a voter to cast a vote, that the identity of the voter is the same as claimed, and that the voter is eligible to vote

2.0 INTRODUCTION

2.1 The Independent Panel on Internet Voting

Three key developments led to the forming of the Independent Panel on Internet Voting:

- March 2011 – The City of Vancouver requested approval from the Minister of Community, Sport and Cultural Development to use Internet voting for the November 2011 local government elections. The request was not granted and the 2011 Local Government Elections were held in the traditional manner.
- August 2011 – Elections BC submitted *Discussion Paper: Internet Voting* to the Legislative Assembly to further public dialogue on the topic.
- November 2011 – The Chief Electoral Officer submitted to the Legislative Assembly the Report of the Chief Electoral Officer on Recommendations for Legislative Change. Of the four recommendations in the report, one was entitled Trialing New Voting Technologies and suggested that "legislators may wish to consider providing greater flexibility to the Chief Electoral Officer to introduce, on a pilot basis, a variety of new voting technologies." This recommendation was intended to cover a host of technologies including, but not limited to, Internet voting and to increase the possibilities for further detailed assessment of new voting technologies in British Columbia.

On August 7, 2012, the Minister of Justice and Attorney General invited the Chief Electoral Officer to convene a non-partisan panel to review best practices with respect to Internet voting in other jurisdictions and to examine the issues associated with implementing Internet voting in British Columbia. The request included that the panel examine Internet voting in both local and provincial contexts.

On August 9, 2012, the Chief Electoral Officer responded to the Minister of Justice and Attorney General advising that he was pleased to convene and chair such an independent panel and laid out how he would proceed in doing so.

> Authority: convening a panel to research and draft recommendations to the Legislative Assembly is authorized pursuant to section 12(2)(a) of the *Election Act*
>
> Scope: building upon the *Discussion Paper: Internet Voting*, the panel will examine opportunities and challenges related to the potential implementation of Internet-based voting for provincial or local government elections in B.C.
>
> Reporting: the method for gathering input and feedback from experts and the public will be determined by the panel, as will a timeline for reporting

Composition: the Chief Electoral Officer will chair the panel and invite four additional members; members will be drawn from a wide spectrum reflecting expertise in technology, cryptography, Internet security policy, and electoral administration; all members will have a high level of independence and judgment

Secretariat: will be provided by Elections BC

Budget: estimated to be $420,000

2.2 The work of the panel

Upon agreeing to convene and chair the panel, the Chief Electoral Officer proceeded to identify and select panellists who had the required expertise, independence and judgement. On September 10, 2012, the composition of the panel was publicly announced.

Panellists were selected based on their expertise and experience, with an eye to ensuring appropriate gender and geographical distribution. All panellists live and work in B.C. Two are university professors with experience in computer science, computer engineering and computer and network security. One is a local government administrator with experience in elections, and one is a former Auditor General.[5]

The panellists agreed early on that they would undertake to educate themselves about Internet voting so as to be able to make informed recommendations to the Legislative Assembly. On that basis, it was decided that the time line for the panel's work would depend largely on what it learned during the examination period. At the same time, the panellists were aware that local governments were hopeful they would learn the recommendations of the panel in sufficient time to plan for the 2014 local government elections under either outcome.

The panel agreed with the Chief Electoral Officer's response to the Minister of Justice and Attorney General that it would use the Elections BC *Discussion Paper: Internet Voting* as a starting point for determining the scope of its work. The panel wanted to build upon the Discussion Paper and learn more about the benefits and challenges to implementing Internet voting and, as well, learn about the jurisdictions that have investigated and implemented Internet voting, both in Canada and around the world.

At its meetings the panel reviewed some of the academic and practitioner literature on Internet voting, received presentations from experts on a variety of topics and reviewed the actual and perceived benefits and challenges to the implementation of Internet voting. The panel divided its time between reviewing material, listening to presentations, and debating the issues that had been identified.

5 For more information about the panellists, see Appendix B – Panel members, page 54

The panel met monthly between September 2012 and February 2013 before a three month hiatus while the Chief Electoral Officer focused his attention on administering the 2013 Provincial Enumeration and Provincial General Election under the existing election administration model. Prior to taking this break the panel determined that it had gathered much of what it had hoped to learn and that, upon resuming its work after the election, it would conclude its information gathering phase, begin its deliberations, and proceed to produce a preliminary report by the fall with preliminary recommendations for public distribution and feedback.

The preliminary report provided the public with a research summary of both the benefits and challenges to implementing Internet voting for provincial or local government elections in British Columbia, and outlined the panel's preliminary conclusions and recommendations. The preliminary report was available on the panel's website (internetvotingpanel.ca) beginning on October 23, 2013 and the panel invited public comment from B.C. residents. Input could be submitted to the panel by the panel website, email address and traditional mail for a six week period concluding December 4, 2013.

During that period the panel received input from over 100 individuals from across British Columbia. Of the comments in favour of Internet voting, common themes included: the potential for increased convenience and the removal of barriers for people with accessibility challenges; the need for voting to keep up with an increasingly digital lifestyle; and anecdotal evidence that Internet voting would lead to increased voter turnout. Of the comments opposed to Internet voting, common themes included: concerns about Internet security generally and the potential for compromised election results because of security challenges; a lack of trust in results that aren't scrutinized in the traditional manner; and a feeling that if Internet voting won't improve voter turnout, it is not worth the risk.

In addition to comments from B.C. residents, the panel also received input from experts in the field of Internet security outside of B.C, as well as from vendors of Internet voting technologies, and groups representing persons with disabilities in B.C.

It cost approximately $150,000 to administer the Independent Panel on Internet Voting.

2.3 Voting in local and provincial government elections

Given the mandate to examine the suitability of Internet voting for both local and provincial government elections, early in the life of the panel the members sought to develop a clear understanding of the existing voting processes used in British Columbia. The panel invited staff of Elections BC and the Ministry of Community, Sport and Cultural Development to brief it on the universal standards for democratic elections and explain to it how they are met in legislation and in practice.[6] The staff also informed the panel about the voting model used at each level of government and the various voting opportunities currently in place. Ministry staff emphasized to the panel that each local government was responsible for the administration of elections in its jurisdiction and, as such, the elections are not administered precisely the same way in each. The following table summarizes the information contained in those presentations:

	Local government elections	Provincial elections
Frequency	Every 3 years (general elections); As required (by-elections, other voting)	Every 4 years (general elections); As required (by-elections, referenda)
Elected offices	▪ Municipal (mayor, councillors) ▪ Regional District (electoral area directors) ▪ Parks boards ▪ School boards (trustees) ▪ Islands Trust	▪ Legislative Assembly (Members of the Legislative Assembly)
Number of positions filled	~1,650 individuals to ~250 government bodies	85 individuals to 1 government body
Administered by	~190 local governments (Chief Election Officer appointed by council or board)	Elections BC (Chief Electoral Officer appointed by Legislative Assembly)
Budget set by	Local governments	Elections BC
Funded by	Local governments	Province
Legislative framework (primary)	*Local Government Act, Vancouver Charter*	*Election Act, Referendum Act*
Legislation covers	Election administration Candidate nominations Conduct of voting Conduct of counting Campaign finance rules Election offences Invalid election procedures	
Voters list used	Subset of provincial voters list; OR Own voters list; OR No voters list (election day registration only)	Provincial list of registered voters, updated on a continuous basis from various sources

6 References #283, 284, 285

Voter registration by telephone or Internet	No	Yes
Voter registration on voting day	Yes	
General Voting Day	Consistent across province	
Advance voting	1 day (consistent across province); 1 additional day for communities over 5000 (day and time set by local government); Additional days at discretion of local government	4 days (consistent across province)
Vote by mail	At discretion of local government	Required
Other voting opportunities	At discretion of local government (special voting opportunities in hospitals, long-term care facilities, or other places where an elector's mobility may be impaired)	At the district electoral office; At any other provincial voting opportunity in the province
Vote by telephone or Internet	No	
Qualifications to vote	Resident elector: ▪ Canadian citizen ▪ 18 years of age or older ▪ Resident of the jurisdiction where you intend to vote for at least 30 days ▪ Resident of B.C. for at least six months ▪ Registered as a voter ▪ Not disqualified by law from voting **OR** Non-resident property elector: ▪ Canadian citizen ▪ 18 years of age or older ▪ Have owned property in the jurisdiction where you intend to vote for at least 30 days ▪ Resident of B.C. for at least six months ▪ Registered as a voter ▪ Not disqualified by law from voting	▪ Canadian citizen ▪ 18 years of age or older ▪ Resident of the electoral district ▪ Resident of B.C. for at least six months ▪ Registered as a voter ▪ Not disqualified by law from voting
Frequency of by-elections	Varies (e.g. 19 by-elections in 2012)	Varies (e.g. two by-elections in 2012)
Frequency of other voting	Varies	Varies (referendum held in conjunction with general elections in 2005 and 2009, stand-alone mail-based referendum in 2011)

3.0 INTERNET VOTING: DEFINITION AND SCOPE

Internet voting refers to a voting method "where votes are transferred via the Internet to a central counting server".[7]

Internet voting can be further separated into on-site Internet voting and remote Internet voting. On-site Internet voting is conducted at controlled settings such as voting places or kiosks established in high-traffic areas where election officials may be available to authenticate voters and ensure the integrity of the device and software used by voters to vote in private. Remote Internet voting allows voters to cast their ballot from any Internet connection to which they have access, such as a home computer or smartphone.

The Independent Panel on Internet Voting limited the scope of its work to remote Internet voting. Accordingly, both on-site Internet voting and the use of electronic voting and counting machines in the voting place were out of scope.

Internet voting conducted on supervised machines in the voting place could be considered to be a step towards familiarizing voters and election administrators with processes and technology for eventual remote Internet voting. However, on-site Internet voting in the voting place would not provide any accessibility or convenience benefits for voters who would still need to attend the voting place, and does not address many of the security concerns related to Internet voting.

Throughout this report, references to Internet voting should be read as *remote* Internet voting unless otherwise specified.

While Internet voting can, and is, used for some non-governmental elections such as for student groups, trade unions and professional organizations, references to Internet voting in this report are limited to its use in governmental elections.

The purpose of the panel was not to evaluate a particular technology or process for use in B.C. The implementation of Internet voting differs from one jurisdiction to the next. Whether due to differences in public policy, legislation, existing voting processes or the technology chosen by the jurisdiction, there is no common practice for what Internet voting looks like when implemented. Therefore the panel chose to consider many of the ways Internet voting has been implemented to determine if Internet voting in some form could be appropriate for use in British Columbia.

7 Reference #130

4.0 PERCEIVED AND ACTUAL BENEFITS OF INTERNET VOTING

A significant amount of research has been conducted into the benefits of Internet voting, but the research community and stakeholders do not agree on a common list of benefits or a ranking of their relative importance.

In a particular jurisdiction an issue may or may not be a benefit, and could even be seen as a challenge, depending on the perspective of the stakeholder and the specific implementation of Internet voting being considered. Across jurisdictions there is even more disagreement as to whether a perceived benefit of Internet voting can be realized in practice.

The panel chose to examine all of the perceived benefits mentioned in the literature and evaluate for itself what actual benefits could be realized in B.C. by implementing Internet voting for either local or provincial government elections.

4.1 Increase voter turnout[8]

Academic publications suggest that, since the 1970s, citizens in Western democracies have been taking up the act of voting at later points in their life and in smaller numbers, and accordingly overall voter turnout has dropped from approximately three-quarters of eligible voters in the 1970s to approximately half of eligible voters today. In the 2013 Provincial General Election overall turnout was 55.3% of eligible voters, but only 29.9% of eligible voters aged 18-24 chose to vote.[9] At the local government level turnout is also trending down, but to an even lower level. In the 2011 B.C. Local Government Elections, voter turnout averaged 29.6%.[10]

Internet voting is seen by some as a potential solution to this trend of declining voter turnout. It is often claimed that individuals who are not motivated to attend a voting opportunity in their community in person would vote online if given the opportunity. However, political science research into jurisdictions that have implemented Internet voting is more sceptical.

While there have been some Internet voting elections where voter turnout has increased, when other factors such as the apparent closeness of the race and interest in particular contests (e.g., a mayoral election without an incumbent) are taken into consideration, research suggests that Internet voting does not generally cause non-voters to vote. Instead, Internet voting is mostly used as a tool of convenience for individuals who have already decided to vote.

8 For more information on this matter, see references #48, 60, 75, 131, 145, 152, 157, 164, 207, 208, 215, 216, 275, 276
9 Reference #336
10 Reference #228

Some proponents argue that the novelty factor provided by Internet voting leads to voters paying increased attention to otherwise lower interest elections, particularly at the local government level. However, research suggests this increased attention may be limited to the first instances of Internet voting before returning to more typical levels.

Researchers have also looked at the demographics of Canadian voters who have used Internet voting and have found that Internet voting is most popular among middle-age voters and least popular among youth and therefore reflects traditional voter turnout demographics. These findings run contrary to the widely expressed belief that Internet voting will lead to increased participation by youth.

Conclusion

The evidence for Internet voting to lead to increased voter turnout in British Columbia elections appears to be at best mixed, and the panel is not convinced that introducing Internet voting in British Columbia will result in increased voter turnout at either the local or provincial government level in the long run.

4.2 Increase accessibility and convenience[11]

The next most popular potential benefit of Internet voting among proponents is its ability to make voting more convenient and increase the accessibility of the electoral process for those who do choose to vote. Unlike increasing turnout among voters, increasing the accessibility of the process is more in line with the perceived or legislated responsibilities of election administrators.

Under the current provincial voting model, voters have many opportunities to vote outside of their assigned voting place near their home. The provincial absentee voting rules allow a voter to cast a ballot at the local office of the District Electoral Officer, at any voting location in the province, or by requesting a ballot be mailed to them (vote by mail). While the multitude of absentee voting provisions address individuals' absence from their community or the province, it still requires a voter to either travel to a voting place in the province or request, receive and mail back a ballot. Mailing ballots back and forth takes time, which places notable constraints on voters in remote areas or foreign countries. In 2013, approximately one-third of voting packages requested were not returned to Elections BC on time, or at all.[12] Beginning in 2013, Elections BC will mail a write-in ballot to voters up to 30 days before Writ Day for a fixed-date general election, but voters must still wait to mark their ballot until after the writ of election is issued and must mail it back so that it is received before the close of voting on general voting day (28 days after the writ of election is issued).

11 For more information on this matter, see references #48, 131, 136, 142, 144, 146, 194, 204
12 Reference #335.

In 2013, voting packages that were sent to international addresses before Writ Day were returned at a rate significantly higher than those that were sent after Writ Day (60% compared to 38%). Local governments that choose to offer vote by mail are limited to a three week window in which the ballot must be requested, mailed to the voter, marked and mailed back so that it is received by the legislated deadline.

Internet voting could enable voters that currently rely on the vote by mail process to have better access to the ballot and provide these voters with greater certainty that their ballot will be received by the election administration before the close of voting.

As there are fewer absentee voting options at the local government level in B.C. and vote by mail is only offered in some communities, an Internet voting option has the potential to benefit these absentee local government voters.

Providing voters with the opportunity to vote without travelling to a voting place can lower both the financial and time cost of voting. For example, the incremental financial cost to a voter casting an Internet ballot is likely to be less than that for an individual voting in person after having taken time off work, travelling to a voting place, and extending the hours required for child care. Similarly, while the act of voting in person typically takes only five minutes[13] after arrival at the voting place, casting a ballot online would likely be faster than the total amount of time spent planning a change to an existing schedule, travelling to a voting place, casting a ballot and returning home.

In many jurisdictions offering internet voting, it has been offered around the clock during the applicable voting period rather than limited to traditional voting hours. This enables voters to choose to vote at the time most convenient for them.

Local government elections are held on the third Saturday in November every three years. In many communities in B.C., the snow and other bad weather common at that time of year can make it difficult for voters to attend in-person to vote. While local governments in B.C. are petitioning the provincial government to move general voting day up to October, introducing Internet voting would lower the risk of voters in these communities being unable to vote due to seasonal inclement weather. As provincial general elections are held in May, this is less of an issue for provincial voters.

Another benefit of Internet voting is that it has the potential to allow voters with disabilities[14] additional opportunities to vote independently using technology they already have access to and are familiar with. Some Internet voting systems can vary the format of the ballot to meet the needs of individual voters with respect to font sizes, languages, etc. While provincial and local government voters in hospitals and long term care facilities are often visited by election officials in person, many voters with special needs outside of these facilities would also benefit from Internet voting.

13 Reference #244
14 E.g. There are an estimated 127,000 sight-impaired British Columbians over the age of 15. Reference #334.

Internet voting could have a significant impact on their ability to vote, and their ability to do so independently. There may also be other potential ways for election administrators to address these challenges (e.g. accessible voting machines in voting places).

Most implementations of Internet voting require voters to be registered to vote prior to casting an Internet ballot, and many require a second level of registration to qualify for Internet voting. Implementations of Internet voting that rely on authentication credentials being mailed to voters ahead of the voting period will not meet the needs of voters who are away from home for extended periods or do not receive home mail delivery.

Conclusion

Increased accessibility and convenience for British Columbia voters is the most significant potential benefit of Internet voting. Given the broader absentee voting opportunities available in the existing provincial electoral process, and considering the seasonal weather constraints for fall local government elections, the panel believes the potential benefits are greater for local government elections, but that they are also significant for provincial elections.

B.C. survey research into voter turnout has identified issues of convenience (e.g., too busy, out of town, family emergencies, illness) as the reason given for not voting by approximately one-third of respondents. This suggests that jurisdictions that offer Internet voting should see a significant increase in turnout over previous elections in those jurisdictions or over other comparable jurisdictions where Internet voting is not used. However, as described earlier in 4.1 - Increase voter turnout, the evidence does not show this.

4.3 Improve speed and accuracy of results[15]

Another commonly held view is that, because ballots are cast and counted electronically under Internet voting, tabulation with perfect accuracy is near instantaneous once voting closes. However, this perceived benefit is not always realized in Internet voting elections.

The Internet voting technology used in the 2012 Halifax Regional Municipality (HRM) elections required ballots to be digitally encrypted as they were cast in order to ensure the secrecy of the individual ballot and prevent anyone from being able to determine the results of any Internet ballots cast before the close of voting. After the close of Internet voting,[16] the process to mix[17] the 66,000 ballots took approximately half an hour. Due to the potential delay to the announcement of results if conducted on

15 For more information on this matter, see references #130, 131, 141, 187, 278
16 Internet voting was only available during the advance voting period
17 For more on mixing ballots cast on an Internet voting system, see Norway in Appendix F - Experience with Internet voting in other jurisdictions

election night, HRM chose to conduct this process at the close of Internet voting, ahead of election day, but did not produce the report that would indicate the tally of the votes until after all in-person voting was complete.

Similarly, an Internet voting pilot held in ten of 429 communities during the 2011 Norwegian Local Government Elections found that there was no statistically significant reduction in time required for the counting and reporting of results compared to control communities using traditional counting and reporting methods. While the Norwegian pilot used different technology and processes than HRM, it also found that processes unique to Internet voting meant that tabulation could not begin immediately upon the close of voting.[18] Further, there was "no relationship between the level of use of Internet voting and the time taken for the counting and results reporting process."[19] That is, contrary to expectations, even where Internet ballots were a higher proportion of all ballots cast, there was not a corresponding decrease in the amount of time it took for all ballots to be counted.

Although the time required to count and report results is not improved, the accuracy of counting and reporting can be.

While the provincial election ballot is fairly simple, election officials can sometimes make errors in the adjudication, counting and reporting of the several hundred ballots in their ballot box after administering voting for twelve hours. The complexity of the ballots used in local government elections compounds this issue. Internet voting enables a standard adjudication of ballots and precludes a potential variation between officials (anywhere from a few in a small local government community to thousands for a provincial election) and eliminates human error in counting, particularly when there are multiple ballots for officials to count or complex ballots are used. However, experience from provincial recounts shows a very low level of errors due to ballot adjudication and counting. For example, a recount in the electoral district of Saanich North and the Islands following the 2013 General Election found that only 13 of 31,697 ballots were adjudicated differently between the two counts, or were miscounted at the initial count.[20] Election administrators at both the local and provincial levels have a high level of confidence in the accuracy of current manual counting processes.

18 If a voter casts a ballot in-person it supersedes a ballot cast online, so Internet ballots could not be counted until it was determined that the voter did not vote in-person on election day. Dealing with ballot encryption also delayed the start of the Norwegian tallying. Reference #141.

19 Reference #141

20 Reference #256

The major speed issue in provincial elections relates to the gap between the initial count on election night and the release of the official results. Local government officials must release the official results by the end of the fourth day after general voting day. In B.C. provincial elections there is a legislated period of 13 days between the initial count and the beginning of the final count in which to process and count absentee ballots; such ballots may be cast until the close of voting on general voting day.[21] This additional time at the provincial level is required to ensure no multiple voting occurs under the current voting model. An Internet voting model added as an additional channel to the current system would not produce an earlier result.

Conclusion

Jurisdictions that have introduced Internet voting have had mixed results in terms of the speed in which results are available. At both the provincial and local government levels, preliminary results are typically available between thirty minutes and three hours after the close of voting. In local government jurisdictions where vote tabulation machines are already in use, results can be available even sooner. The panel feels that the existing speed and accuracy of results sufficiently meet the needs of voters, candidates, political parties and the media. Further, even if Internet voting results could be made available sooner, overall results for any election would still need to wait for the majority of votes that are cast on paper ballots to be counted by hand according to the traditional timeline.

While a standard adjudication of ballots could be an improvement, the panel trusts the accuracy of the existing manual counting processes.

The panel does not find the potential benefit of improved speed and accuracy of ballot counting, of itself, to be a compelling reason for the introduction of Internet voting as an additional channel at either the provincial or local government levels.

4.4 Cost savings of administering Internet voting over in-person voting[22]

For the 2013 Provincial General Election the cost of hiring election officials and renting voting places represented just over one-third of the total cost of administering the election. It is commonly advanced that Internet voting does not require the renting of voting places and the hiring of election officials and so a significant cost savings can be found over traditional in-person voting.

21 In both local and provincial government elections there is also a period after the announcement of the official results in which a judicial recount may be requested.
22 For more information on this matter, see bibliography references #76, 130, 131, 279, 337

However, this perceived financial benefit is based on Internet voting being used in place of traditional in-person voting opportunities. With only a few exceptions, jurisdictions that have implemented Internet voting have offered it as an additional channel of voting to supplement existing in-person voting. In these cases all costs associated with Internet voting are in addition to traditional expenses and, as a result, the total cost of administering the election increases.

Some jurisdictions have looked to partially offset the costs of adding Internet voting by reducing the number of in-person voting opportunities. This is because individuals who vote online will not need to attend a voting place and so fewer voting places and officials may be needed. Further, some officials hired may be needed for shorter periods of time as they are not counting ballots after the close of voting. For example, after initial success with Internet voting in 2008 and 2009, Halifax Regional Municipality believed that fewer voters would vote in person and so reduced the number of voting places for the 2012 election from 146 to 102 and the number of voting stations from 600 to 491. Such assumptions need to be carefully considered, as the Ontario City of Peterborough reported after its 2006 pilot that it had overestimated the impact of Internet voting on in-person voting and, accordingly, for the next election would need to hire more election officials for the voting places to reduce the long line-ups that resulted from the reduced staffing.

Internet voting also has the potential to reduce logistics and costs associated with the distribution of ballots and supplies around the jurisdiction. As well, Internet-only voting can facilitate late changes to the ballot to account for the inclusion or exclusion of candidates or political parties.

Conclusion

The panel considered three scenarios for implementing Internet voting having different consequences for the cost of elections.

In the first scenario Internet voting is grafted onto the current voting model as an additional channel. Under this scenario, there would be additional costs.

A second scenario is that as Internet voting is grafted onto the current voting model as an additional channel, the budget for the election is held constant, and the number of traditional voting places is reduced as a cost-saving initiative.

A third option is for a jurisdiction to offer Internet-only voting. This has the potential to provide significant cost savings over the traditional voting model.

The panel is of the view that if any Internet voting option is introduced in B.C., it should be done in a limited manner. Therefore, in the short- to medium-term, the panel believes that Internet voting provides little or no cost savings,

while recognizing that in the longer-term, if an Internet-only voting model were to be used, cost savings are possible. Elections Ontario considered piloting Internet and telephone voting in an Ontario by-election (approximately 85,000 voters) and reported that such a pilot "could cost close to $2 million".[23] British Columbia would have to conduct its own detailed cost assessment of a pilot project should it consider trialing Internet voting at either the local government or provincial level.

The panel does not consider the potential ability to make late changes to the ballot to be a determining factor in the consideration of Internet voting.

The cost of Internet voting is also seen by some to be a potential challenge (rather than a potential benefit) to implementing Internet voting. For further discussion of the issues related to the costs of implementing Internet voting, see Cost on page 39.

4.5 Require fewer resources of parties and candidates[24]

Just as in-person voting requires significant numbers of paid election officials to administer voting, in-person voting also places significant demands on candidates and political parties to find sufficient volunteers to attend the voting places and scrutinize the voting process. As political parties and candidates have increasing difficulty finding sufficient volunteers, the benefit of centralized observation of Internet voting becomes apparent. Instead of recruiting one volunteer for each ballot box in the jurisdiction, political parties and candidates would have to recruit sufficient volunteers and experts to audit the voting system.[25] Internet voting also makes it easier for candidates and political parties to identify in real time who has voted.

Conclusion

If Internet voting were to be the sole channel for voting it would reduce the amount of human resources required by candidates and political parties to scrutinize the electoral process, but if offered as an additional channel to in-person voting, Internet voting would, in fact, require more volunteers with different skills than at present. The panel does not think this is a compelling argument for introducing Internet voting.

23 Reference #232. For more information on Ontario's consideration of Internet voting, see Ontario in Appendix F - Experience with Internet voting in other jurisdictions
24 For more information on this matter, see reference #146
25 For more on the skills required to scrutinize Internet voting see 5.6 Transparency and auditability, page 33

4.6 Reduce/eliminate errors made by voters when casting ballots[26]

Another potential benefit to Internet voting is that technology can be designed to prohibit a voter from casting a ballot that has an error on it; that is, too many or too few candidates selected, unclear markings, or markings that identify the voter. Alternatively, the technology could still allow the voter to cast a ballot with an error to enable them to "spoil" their ballot after warning them that they are doing so.

In the 2013 Provincial General Election, 11,763 of all ballots cast were rejected. This represented 0.65% of the total number of ballots cast. It is not known whether these ballots were spoiled in error through incorrect markings by the voter, or whether they were spoiled by the voter in an effort to provide a statement on the election.

Conclusion

Internet voting has the potential to eliminate errors due to incorrect markings, but has no impact on ballots that are intentionally spoiled. The panel does not find the potential benefit of reducing or eliminating the number of errors made by voters when casting ballots to be a compelling reason for the introduction of Internet voting at either the provincial or local government levels.

4.7 Maintain relevance by keeping up with other aspects of society[27]

As the public becomes accustomed to using the Internet for other aspects of their lives there is an increased expectation that voting should be provided in the same way. Some researchers claim that if the methods for voting do not evolve in a manner similar to shopping, banking, socializing and playing games, voting may be pushed to the margins.

Other researchers have raised the opposite view and have described voting as having a unique role in a democratic society that merits retaining a different and distinctive set of procedures. This view suggests that voting is by definition a very public activity, and that it should occur in a public place, thereby emphasizing the community-based character of political participation. These views are reflected in anecdotal reports of Norwegian youth preferring to vote in person for social reasons.[28]

26 For more information on this matter, see references #48, 141, 146, 205, 338
27 For more information on this matter, see references #141, 231, 280
28 For more on the social preferences of Norwegian youth, see Norway in Appendix F - Experience with Interet voting in other jurisdictions

Some of these researchers also suggest that the actual costs of voting (attending a voting place for a few minutes every few years) are not an overly onerous component of the democratic system.

Conclusion

The panel recognizes the symbolic benefit of Internet voting as a way to maintain or increase the relevance of voting in our increasingly digital lives, but does not consider this benefit to be a significant one for B.C.

4.8 "Greener"[29]

Reducing the amount of paper required to print ballots and the amount of energy to distribute them across the jurisdiction is another perceived benefit of introducing Internet-only voting. Similarly, researchers suggest that Internet voting could also reduce the amount of fossil fuels burned by voters, election officials and scrutineers in travelling to and from the voting place by car or even public transit.

Conclusion

The panel recognizes the perceived potential environmental benefits of Internet voting, but did not evaluate the full environmental costs of Internet voting (including the energy required to power the computer systems and infrastructure) or the traditional voting channels and infrastructure and therefore does not take a position on the relative "greenness" of Internet voting.

29 For more information on this matter, see references #146, 215, 227

5.0 PERCEIVED AND ACTUAL CHALLENGES TO IMPLEMENTING INTERNET VOTING

Perception of the challenges or risks of implementing Internet voting differs among stakeholders. Vendors claim that the challenges have largely been overcome and the risks are minimal, whereas most technical experts state that ongoing concerns related to security are still to be resolved. While the public may desire to vote in a more convenient way, and some election administrators may desire to offer such conveniences, both groups do not always have all of the facts about the challenges of implementing Internet voting.

The kinds of risks involved in Internet voting are largely different from the kinds of risks faced in traditional voting opportunities. The degree of risk and the consequences of those risks also differ and need to be assessed. While there are accepted standards for assessing safety-critical systems generally, to date there is no common methodology for measuring the risks associated with Internet voting.

5.1 Security[30]

The challenge of providing secure Internet voting is perhaps the most significant of all the challenges the panel discussed.

In July 2013, a large group of notable American computer scientists wrote an open letter to a Virginia state legislative commission examining a Bill related to Internet voting stating that in their opinion "the technology necessary to support Internet voting, while also protecting the integrity of the election and voter privacy, does not yet exist."[31]

Broadly, there are three potential sources of security vulnerabilities in Internet voting systems:

- At the voter's device
- In transit
- At the election server

5.1.1 At the voter's device[32]

Most researchers and Internet voting solution vendors agree that the voter's device is the least secure of the three due to (1) the wide variety of devices used by voters, the efforts put into the maintenance of the software on those devices, and the technical background of those maintaining the devices, as well as (2) the lack of control over the voter's device by the election administration or Internet voting system vendor.

30 For more information on this matter, see references #83, 94, 95, 121, 144, 150, 203, 211, 213, 246, 247, 267, 272, 274, 281, 282

31 Reference #317

32 References in this report to the voter's "device" can be read as any means by which an individual could cast a ballot for Internet voting (e.g., computer, tablet, smartphone)

Personal computers are already the target of malware,[33] phishing attempts and other attacks. The precise amount of malware prevalent on computers is unknown and estimates (1-50%) vary widely within the security community. Researchers fear that existing malware that has been developed for other purposes such as capturing credentials used for online banking and purchases can be used to record the voter's authentication credentials or track who an individual has voted for. It is also possible that new malware written to target specific voting systems could track how an individual votes, or even alter how the ballot is marked, and that either activity could take place without the voter's knowledge. While malware is typically developed by individuals or small groups, state-sponsored malware is also believed to exist.

While anti-virus software can detect known malware, such software relies on threats being identified with sufficient time for an update to be developed that denies the effectiveness of the malware or removes it from the system. No anti-virus program can guarantee 100% detection of all fraudulent software. Most critically, protection against even known malware requires appropriate and up-to-date anti-virus software on every voter's device that is to be used for Internet voting. Despite the existing real threats of malware, use of regularly updated anti-virus software is not widespread.

Also, based on existing Internet security issues, Internet voting can be susceptible to phishing attempts and imposter websites. This refers to the practice of attempting to acquire authentication credentials or other personal information by posing as a trustworthy or legitimate entity. This often relies on users being directed to a fraudulent website that mimics the authentic site and thereby tricks the user into entering their credentials or other personal information. A forged Internet voting site could capture the voter's credentials and then present an error message to the voter that the voting site is temporarily unavailable, giving the creator an opportunity to use those credentials on the real Internet voting site.

There is also a concern that both malware and phishing attempts could be automated to enable creators to affect large numbers of votes with little manual effort. It is for this reason that Internet voting is seen as significantly more risky than existing in-person or even vote by mail opportunities that carry their own risks.

An individual's ability to vote depends on the security of their own device, for which the individual is responsible. While a means can be provided for the individual to check that their vote is counted, this would depend on the individual having a way to communicate and compute which is secure from the malware.[34]

It has also been reported that some personal computer hardware is not trusted to provide secure transactions.[35]

33 Merriam-Webster: malicious software; software designed to interfere with a computer's normal functioning (e.g., viruses, trojan horses, spyware)
34 For more on cryptography and voter verification, see 5.6 Transparency and auditability, page 33
35 Reference #274

5.1.2 In transit

Once a voter has cast an online ballot on a device, the contents of the ballot must be transmitted to the election servers over the Internet. The transmission of any data over the open Internet can be susceptible to attempts by third parties to read, intercept or modify that data if appropriate security measures are not taken. Secure protocols (e.g., SSL/TSL) do exist that can create a direct link between the voter's device and the election server. Encryption and digital signatures can also be used to protect the integrity and authenticity of the data in transit. Voter verification methods can also identify to the voter if the ballot has been tampered with.

5.1.3 At the election server

Distributed Denial of Service (DDoS)

A Denial of Service (DoS) attack is an attempt to overwhelm a server's capacity with traffic so that it is unable to perform its usual duties and respond to its intended users. A server subject to a DoS attack may respond very slowly to its intended users or appear unavailable altogether. A Distributed Denial of Service (DDoS) attack is a DoS attack that is conducted by a large number (thousands) of computers, typically controlled remotely through malware. A DDoS attack on an election server during a voting period could have the effect of making it very difficult, if not impossible, for voters to cast ballots online.

The Internet voting component of the 2012 federal NDP leadership election was the subject of multiple DDoS attacks during the voting period. The attacks caused the voting sites to be unavailable to most voters and the time for voting online had to be extended. While the Internet voting vendor stated that the target of the DDoS attacks (and therefore the failure point) was the political party website that directed voters to the actual voting page hosted by the vendor, and therefore the Internet voting servers were technically unaffected, the end result for the voter was still the same.

Some researchers state that DDoS can be mitigated by hidden or dynamic website addresses; however, this approach makes it more difficult for voters to confirm that they are at the legitimate Internet voting website and not a fraudulent imposter site because they are unable to match the website address they see against a known valid address.

It is partly the threat of DDoS attacks that leads jurisdictions to permit Internet voting for multiple days and only ahead of general voting day.

Remote intrusion

In order for voters to access the election server for voting, it must be available over the public Internet. This also makes the server accessible to anyone who wishes to try to break in to, or compromise, it. Nearly every major website has been compromised, including the U.S. Department of Defence, Google, the FBI, and various financial institutions. Internet voting servers are likely no more secure than these major financial and government servers.

While no Internet voting server has reportedly been compromised during an election, Washington D.C. election servers were successfully compromised by a professor and a group of graduate students from the University of Michigan during a public test of the system's security. Ahead of the 2010 D.C. election, administrators invited the public to test the security of its system in a mock election scheduled for the month prior to an actual election in which Internet voting would be used. The University of Michigan group was able to take advantage of flaws in the system's source code and poor security management implementation (e.g., not changing default passwords to associated systems) to completely compromise the integrity of the Internet voting system. The group was able to add fraudulent ballots, change the results of previously cast ballots, and observe how voters were voting without being detected by the election officials, or by the firm engaged to audit the voting process. Based on the complete failure of the security, the Internet voting component of the 2010 election was cancelled.

One of the most critical technical challenges is detecting a compromise of a voting system. The state of the technology today is such that it is virtually impossible to guarantee that an intrusion would be always detected. It is also virtually impossible to guarantee that a voting system has not been compromised during an election. The risk is significant, as a compromise of a voting server can lead to a large-scale fraud.

Insider threats

There is also a risk that an insider could have access to results as votes are cast, be able to change results, or be able to associate ballots with specific individuals. Systems need to guarantee that no individual, including election administrators and system technicians, can compromise the secrecy of any ballot cast. Votes must be encrypted in a way that prevents any single individual from decrypting individual ballots. The key to decrypt the votes can be broken into pieces and shared among multiple individuals or stakeholders, of which a minimum number of pieces must be used to decrypt the ballots for counting.

To prove that the integrity of an Internet voting system has not been compromised by an insider through inserted code, Internet voting systems are typically assessed by contracted auditors and experts.[36]

36 For more on maintaining the integrity of software code see 5.6 Transparency and auditability, page 33

Conclusion

While there is no evidence that an election making use of Internet voting has been successfully compromised, this is not proof that it has not occurred, only that if it has occurred it has not been detected. The Washington D.C. example discussed above illustrates that an undetected compromise is possible. However, this argument could be applicable to all elections, including those that use traditional voting channels.

Some of these security issues could eventually be resolved by advances in hardware and software tools.

Although traditional voting is not without risk, it is much harder to perform and conceal large-scale fraud in traditional voting than in Internet voting. Policy-makers must decide what is an acceptable level of risk to a jurisdiction.

5.2 Compromised election results[37]

From banking and the purchase of goods and services, to communicating with friends and the public at large on social networking sites, the Internet is used for a wide variety of transactions by British Columbians every day. When those transactions are affected by security breaches and fraud, users may temporarily or permanently lose money (depending on whether those transactions are guaranteed by a financial or credit institution), be the subject of identity theft, or have their individual reputations tarnished by communications purportedly made on their behalf.

In comparison, the consequence of an election being affected is significantly higher than most Internet transactions if the wrong candidate or political party is elected with the ability to exercise the functions and powers of government.

It is easier for a smaller number of people to have a larger effect on votes in an Internet voting election than a traditional in-person election. Instead of having to corrupt the process for one voter at a time, automation of the processes allows for the automation of that corruption. Further, those wishing to have an effect on votes do not need to be present in the jurisdiction.

It has been suggested that some jurisdictions are not large enough targets for individuals or organizations looking to compromise an Internet voting system, and therefore the consequences of introducing Internet voting in those jurisdictions are less. However, the discovery of a vulnerability in one jurisdiction may increase the risk of that vulnerability being used in any other jurisdiction that uses the same technology, regardless of the size of the jurisdiction.

37 For more information on this matter, see bibliography references #121, 247, 281

The risk is even greater when there are a limited number of vendors serving all jurisdictions. Further, since security vulnerabilities can be purchased, the individual or group interested in compromising a system does not need to have discovered the vulnerability themselves.

Permitting Internet voting only ahead of general voting day and requiring pre-registration are seen as mechanisms to reduce the consequence of a security breach or other failure of the Internet voting system.

Conclusion

While the panel acknowledges that higher profile elections may make more attractive targets to individuals or groups looking to affect an Internet voting result, the panel believes that the election of the wrong candidate or party in even the smallest community in British Columbia is a serious matter.

5.3 Accessibility, usability and availability[38]

Unlike many other Internet transactions, the period for conducting an election is legislated. This means that Internet voting systems must be available to voters at precise times and voting cannot ordinarily be delayed if systems are compromised.

In traditional elections it is rare for a problem to occur that affects voters beyond a single voting place or community. However, a problem with an Internet voting system, such as a Distributed Denial of Service (DDoS) attack, could potentially impact all eligible voters. While the Chief Electoral Officer (for provincial elections) and the Minister responsible for the *Local Government Act*, chief election officers and presiding election officials (for local government elections) have the authority in law to extend or alter key dates of the election in exceptional circumstances, any changes would be difficult and expensive to communicate to voters. For this reason, most jurisdictions offer Internet voting over an extended period of time, prior to general voting day, and as an additional opportunity for voting rather than the sole option.

While Internet voting systems have the potential to improve services for voters with disabilities, these systems need to be compatible with a wide range of commonly used accessibility software and hardware by these voters in order for this benefit to be realized.

Increasing the security of an Internet voting system can increase the complexity of the system which may in turn reduce the usability of the system by voters. This is particularly a concern for voters with low technical capabilities or literacy levels.

38 For more information on this matter, see references #48, 121, 142

Researchers also speculate that if Internet voting replaces existing voting opportunities it risks creating a "digital divide" in which those without (or with reduced) Internet access have less access to voting than others.

Conclusion

Compatibility of the Internet voting system with widely used accessibility software and hardware needs to be considered if Internet voting is to be a benefit for voters with disabilities that encounter challenges with the traditional voting processes.

Provided traditional voting opportunities are maintained, the digital divide is not a significant concern for the panel.

The panel considers the specific issues of accessibility, usability and availability of Internet voting to be challenges that can be largely overcome or mitigated by jurisdictions if they consider these issues early in the planning phase prior to implementation.

5.4 Authentication and ballot anonymity[39]

Authentication and anonymity are two opposing, but interrelated, concepts. To ensure a voter is eligible and only votes once, the individual requesting a ballot must be confidently authenticated by the election administration; however, once authentication is confirmed, the voter's identity must be disassociated from the ballot to ensure the principle of the secrecy of the ballot is maintained.

Under traditional in-person voting processes, authentication occurs in a face-to-face transaction where the voter uses identity documents or other methods to satisfy the voting official as to the voter's identity and place of residence.[40] Anonymity is protected by giving all voters an identical ballot with no personally identifying markings and asking the voter to place the marked ballot in a ballot box where it is mixed with all other ballots before the box is opened at the end of the voting period and counted.

Authentication

When authentication occurs remotely, traditional identity documents must be replaced with another form of credential that can be used and verified electronically. In order to assign such credentials to the voter, the election administrator must know with a high degree of confidence who the voter is and whether they are entitled to vote.

39 For more information on this matter, see references #48, 94, 121, 139, 140, 180, 190, 207, 231, 258, 286

40 While some voters may vote using absentee voting processes, most of these opportunities also take place in public under the eye of candidate representatives who scrutinize the process. Only voters who cast ballots by mail are authenticated differently. For more on this issue, see 5.6 Transparency and auditability, page 33.

Most jurisdictions that offer Internet voting require some form of pre-registration prior to allowing an individual to vote online. This enables the election administration to compare registration to existing voter authentication data. In some places, simply being a registered voter in the jurisdiction is sufficient but, in others, Internet voting requires a separate Internet voting registration process. In either case, individuals who have not previously registered to vote or applied to vote online will be unable to cast an Internet ballot if they wait until the last minute. While Internet voting can be a method of increased convenience for voters, it still requires some prior planning in order to be used.

There are various ways that authentication credentials can be provided to voters, depending on how Internet voting is implemented. Many jurisdictions that have a high level of trust in the postal system will mail the credentials to all eligible Internet voters ahead of the voting period. Credentials vary, but often take the form of a unique Personal Identification Number (PIN) or passcode. Depending on whether there is a second level of Internet voting registration, the voter may then use that PIN online, typically in combination with the voter's date of birth or another "shared secret",[41] to register to vote electronically or to vote directly. When a second level of registration is required, the voter is given a new PIN either during the online registration or subsequently in the mail. The voter may also have the opportunity to create their own password that will be used in combination with the provided PIN in order to vote.

Once credentials have been provided to voters, the election administration must still be assured that the person using the credentials is the person to whom the credentials were issued. Requiring the voter to provide a shared secret in addition to what is mailed is one way to reduce the risk of impersonation, but some shared secrets such as date of birth are not as secret as they were once considered to be. While requiring a date of birth may be a reasonable way to prevent the average person who intercepts the mailed credentials from using them to vote on the voter's behalf, family members and close acquaintances may also know that shared secret, particularly with the increased disclosure of birth dates through social media.

In any form of remote voting outside of the relative protection of the voting place, voters are more susceptible to attempts of intimidation and improper influence of the voting intentions. This applies to both Internet voting and traditional vote by mail provisions.

In some jurisdictions citizens already have electronic credentials that are used for accessing other government services and can also be used by eligible voters for Internet voting. This eliminates the need for the election administration to provide unique credentials. These credentials that are used for multiple purposes are less likely to be lent or sold for the purposes of allowing someone else to cast a ballot on the voter's behalf.

41 Term for a fact or idea that both the voter and the election administration know, but that few or no other individuals will know.

Voters are also more likely to keep them safe. However, the longer the same authentication mechanism is used, the more likely vulnerabilities in the authentication mechanisms will be discovered.

British Columbians do not currently have electronic credentials for accessing government services. The Ministry of Technology, Innovation and Citizens' Services has developed a new foundational identity document called the BC Services Card to combine the BC Drivers' Licence or BCID card and BC CareCard. This new card contains enhanced security and privacy components and has the potential to be used for secure authenticated interaction with government services, including some services offered online. The card is being distributed to eligible[42] B.C. residents on a five-year rolling basis from 2013 to 2018. The authentication capabilities have yet to be implemented.

Ballot anonymity

Ballot anonymity refers to the inability to link a ballot with the individual who cast it. This is directly related to the principle of the secret ballot (below) and the security of the Internet voting system (above). In contrast to in-person voting where identical paper ballots are placed in physical ballot boxes where they are mixed with all other ballots prior to counting, the connection between the voter's identity and the content of the ballot cast electronically is fundamentally and necessarily linked for both technological and policy reasons. The order in which the ballots are cast, stored by the system and eventually counted will match the order in which voters were marked as having voted, and unless these linkages are broken somehow, it would be possible to identify a voter with their ballot. Further, when voting systems allow voters to cast multiple ballots[43] the Internet voting system, and therefore election administrators, must be able to identify which ballots have already been cast by the voter so that the subsequent ballot replaces the previous ballot. If the link between the ballot and the voter is broken before the end of all voting, this cannot be done.

The absentee voting process used in B.C. provincial elections and for mail ballot voting in B.C. local government elections provides authentication and anonymity through a double-envelope process.[44] Digital versions of this process exist for Internet voting.

---

42 B.C. residents aged 19-75

43 For more on this matter, see Norway in Appendix F - Experience with Internet voting in other jurisdictions

44 The marked ballot is placed in an unmarked "secrecy" envelope. The secrecy envelope containing the ballot is placed in an outer "certification" envelope that identifies the voter. At the conclusion of voting, the certification envelope is examined to ensure the voter was eligible to vote and has not voted at another voting opportunity. If the voter was entitled to vote via the absentee process the certification envelope is opened and the secrecy envelope is removed from the certification envelope. The secrecy envelope is placed in an unmarked ballot box and the certification envelope set aside. Once all absentee ballots have been reviewed in this manner, the ballot box containing the secrecy envelopes is shaken to shuffle the secrecy envelopes. That ballot box is opened and each secrecy envelope is opened. The ballots are separated from the secrecy envelopes and placed into a new ballot box, which is then shaken to mix up the order again. The ballots are now two steps removed from the certification envelope that listed their identity and so can be counted per the ordinary ballot counting process.

It is possible that over time the current encryption methods will be broken and any public voter validation codes could be used to identify how individuals that used those encryption methods voted in past elections.

Conclusion

The panel considers authentication to be a key issue for jurisdictions considering Internet voting.

While two-step authentication methods can be more secure than single step authentication, such processes are more complex to administer and for voters to use. Two-step authentication models also require additional forethought by the voter ahead of voting thereby reducing convenience.

However, if the BC Services Card works as promised, authentication could be a less significant issue. If the BC Services Card were to be considered as a secure authentication credential for Internet voting, Internet voting vendors and the B.C. government would need to collaborate to ensure the two systems could work together.

Any Internet voting option should provide for anonymity using properly implemented secure methods.

5.5 Secrecy of the ballot[45]

The secret ballot is a tool to protect the freedom of voting. Secrecy prevents third parties from knowing how an individual has voted, which prevents vote buying and voter coercion. Unsupervised voting (e.g., vote by mail and Internet voting) is more susceptible to vote buying and coercion than in-person voting because it cannot be guaranteed that voters are casting their ballots alone.

Researchers disagree as to precisely how the principle of a secret ballot should be interpreted. Some claim that the law must prevent voters from voting in a way in which the level of secrecy is reduced. Others claim that the principle only requires the opportunity for a secret ballot, while allowing for voters to choose less secret options. Most Canadian policy-makers (including those responsible for provincial and local government election policy in B.C.) have accepted the reduced level of secrecy offered by vote by mail in order to provide a more accessible voting process. Voters who need assistance marking their ballot in a voting place, either from an election official or a friend or family member that accompanies them to the voting place, also sacrifice some secrecy in return for the ability to vote.

The level of secrecy afforded to Internet voters depends on the specific form of Internet voting implemented in the jurisdiction.

45 For more information on this matter, see references #7, 130, 142, 180

If the voter is required to use the voter's ID card or drivers licence, the voter will be less willing to provide it to someone else because it has other uses. If the mechanism for authentication is not valued highly by the voter (e.g., a one-time-use PIN distributed by election administrators and not tied to other uses), the likelihood of selling or transferring the authentication credentials increases.

Some jurisdictions permit voters to cast multiple ballots, with only the final ballot ultimately being counted. This technique attempts to counter the impact of an influenced vote by enabling the voter to replace the influenced vote with a subsequent one that is cast free of influence (either online or in-person). Not only does this enable the voter to achieve the right to a secret ballot, it reduces the incentive to buy a vote in the first place because the purchaser cannot guarantee that the ballot they observed being cast will be the ballot that gets counted.

Traditional voting opportunities protect the secrecy of the ballot at the expense of the voter being able to have confidence that their vote has been included in the tally of votes for the candidate of their choice. This is accepted as a reasonable trade-off in Canada as ballots are fairly simple to mark correctly[46] and voters have a high level of trust in the election officials to interpret and count their ballot correctly. Internet voting systems that incorporate end-to-end verifiability[47] enable the voter to have a higher degree of confidence that their vote was counted as they intended.

Conclusion

The panel acknowledges the reduced level of secrecy offered by all remote voting opportunities, including Internet voting and voting by mail. That risk, for voting by mail, is mitigated by the fact that voting by mail is done by a very small fraction of the electorate. Risks to secrecy for Internet voting could occur on a wider scale if Internet voting was more widely adopted.

Internet voting implementations that permit voters to cast multiple ballots to counter the effects of improper outside influences, provided that only one vote is counted for a single voter, may mitigate this risk, as would ending the availability of Internet voting ahead of general voting day and establishing that any paper ballot cast by a voter would supersede an Internet ballot cast by the voter.

While Internet voting systems that provide a receipt[48] contravene the strict principle of a secret ballot by enabling the voter to prove to another individual how the voter voted, the panel does not consider the likelihood of voter coercion or vote selling to be high if this is implemented in B.C. In a new

46 In the 2013 Provincial General Election approximately 0.65% of ballots were rejected. For more information on this matter, see 4.6 Reduce/eliminate errors made by voters when casting ballots, page 20.

47 For more on end-to-end verifiability, see 5.6 Transparency and auditability, page 33

48 For more on the use of receipts, see 5.6 Transparency and auditability, page 33

Internet voting system that uses a receipt, it may be necessary to reduce the level of secrecy in return for an increased level of trust.[49]

5.6 Transparency and auditability[50]

In B.C. and most jurisdictions, candidates are entitled to appoint representatives (commonly referred to as scrutineers) to attend the voting place on their behalf and observe the registration, voting and counting processes. They are entitled to witness the activities of the election officials and voters and ensure that the requirements of the applicable laws are followed and that the process is administered consistently and fairly. They may record who has voted and report this to their campaigns and, after monitoring the counting process, take a copy of the official results for each ballot box back to their campaign. While they may not know the intimate details of the election laws, most eligible voters are familiar enough with the traditional in-person voting process and underlying principles to act as scrutineers at a provincial or local government election in B.C. Many jurisdictions also allow for independent observers to monitor the processes. This ability to scrutinize the registration, voting, and counting processes is a key aspect of a transparent electoral system.

Reviewing and evaluating Internet voting and electronic counting is very different from scrutinizing in-person voting and counting. Since voters are authenticated and ballots are cast remotely, observers cannot monitor the casting of individual ballots. Instead, observation of Internet voting usually involves the review and evaluation of the hardware, software and processes involved in administering the online voting before voting takes place. This type of observation is sometimes referred to as auditing. These reviews require specialized skills and knowledge that significantly limit who can perform them. Some Internet voting systems also have audit functions built into the software to allow for independent review and evaluation while voting takes place. Such functions can include the ability to see a live list of who has voted and even log in and cast "audit ballots" using the same processes as voters to ensure that the system is performing appropriately.[51]

Many election authorities rely on an outside individual or organization to act as an auditor for the entire Internet voting process on behalf of both the election administration and the candidates and political parties. Anyone acting as an auditor for an Internet voting process must be capable of performing appropriate process audits and the election administrator must be capable of understanding the results and limitations of those audits.

49 For more on trust, see 5.7 Trust, page 37
50 For more information on this matter, see references #27, 94, 142, 144, 156, 167, 195, 206, 228, 254, 286, 310
51 Audit ballots are specially marked ballots that would not be counted with ordinary ballots and so would not affect the results of the election.

Despite the reliance on outside auditors, most vendors state that any authorized individual would be entitled to review the system under a non-disclosure agreement (NDA). As most commercial Internet voting systems are built with proprietary technology, Internet voting vendors typically require those reviewing, certifying or auditing its systems to sign a non-disclosure agreement limiting what the subject can share publicly. These restrictions can be seen to reduce the level of transparency to the entire process.

To balance this lower level of transparency and maintain trust, policies, procedures and system documentation need to be available to participants and opponents alike.

The Norwegian election administration released the source code for its Internet voting systems in summer 2013 in order to inspire trust, enhance transparency and enable verification of its security by all experts, rather than just those willing to sign an NDA. The Estonian election administration released most of the source code for its Internet voting systems. However, the most security-critical portions of the code were not released and therefore a complete security assessment by outside experts was not possible. Open source code can permit any individual with the appropriate skills to review the software that is used and identify flaws in the code in order that such flaws come to light faster. In order to be run by a computer, source code must be compiled and translated into machine code. This process can also introduce errors that would be difficult to detect.

A complete assessment of all software code, systems and processes is very time-consuming and requires a high level of specialized skills and knowledge. Such a review would need to be conducted sufficiently ahead of the scheduled election so that any problems identified in the review could be rectified, and retested. Such thorough reviews could also prove to be expensive. There is currently no recognized standard for Internet voting technology to be evaluated against, either in Canada or internationally. However, components of these systems, such as the cryptography used, can be evaluated against well-established international standards.

An audit is "an independent pre- and/or post-election evaluation of an organization, system or process which includes quantitative and qualitative analysis."[52] Auditability refers to the degree to which the integrity of the overall system (technology and processes) and, ultimately, the results of the election can be confirmed. Thought of most broadly, this could include a review and certification of the hardware, software (including source code) and processes used by the Internet voting vendor and election administration prior to use, monitoring of those systems and processes during use, and evaluation of those systems and processes after use.[53] However, no standards for measuring the quality of such monitoring currently exists.

52 Reference #235
53 Systems must be monitored as soon as they are brought online (and therefore subject to attack), not just once voting begins.

In practice, third party audits of Internet voting systems are typically quite limited in scope. The audit report of the 2012 Halifax Regional Municipality (HRM) Internet voting system mentioned below specified that the application of the "Specified Auditing Procedures" established by HRM "[did] not constitute an audit or review engagement and, accordingly, no assurance is expressed." The reference to this statement here is not meant to pass judgment on the process used in Halifax or imply that the audit raised specific concerns or that the results were not accurate. It is raised here only to highlight an example of the limited scope of these observations characterized as audits and illustrate that they do not necessarily provide the same level of confidence that lay individuals may infer from the term "audit" and the reputation of the firms involved.

Auditability can also simply refer to the degree to which the results can be independently confirmed. Paper ballots can be recounted if requested by a candidate, if process dictates by an election administrator, or if ordered by the courts. Such a recount is easy to follow visually and the results of the initial count can be independently confirmed or overturned.

When votes are cast electronically, there are no physical representations of the ballot to be manually counted. Instead the system tallies the results from each electronically recorded ballot and generates a report of those totals. To recount those ballots means to regenerate another copy of the same report based on the system's existing interpretation and record of how those ballots were cast. Because they are based on the same underlying information, the regenerated report will always provide the same results as the initial tally.

For example, when a close result in a 2012 Halifax Regional Municipality election triggered a requirement for a judicial recount, the bylaws governing that election required that the election administrator provide a copy of the regenerated results report to the court and those results were added to the judge's count of the paper ballots. The election administrator also provided a copy of a third party auditor's report that confirmed that the tally of the system's interpretation of each ballot was correct. Such an audit does not determine if the system recorded the voter's intention accurately in the first place.

Due to the nature of how Internet ballots are cast, the concept of a recount under an Internet voting system shifts from a reconsideration of each ballot that was cast to an audit of the integrity of the system and processes by which those ballots were cast. This is a fundamental change to how stakeholders currently view the process.

Some Internet voting systems employ protocols commonly referred to as end-to-end verifiable (E2E) cryptographic systems. They are designed to answer three questions:

- Was the ballot marked as intended?
- Was the ballot collected by the system as the voter marked it?
- Was the ballot counted as the voter cast it?

While E2E systems enable anyone to tally the results and confirm that all votes were cast by eligible voters, they also generate new challenges for the voting process. Most significantly, they require voters to take further action after casting their ballot if they wish to verify the integrity of the system. This takes additional effort and adds another level of complexity to the process for the voter.

Even if used fully by voters, E2E systems are not the panacea to the issue of Internet voting security. E2E systems do not help when authentication credentials have been used by a third party. Malware could change the voter's intent if the voter uses an unsecured device, although an E2E system could enable the voter to detect such tampering. Depending on the implementation of the voter verification process, some E2E systems that provide voters with a receipt can enable a voter to definitively prove how they have voted, but this compromises the principle of a secret ballot and allows for coercion.

Perhaps the most significant challenges related to E2E systems that can prove tampering occurred are related to matters of public policy. How can tampering be distinguished from voter error (e.g., voter selects the wrong candidate)? What happens if evidence of tampering is identified? How much tampering must be identified to call the entire Internet vote into question? What is done when the Internet vote is called into question? Do all Internet ballots get disqualified? May affected voters cast a replacement ballot in-person? When does this determination get made? What happens if evidence of tampering is found after results are announced? If multiple jurisdictions use the same system concurrently, does tampering in one election affect decisions about the other?

Conclusion

The panel believes that the ability of parties, candidates and smaller jurisdictions to effectively audit an Internet voting process is quite limited and may in fact need to be outsourced. How these entities employ others to do this could conflict with vendor restrictions on access to proprietary systems, source code and documentation. At the local government level it may be necessary for multiple jurisdictions to work together, or perhaps with the provincial government, to develop a centralized oversight and auditing body. While better than relying on vendor assurances, these reviews are still no guarantee that the systems work as promised.

Whether or not the existing process is actively overseen, the capability to oversee the voting and counting process is there, and in a far different manner than an Internet voting system. Internet voting shifts the nature of oversight from individual ballots to the system as a whole.

The panel believes encryption and individual and independent verifiability (e.g. end-to-end verification) are key factors in assessing Internet voting and should be considered important aspects of ensuring transparency and auditability by any jurisdiction considering the implementation of Internet voting.

5.7 Trust[54]

When radical changes are made to known and trusted processes there is a significant risk that a degree of trust will be lost at least temporarily and will need to be re-earned. Introducing Internet voting, even as a complement to existing voting opportunities, can be such a radical change. In contrast to traditional voting processes, the level of knowledge about Internet voting processes is very low and this lack of knowledge creates distrust. If the losers in an election and their supporters do not trust that they lost fairly, the legitimacy of the elected government is in jeopardy.[55]

Voters trust local government chief election officers and Elections BC to administer elections in a manner that is fair and in accordance with the applicable laws. Public confidence in the electoral process and the legitimacy of elected officials in British Columbia is high. This legitimacy of elected officials and the government of the day are fundamental to our democracy. If an election conducted using Internet voting is compromised, or even suspected to be compromised, the legitimacy of the elected government is at stake.

When voters cannot easily observe the voting process and laypersons are replaced by information technology experts in the administration of voting, the level of trust is also affected. There may also be a fear of the "privatization of democracy."[56] Ways to generate trust include: ensuring that information is made available about the Internet voting system; ensuring proper testing, certification and audit mechanisms are in place; and implementation of an independently verifiable and evaluated system.

Conclusion

There currently exists a high level of trust in local government and provincial elections in B.C. Many of the other challenges outlined in this report can affect the level of trust stakeholders will have in an Internet voting system, and the ability of an election administration to satisfy those challenges is a key determinant in the level of trust stakeholders will have in an Internet voting

54 For more information on this matter, see references #142, 167
55 For more on this matter, see 5.2 Compromised election results, page 26
56 Reference #167

system. However it is important to note that not only should stakeholders perceive the election system to be trustworthy, but the election system should in fact be trustworthy. Trust in an election system comes from developing a system that is trustworthy.

The panel acknowledges that when first implemented, Internet voting will not have the same level of trust as the existing voting processes, but wholeheartedly recommends that jurisdictions considering the implementation of Internet voting take all reasonable efforts to build as high a level of trust as possible with stakeholders and to begin doing so as early in the planning phase as possible.

5.8 Stakeholder management[57]

The introduction of Internet voting introduces a new stakeholder in the electoral process – the Internet voting technology vendor. In order to work effectively with, and maintain control over, the vendor, election administrators must become, or surround themselves with, technology experts. If election administrators fail to do this they will effectively delegate oversight of the election to the technology vendor.[58]

Election administrators must educate voters, work with opponents of Internet voting and learn how to address public concerns.

Election administrators themselves may also need to build a refocused skill set that includes management of technology implementation and increased focus on open information policy in order to build and maintain trust in Internet voting.

Conclusion

Some vendors the panel heard from claimed that election administrators implementing Internet voting would need only minimal technical expertise within their organization. The panel feels that vendors may underestimate the significance of election administrators delegating oversight of the key elements of an Internet voting election to a technology vendor. Election administrators must retain sufficient oversight capability to identify vulnerabilities that a vendor may not want to disclose for business or competitive reasons. Given the variation in how elections are administered in B.C., the panel also questions whether vendors have sufficient capacity to manage a large number of new clients while still providing a high level of service.

The panel recognizes that developing adequate technical expertise and maintaining control over the technology vendor and ultimately the electoral process will be more difficult in smaller jurisdictions without assistance from the provincial government or other jurisdictions having the required technical expertise.

57 For more information on this matter, see bibliography reference #142
58 Election administrators must avoid simply delegating such oversight to technology contractors.

At the provincial level the administration of Internet voting would likely be centralized. This may change the nature of the relationship between the candidates and Elections BC. Instead of working almost solely with the District Electoral Officers in the electoral districts on issues related to the voting process, candidates and their campaigns would likely want to have, as well, a closer relationship with Elections BC headquarters staff managing the Internet voting technology.

5.9 Cost[59]

While some see Internet voting as a way to reduce the costs of election administration, Internet voting is usually offered as an additional channel for voting and therefore increases the total cost of election administration.[60]

Further, Internet voting introduces numerous new activities beyond the administration of voting that also will require budgeted funds and significant amounts of time. These include: developing and implementing an effective communications strategy to inform and educate voters about the new voting opportunities and voting processes;[61] a comprehensive evaluation of the Internet voting system, including a review of all hardware and software (e.g., source code) and mock elections, well ahead of implementation; and a thorough audit and review of the system and processes after the election. Some of these activities may be one-time costs that could be amortized over multiple elections, but others will be necessary each time an Internet voting election is held. Some activities that appear to be one time costs (e.g. source code analysis and penetration testing) may actually become ongoing costs, because even if the system has not changed since it was last used, the skills and motivations of potential attackers will evolve over time.

The precise costs of implementing Internet voting are not easily determined. Jurisdictions do not account for, and report, costs associated with elections and Internet voting in a consistent manner.[62] Due to these significant differences the panel could not do an "apples to apples" comparison and therefore did not attempt to determine the specific costs of implementing Internet voting for either provincial or local government elections in British Columbia.

59 For more information on this matter, see references #48, 121, 144, 146, 195, 217, 227, 290, 292

60 See 4.4 Cost savings of administering Internet voting over in-person voting, page 17

61 Elections Ontario's recent research into Internet voting "indicated that the communications and outreach materials represent approximately 10% of the budget for implementing [Internet voting]." Reference #292.

62 For example, the City of Markham claims a "cost per elector" of $0.81 for Internet voting in its 2010 municipal election compared to $5.63 for in-person voters. It is unclear if those published costs of Internet voting include all of the marginal costs of adding Internet voting to an existing election (e.g., costs associated with producing and distributing authentication credentials by mail, public information campaigns associated with Internet voting, etc.), or just the service contract with the vendor. It is also unclear whether the cost per in-person voter includes all costs related to Markham's election administration, or strictly the costs attributable to in-person voting (e.g., voting place rental, staffing, printed supplies, etc.).

Internet voting system vendors typically charge on the basis of a cost-per-registered voter and not based on the number of voters who choose to use Internet voting in the election. This means that the cost of the service can be determined ahead of time. It is unclear to the panel whether this cost model depends on a minimum number of registered voters.

Developing an Internet voting system and selling the service of administering Internet voting is still a relatively new business. It is not known whether the amount charged by vendors today represents a stable cost over time, or whether it is being offered at a reduced rate in order to acquire customers and could increase over time.

A jurisdiction considering Internet voting must decide between purchasing the services of one of a limited number of vendors and developing its own Internet voting system. Purchasing the existing services of an Internet technology vendor is seen to be significantly less expensive than a jurisdiction developing its own Internet voting system. When determining whether to purchase the services of a vendor or develop an in-house system, the impact on system security will also need to be considered. All Canadian jurisdictions that have used Internet voting have purchased the services of one or more vendors. Estonia, Geneva and Norway are three of the more well-known jurisdictions that have developed their own Internet voting system.[63]

Conclusion

The precise costs associated with implementing Internet voting will highly depend on the size of the jurisdiction (number of registered voters), the existing capacity within the jurisdiction to manage this new process, and whether the jurisdiction develops a new system or purchases the services of an Internet voting system vendor.

Developing an Internet voting system is more expensive at the outset, and possibly over time, than purchasing the services of an existing vendor. However, with the additional cost to develop a new system comes an increased flexibility to design a system that meets the specific needs of the jurisdiction and a potential for increased transparency. Policy-makers will need to determine whether the financial costs of developing a new system outweigh any benefits. The panel does not believe that any local government in B.C. could afford to develop its own system without the assistance of the provincial government and would almost certainly need to purchase Internet voting services from a vendor.

In any case, jurisdictions considering implementing Internet voting must recognize that there are significant financial costs to the decision beyond the Internet voting system contract.

63 For more on the Canadian and international jurisdictions that have used Internet voting, see Appendix F - Experience with Internet voting in other jurisdictions

6.0 SUMMARY

After this review, the panel notes that the benefits of Internet voting are not as persuasive as one might initially think. The panel also recognizes that policy-makers and election administrators will need to seriously consider the ability of each jurisdiction to satisfy the challenges posed by introducing Internet voting. The following represent the panel's assessment of the perceived and actual benefits and challenges to implementing Internet voting at the local and provincial government levels.

6.1 Perceived and actual benefits

Increase voter turnout:

- Evidence is mixed, at best
- Not convinced Internet voting will result in increased turnout at either level in the long run
- Not a compelling reason for introducing Internet voting

Increase accessibility/convenience:

- Most significant potential benefit for B.C. voters
- Potential benefits greater for local government elections due to seasonal weather constraints for fall elections
- Fewer potential benefits for provincial elections due to broader existing absentee voting opportunities
- Most compelling reason for Internet voting

Improve speed and accuracy of results:

- High level of confidence by election administrators at both levels in current counting methods
- Speed of overall results still dependent on hand-counted paper ballots (unless Internet voting is only channel)
- Preliminary results already reported quickly on election night for both local government and provincial elections
- Not a compelling reason for introducing Internet voting

Cost savings of administering Internet voting over in-person voting (see also Cost on page 44):

- Opportunities for cost savings require Internet as only option
- As an additional channel, Internet voting will result in increased costs
- May be possible to offset some Internet voting costs with reduced in-person voting

- More costs to consider than the contract with the vendor or initial development of system in-house
- Not a compelling reason for introducing Internet voting, at least in the short to medium term

Requires fewer resources of parties and candidates:

- Fewer volunteers possible if Internet voting is only option
- As an additional channel, more volunteers required
- Volunteers need different skills under Internet voting
- Not a compelling reason for introducing Internet voting

Reduce/eliminate errors made by voters when casting ballots:

- Potential to eliminate errors due to incorrect markings
- No impact on ballots that are intentionally spoiled
- Not a compelling reason for introducing Internet voting

Maintain relevance by keeping up with other aspects of society:

- Symbolic potential benefit not considered significant for B.C.
- Not a compelling reason for introducing Internet voting

Greener:

- Relative "greenness" unknown without full evaluation of both Internet voting and traditional voting

6.2 Perceived and actual challenges

Security:

- Potential for large-scale fraud is greater for Internet voting than traditional voting opportunities
- Policy-makers must decide an acceptable level of risk to a jurisdiction

Compromised election results:

- Higher profile elections may make more attractive targets
- Consequences likely higher at more senior levels of government
- Election of wrong candidate or party in even the smallest community a serious matter

Accessibility, usability and availability:

- Compatibility with accessibility software and hardware needs to be considered
- Digital divide not a significant concern
- Can be largely overcome if considered early enough

Authentication and ballot anonymity:

- Key issue for jurisdictions considering Internet voting
- Two-step authentication can be more secure, but also more complex for administrators and voters
- BC Services Card could make authentication a less significant issue if considered secure and can be incorporated into an Internet voting system

Secrecy of the ballot:

- All remote voting opportunities offer reduced degree of secrecy
    - Use of vote by mail very low at both levels
    - If Internet voting widely adopted, this risk increases
- Effects of improper outside influences (e.g., coercion, vote-buying) can be mitigated by:
    - Permitting voters to cast multiple ballots, with each subsequent ballot replacing the previous ballot
    - Establishing that a paper ballot supersedes any Internet ballot cast by a voter
    - Ending Internet voting ahead of general voting day

Transparency and auditability:

- Oversight significantly different from traditional voting
- Nature of oversight shifts from individual ballots to the system as a whole
- Limited ability of candidates/parties/smaller jurisdictions to effectively audit Internet voting
    - May need to be outsourced
- Centralized oversight and auditing body may be necessary for local government elections (e.g., provincial government, multiple jurisdictions)
- Reviews and audits are no guarantee that a system works as promised
- Encryption and individual and independent verifiability (e.g. end-to-end verification) are important aspects of ensuring transparency and auditability

Trust:

- High level of trust in B.C. local government and provincial elections
- Internet voting will not have same level of trust as existing voting processes
- Election administrators' ability to satisfy other challenges can affect level of stakeholder trust
- Take all reasonable efforts to build as high a level of trust with stakeholders as possible; this is done by developing a system that is trustworthy

Stakeholder management:

- Vendors may underestimate significance of election administration delegating oversight
- Vendor capacity to manage large number of new clients questionable
- In-house technical expertise low in smaller local governments
    - More difficult to maintain control over vendor
    - May need assistance from provincial government or other jurisdictions
- Centralized voting administration by Elections BC for provincial elections has implications for relationship with candidates and political parties

Cost (see also Cost savings of administering Internet voting over in-person voting on page 41):

- Costs to implement not consistently defined or reported
    - Difficult to fully assess the costs of Internet voting
    - Numerous costs in addition to vendor contract/system development (e.g., system review, audit, voter education)
    - Affordability for smaller local governments questionable

7.0 EXPERIENCE WITH INTERNET VOTING IN OTHER JURISDICTIONS

A number of jurisdictions around the world have implemented Internet voting and many more have investigated it. The panel examined some of these jurisdictions and took the following lessons from those experiences. More information about the experiences of jurisdictions that have considered Internet voting, and either implemented or rejected it, is included in Appendix F.

7.1 Lessons learned for B.C.

- Internet voting is not a panacea for voter turnout (Markham)
- The more complex the process for acquiring authentication credentials, the less likely voters will be to use it (Markham, USA)
- Any pilot project must be adequately planned, tested, implemented and evaluated using predetermined criteria (UK)
- Rushing implementation results in insufficient testing and review and significantly increases the likelihood of issues that will not be identified or resolved in time (New South Wales)
- The process in use must be trusted as secure as there is no significant potential for a meaningful recount (Halifax, Estonia)
- Internet voting does not lead to increased turnout by youth (Markham, Norway)
- Allowing voters to cast a ballot multiple times (while counting only the last ballot) is an effective way to reduce the likelihood of coercion in remote voting (Estonia, Norway)
- A post-election audit by a third party should always be conducted to determine whether the integrity of the election may have been compromised and to identify opportunities for improvement (Norway, New South Wales)
- Even in jurisdictions where Internet voting is widely accepted, it still only accounts for 1/5 to 1/3 of all votes cast (Markham, Estonia)
- Jurisdictions often limit use of Internet voting to a smaller subset of the population to mitigate risk (Geneva, New South Wales)
- Most jurisdictions only offer Internet voting during advance voting periods and only allow paper ballots on general voting day (Markham, Halifax, Estonia, Norway)
- Public education and outreach ahead of an election that uses Internet voting can significantly contribute to public acceptance of Internet voting, and perhaps have an effect on voter turnout (Truro)
- Most jurisdictions claim voter convenience as a primary reason for implementing Internet voting, but many still hope it will have a positive impact on voter turnout, despite the lack of evidence (Markham, Halifax, Truro, Estonia, Geneva)

- Concerns of security and cost are most frequently given as reasons why Internet voting should not be introduced (Kitchener, Edmonton, Ontario, Canada, USA)
- Public confidence in related electoral matters (e.g., voting technology generally, electoral administration) can strongly influence the perception of Internet voting (Netherlands, Canada)

8.0 RECOMMENDATIONS

1. **Do not implement universal Internet voting for either local government or provincial government elections at this time. However if Internet voting is implemented, it should be limited to those with specific accessibility challenges. If Internet voting is implemented on a limited basis, jurisdictions need to recognize that the risks to the accuracy of the voting results remain substantial.**

   The risks of implementing Internet voting in British Columbia outweigh the benefits at this time. Therefore it is premature to implement Internet voting on a universal basis.

   Because of the strengths of Internet voting to provide increased accessibility for certain segments of the population (e.g., remote voters, voters with disabilities and voters who would otherwise need assistance to vote), Internet voting could be used in the future on a limited basis to improve access to the ballot for these groups.

   There are significant risks to implementing Internet voting that can jeopardize the integrity of an election, no matter the extent of implementation. If Internet voting is to be used in British Columbia in the future, the following three recommendations must be adhered to, including all of the principles outlined in recommendation #4.

2. **Take a province-wide coordinated approach to Internet voting.**

   If Internet voting is to be implemented at either the local government or provincial government level, election administrators should work with each other and with the provincial government to conduct a more rigorous review of the options, establish a common framework for implementation and retain control and oversight over election administration during implementation.

3. **Establish an independent technical committee to evaluate Internet voting systems and support jurisdictions that wish to implement approved systems.**

   Provincial and local government election administrators do not have the necessary technical expertise in-house to properly evaluate, verify and test high security systems such as Internet voting systems. A technical committee independent from vendors, political parties, and elected representatives, and made up of election administrators and recognized experts in Internet voting, cryptography, and computer security should be established to support the province-wide coordinated approach. The technical committee would be established by, and would report to, the B.C. Chief Electoral Officer. Such a reporting structure would emphasize the technical committee's independence. Such a committee would have to stay abreast of changes in available and emerging technology in order to establish standards and requirements that would have to be met by any Internet voting system to be

used in British Columbia. The committee would also be responsible for overseeing a rigorous review of any system being considered for use against those standards and requirements to ensure high security. Only Internet voting systems approved by the technical committee should be authorized for use in B.C. jurisdictions. The technical committee would also be responsible for monitoring the security of the systems while in use and conducting a full audit and evaluation afterwards. The work of the technical committee should be made public to ensure transparency and to build trust in any system implemented.

4. Evaluate any Internet voting system against the principles established by the panel.

While acknowledging that there will be unique factors to consider in each jurisdiction, the panel recognizes the benefit of establishing a common, or at least similar, set of principles that can be used by multiple jurisdictions in Canada to evaluate Internet voting. There is a growing consensus among election administrators of what these principles are. The panel used the eight principles established by Elections Ontario in its Alternative Voting Technologies Report[64] as a starting point from which to develop principles for British Columbia. Many of the principles outlined below share common elements with Elections Ontario's principles, but some have been amended to reflect a B.C. context or for consistency with the language used in this report. These principles must be met in addition to any standards a technical committee would establish.

Accessibility

The Internet voting process must be readily available to, and usable by, all voters eligible to vote by Internet voting, even in the presence of Internet voting-specific threats.

Ballot anonymity

The voting process must prevent at any stage of the election the ability to connect a voter and the ballots cast by the voter.

Individual and independent verifiability

The voting process will provide for the voter to verify that their vote has been counted as cast, and for the tally to be verified by the election administration, political parties and candidate representatives.

Non-reliance on trustworthiness of the voter's device(s)

The security of the Internet voting system and the secrecy of the ballot should not depend on the trustworthiness of the voter's device(s).

64 Reference #292

One vote per voter

Only one vote per voter is counted for obtaining the election results. This will be fulfilled even in the case where the voter is allowed to cast their vote on multiple occasions (in some systems, people can cast their vote multiple times, with only the last one being counted).

Only count votes from eligible voters

The electoral process shall ensure that the votes used in the counting process are the ones cast by eligible voters.

Process validation and transparency

The procedures, technology, source code, design and implementation details, and documentation of the system must be available in their entirety for free and unconstrained evaluation by anyone for testing and review for an appropriate length of time before, during and after the system is to be used. Policies and procedures must be in place to respond to issues that arise. Appropriate oversight and transparency are key to ensuring the integrity of the voting process and facilitating stakeholder trust.

Service availability

The election process and any of its critical components (e.g., voters list information, cast votes, voting channel, etc.) will be available as required to voters, election administrators, observers or any others involved in the process. If Internet voting should become unavailable or compromised, alternative voting opportunities should be available.

Voter authentication and authorization

The electoral process will ensure that before allowing a voter to cast a vote, that the identity of the voter is the same as claimed, and that the voter is eligible to vote.

APPENDIX A - CONVENING THE PANEL

BRITISH
COLUMBIA

AUG 0 7 2012

Dr. Keith Archer
Chief Electoral Officer for British Columbia
BC Elections
PO Box 9275 Stn Prov Govt
Victoria BC V8W 9J6

Dear Dr. Archer:

As you may be aware, the Premier has made a commitment to request that your office convene a non-partisan expert panel to review best practices with respect to Internet voting in other jurisdictions and to examine the issues associated with implementing Internet voting in British Columbia. I am writing to you now, as the minister responsible for the *Election Act,* to formally make that request.

As you also may be aware, several local governments in British Columbia have expressed a strong interest in offering Internet voting as well. Accordingly, should you be amenable, I would ask that the panel examine Internet voting in both local and provincial contexts, as certain factors may be unique to each level of government.

Your predecessor published a helpful in-house discussion paper on the subject last August that briefly reviewed Internet voting in other jurisdictions and examined a number of issues such as security and transparency. I am sure that paper will be useful to the panel, although of course the panel should be free to draw on research and analysis as it sees fit.

If you are amenable to undertaking this task, my ministry would be happy to assist in whatever ways you feel are appropriate.

.../2

Ministry of Justice

Office of the Minister of Justice and Attorney General

Mailing Address:
PO Box 9044 Stn Prov Govt
Victoria BC V8W 9E2
e-mail: JAG.Minister@gov.bc.ca
website: www.gov.bc.ca/justice

Telephone: 250 387-1866
Facsimile: 250 387-6411

Dr. Keith Archer
Page 2

I appreciate that there would be costs involved in undertaking this project. Accordingly, I am copying Mr. Douglas Horne, MLA for Coquitlam-Burke Mountain and the Chair of the Select Standing Committee on Finance and Government Services, so he is aware that you may be submitting a specific request for funding to the Committee beyond that contained in your annual budget proposal.

I look forward to a reply at your earliest convenience.

Sincerely,

Shirley Bond
Minister of Justice
and Attorney General

pc: The Honourable Ida Chong
Mr. Douglas Horne, MLA
Mr. Leonard Krog, MLA

Mailing Address:
PO Box 9275 Stn Prov Govt
Victoria BC V8W 9J6

Phone: 250-387-5305
Toll-free: 1-800-661-8683/ TTY 1-888-456-5448
Fax: 250-387-3578
Toll-free Fax: 1-866-466-0665
Email: electionsbc@elections.bc.ca
Website: www.elections.bc.ca

August 9, 2012

Honourable Shirley Bond
Attorney General
Ministry of Justice
PO Box 9044 Stn Prov Govt
Victoria, BC V8W 9E2

Honourable Shirley Bond:

Thank you for the invitation to convene and chair a panel that will enquire into prospects for Internet voting in British Columbia.

As an Independent Officer of the Legislative Assembly, I am very pleased to convene and chair a panel for this purpose. I am writing to advise you, as well as those copied on this letter, how I intend to proceed.

Mandate and Authority
Convening a panel to research and draft recommendations to the Legislative Assembly on Internet voting is authorized pursuant to section 12(2)(a) of the *Election Act*.

Scope
Following and extending the Elections BC report entitled, *Discussion Paper: Internet Voting*, the panel will examine opportunities and challenges related to the potential implementation of Internet-based voting for provincial or local government elections in British Columbia.

Reporting
The method for gathering input and feedback from experts and the public will be determined by the panel. Additionally, the panel, when established, will develop a work plan and the timeline for reporting.

Composition
I will chair the panel and will invite four additional members. Members will be drawn from a wide spectrum reflecting expertise in technology, cryptography, Internet security policy, and electoral administration. All members will have a high level of independence and judgment.

Secretariat
The secretariat function of the panel will be provided by Elections BC.

...2/

-2-

Budget
The costs of the panel are estimated to be $420,000. I expect the majority of these costs to be incurred in the current fiscal year, and I will ask the Select Standing Committee on Finance and Government Services to recommend my office be granted access to the Contingencies Vote for 2012/13. Any necessary funding for next fiscal year will be requested as part of Elections BC's annual budget proposal for 2013/2014.

If you, or those copied on this letter, have comments on any aspect of the panel as outlined, please communicate these by August 23, 2012. My intention is to write to the Select Standing Committee on Finance and Government Services the following week to request funding for the panel. I intend to select the panel by September 7 and to convene the first meeting by October 1.

Sincerely,

Keith Archer, Ph.D.
Chief Electoral Officer
British Columbia

c. Honourable Bill Barisoff, MLA
Speaker of the Legislative Assembly

Craig James
Clerk of the Legislative Assembly

Douglas Horne, MLA
Chair, Select Standing Committee on Finance and Government Services

Leonard Krog, MLA
Critic for Attorney General

Honourable Rich Coleman, MLA
Government House Leader

John Horgan, MLA
Opposition House Leader

Honourable Ida Chong, MLA
Minister of Community, Sport and Cultural Development

APPENDIX B - PANEL MEMBERS

KEITH ARCHER, Ph.D.

Keith Archer became British Columbia's Chief Electoral Officer on September 1, 2011. He brings over thirty years of experience in electoral administration research and education to the position of Chief Electoral Officer.

Prior to his appointment, Keith Archer was Professor of Political Science at the University of Calgary (1984) and Director of Research at the Banff Centre. He completed BA and MA degrees in Political Science at the University of Windsor, and a Ph.D. at Duke University. His teaching and research has focused on the study of elections and voting. He is the author, co-author or co-editor of seven books and over thirty articles and chapters in the area.

Keith Archer's experience and expertise has contributed to a number of projects including the Administration and Cost of Elections project (a collaborative initiative of the United Nations, the International Institute for Democracy and Electoral Assistance (IDEA) and the International Foundation for Election Systems, among others), the Royal Commission on Electoral Reform and Party Financing in Canada (The Lortie Commission), Bill C-16 (Expanded Voting Opportunities) and he has provided expert opinion involving the Canadian Charter of Rights and Freedoms on the section 3 "right to vote."

DR. KONSTANTIN (KOSTA) BEZNOSOV

Konstantin (Kosta) Beznosov is an Associate Professor at the Department of Electrical and Computer Engineering, University of British Columbia (UBC), Vancouver, where he founded and directs the Laboratory for Education and Research in Secure Systems Engineering (LERSSE). His primary research interests are distributed systems security, usable security, secure software engineering, and access control. Prior UBC, Dr. Beznosov was a Security Architect with Quadrasis, Hitachi Computer Products (America), Inc, where he designed and developed products for security integration of enterprise applications, as well as consulted large telecommunication and banking companies on the architecture of security solutions for distributed enterprise applications. Dr. Beznosov did his Ph.D. research on engineering access control for distributed enterprise applications at the Florida International University. He actively participated in standardization of security-related specifications (CORBA Security, RAD, SDMM) at the Object Management Group, and served as a co-chair of the OMG's Security SIG. Having published a number of research papers on security engineering in distributed systems, he is a co-author of "Enterprise Security with EJB and CORBA" and "Mastering Web Services Security." He has served on program committees and/or helped to organize SOUPS, CCS, NSPW, NDSS, ACSAC, SACMAT, CHIMIT. Prof. Beznosov is an associate editor of ACM Transactions on Information and System Security (TISSEC) and International Journal of Secure Software Engineering (IJSSE).

LEE-ANN CRANE

Lee-Ann Crane has been employed with the Regional District of East Kootenay since 1979 and has been the Chief Administrative Officer since 1998.

Lee-Ann has served in various capacities on the Board of the Local Government Management Association of BC. She is currently Chair of their Elections Committee and was instrumental in the development and publication of the Local Government Elections Manual, and continues to be responsible for content and editing. Lee-Ann also serves as a resource to local government election officials throughout B.C. and participates in review of local election legislative changes.

DR. VALERIE KING

Valerie King is Professor of Computer Science at the University of Victoria and has been a faculty member there since 1992. She received an A.B. degree in Mathematics from Princeton University and a Ph.D. in Computer Science and a J.D., both from the University of California at Berkeley. She was a post-doctoral fellow at the University of Toronto and Princeton University, a Research Scientist at NECI, Compaq SRC and HP Labs, a Visiting Researcher at Microsoft Research SVC and at the Simons Institute for Theory of Computing in Berkeley, and a Visiting Professor at the University of Copenhagen and Hebrew University. She is currently a member of the Institute for Advanced Study in Princeton.

Dr. King's current research concerns randomized algorithms, data structures, and distributed computing, with applications to networks and security. She has served on numerous technical committees and panels, including panels for the Natural Sciences and Engineering Research Council of Canada and the U.S. National Science Foundation, and has published over sixty scholarly papers and book chapters. She is a member of the Association for Computing Machinery and the State Bar of California.

GEORGE MORFITT, FCA

George Morfitt is a graduate of the University of British Columbia and a Chartered Accountant. After a 20-year career as Chief Financial Officer in the private sector in Vancouver, he served two terms as Auditor General of British Columbia. Mr. Morfitt has held senior executive positions in a number of organizations, including: President, BC Institute of Chartered Accountants; Chair, Universities Council of BC; and Chair, UBC Board of Governors. He is a former alderman for the municipality of West Vancouver and is a past President of the Canadian Squash Racquets Association.

Mr. Morfitt is a Fellow of the BC Institute of Chartered Accountants and a Queen's Diamond Jubilee medalist. He currently serves as Chair of WorkSafeBC and is a past director of the Motor Vehicle Sales Authority of BC, the BC Safety Authority and the Health Council of Canada. Mr. Morfitt is an inducted member of the BC Sports Hall of Fame and is past Chair of Canadian Sport Centre Pacific.

APPENDIX C - EXPERT PRESENTERS

Presentations

Ian Bailey (Executive Director, Architecture and Standards and Information Security, Ministry of Technology, Innovation and Citizens' Services)

Kevena Bamford (Executive Director, Provincial Identity Management Program, Ministry of Technology, Innovation and Citizens' Services)

Anton Boegman (Deputy Chief Electoral Officer – Electoral Operations, Elections BC)

Michelle Dann (Ministry of Community, Sport and Cultural Development)

Ben Goldsmith (Senior Electoral Advisor, International Foundations for Electoral Systems)

Dr. J. Alex Halderman (Assistant Professor of Electrical Engineering and Computer Science, University of Michigan)

Bette-Jo Hughes (Associate Deputy Minister of Technology, Innovation and Citizens' Services & Acting Chief Information Officer)

Stephen Huycke (Acting Deputy Clerk, City of Markham)

Denise McGeachy (Ministry of Community, Sport and Cultural Development)

Susan McMurray (Manager of Research and Policy, Elections Ontario)

Cathy Mellett (Chief Clerk, Halifax Regional Municipality)

Stefan Morales (Ministry of Community, Sport and Cultural Development)

Dr. Ronald L. Rivest (Professor of Computer Science, Massachusetts Institute of Technology)

Dr. Melanie Volkamer (Assistant Professor, Technische Universität Darmstadt)

Lorie Wells (Deputy Chief Electoral Officer, Elections Ontario)

Internet Voting Technology Vendors

Everyone Counts Canada Inc.

Intelivote Systems Inc.

Scytl Canada Inc.

APPENDIX D - QUESTIONS TO INTERNET VOTING VENDORS

1. Must an Internet voting solution require voters to assume responsibility for ensuring their computers are free from malware that could compromise the secrecy of the ballot or prevent their ballot from being cast in the way in which they intend? How does your solution mitigate this risk?

2. With what level of confidence can an election administrator trust that the individual who has cast a ballot using an Internet voting solution is the individual to whom the election administrator believes they have provided the ballot?

3. How would you respond to the following statement:

   > Recent cyber attacks on major organizations such as financial institutions, the U.S. Department of Defense, the FBI and Google have proven that networks cannot be secured against a well-funded coordinated attack and therefore any vendor claiming to provide a secure Internet voting solution is misleading you.

4. When using an Internet voting solution, how can election administrators, political parties, candidates and voters trust that all votes were cast and counted as intended?

5. How much technical expertise must election administrators have within their organization to provide a reasonable level of oversight to a vendor providing an Internet voting solution?

6. To what extent is your application code proprietary? Can it be made available for scrutiny by others, and under what conditions?

7. How can it be proven that the version of application code that has been tested and reviewed is indeed the version that is running during the election?

8. How can political parties and candidates scrutinize an Internet voting solution? Must they delegate this right to a third party (e.g., an independent audit firm)? Can individual political parties or candidates appoint their own scrutineers or must they all trust a single third party appointed by the election administrator?

9. Local government elections in B.C. are administered separately by each jurisdiction, but under a common legislative framework with a common election period. How many simultaneous elections can a single vendor reasonably support? ("support" includes both technical and contract management capabilities)

10. With regard to registration/eligibility for Internet voting and the provision of authentication credentials, how can an Internet voting solution vendor balance the expectations of voters for a simple process with the expectations of election administrators for a secure process?

11. Some jurisdictions distribute elements of Internet voting amongst multiple vendors in order to reduce risk by avoiding relying on a single vendor. How would you recommend an Internet voting solution be divided?

12. Internet voting standards are emerging from various international bodies. Do you evaluate your Internet voting solution against any particular standard(s)? If so, which body's standards are you using and how does your solution meet the standard?

APPENDIX E - REFERENCE LIST

The following resources have been directly referenced in this report. A full bibliography is available on the Independent Panel on Internet Voting website (internetvotingpanel.ca).

7. European Commission for Democracy Through Law (Venice Commission). (July 2002). Code of Good Practice in Electoral Matters: Guidelines and Explanatory Report. Venice, Italy: Council of Europe.

27. Office for Democratic Institutions and Human Rights. (2005). Election Observation Handbook, Fifth Edition. Warsaw, Poland: OSCE/ODIHR.

38. U.S. Election Assistance Commission. (2011, September 14). Testing and Certification Technical Paper #2: A Survey of Internet Voting. Washington, D.C.

45. Beroggi, G. (2007) E-Voting through the Internet and with Mobile Phones. United Nations Public Administration Network.

48. Goodman, N., Pammett, J. H., & DeBardeleben, J. (2010, February). A Comparative Assessment of Electronic Voting. Ottawa, Canada.

57. Department of Defense. (2001, June). Voting Over the Internet Pilot Project Assessment Report. Prepared by the Federal Voting Assistance Program (FVAP). Washington, D.C.

60. The Electoral Commission. (2002, August). Modernising Elections: A Strategic Evaluation of the 2002 Electoral Pilot Schemes. London, United Kingdom.

62. The Electoral Commission. (2007, August). Key Issues and Conclusions: May 2007 Electoral Pilot Schemes. London, United Kingdom.

71. Kim, H. (2005, June 23). Risk Analysis of Traditional, Internet, and Other Types of Voting Alternatives for Town of Markham. Markham, Ontario.

75. McKinstry, J. (2010, January 26). Peterborough's Experience with Internet Voting. Presented at Policy Workshop – Internet Voting: What can Canada Learn? at Carleton University, Ottawa, Canada.

76. Mellett, C. (2010, January). HRM's Experience with Electronic Voting. Presented at Policy Workshop – Internet Voting: What can Canada Learn? at Carleton University, Ottawa, Canada.

83. Ministry of Local Government and Regional Development. (2006). Electronic voting – Challenges and Opportunities. Oslo, Norway.

84. Ministry of Local Government and Regional Development. (2011) Summary of the ISF Report. Retrieved on June 20, 2012, from http://www.regjeringen.no/nb/dep/krd/prosjekter/e-vote-2011-project/evaluering/evaluations-of-the-e-voting-trials/evaluations-of-the-e-voting-trials-in-201/summary -of-the-isf-report.htm?id=685824

94. Hastings, N., Peralta, R., Popoveniuc, S., & Regenscheid, A. (2011, February). Security Considerations for Remote Electronic UOCAVA Voting. Gaithersburg, Maryland: National Institute of Standards and Technology.

95. Regenscheid, A. & Hastings, N. (2008, December). Threat Analysis on UOCAVA Voting Systems. Gaithersburg, Maryland: National Institute of Standards and Technology.

99. New South Wales Electoral Commission. (2011, June). Technology Assisted Voting Audit: Post-Implementation Report. Sydney, Australia.

102. Office for Democratic Institutions and Human Rights. (2007, March 12) OSCE / ODIHR Election Assessment Mission Report: The Netherlands Parliamentary Elections 22 November 2006. Vienna, Austria.

109. State Chancellery. (2007, July). State Council's Report to the Grand Council on the Geneva Electronic Voting Project. Geneva, Switzerland.

118. U.S. Election Assistance Commission. (2011, April 6). Uniformed and Overseas Citizens Absentee Voting Act Registration and Voting Processes. Washington D.C.

120. Tennant, N. E. (2011, January 19). West Virginia Uniformed Services and Overseas Citizens: Online Voting Pilot Project. Charleston, West Virginia.

121. Elections BC. (2011, August). Discussion Paper: Internet Voting. Victoria, Canada: Elections BC.

123. Elections Ontario. (2011, November 15). Request For Proposal for the Provision of Network Voting System Internet and Telephone Pilot Project. Toronto, Canada: Elections Ontario.

130. International Idea. (2011, December). Introducing Electronic Voting: Essential Considerations. Stockholm, Sweden: International IDEA.

131. Goldsmith, B. (2011, May). Electronic Voting and Counting Technologies: A Guide to Conducting Feasibility Studies. Washington, D.C.: International Foundation for Electoral Systems.

132. Elections Ontario (2011). Network Voting System Internet and Telephone Pilot Project Description. Toronto, Canada: Elections Ontario.

135. Elections Canada. (2011, April 1). I-Voting Pilot Project Progress Report. Ottawa, Canada: Elections Canada.

136. Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009, June 26). Internet Voting in Comparative Perspective: The Case of Estonia. PS: Political Science and Politics, 42, 497-505.

139. Working Group on Digital Identity and Authentication. (2011, April 26). Detailed Use Cases for Digital Identity. British Columbia, Canada: Office of the Chief Information Officer.

140. Esteve, J. B. & Goldsmith, B. (2012, June). Compliance With International Standards: Norwegian E-Vote Project. Washington, D.C.: International Foundation for Electoral Systems.

141. Esteve, J. B., Goldsmith, B., & Turner, J. (2012, June). Speed and Efficiency of the Vote Counting Process: Norwegian E-Vote Project. Washington, D.C.: International Foundation for Electoral Systems.

142. Esteve, J. B., Goldsmith, B., & Turner, J. (2012, June). International Experience with E-Voting: Norwegian E-Vote Project. Washington, D.C.: International Foundation for Electoral Systems.

144. Nevo, S. & Kim, H. (2006). How to Compare and Analyze Risks of Internet Voting Versus Other Modes of Voting. E-Government: An International Journal, 3 (1), 105-112.

145. Kim, H. (2010, March 23). A Study of Internet Voting Security Risks and Accessibility Opportunities for the Town of Markham. Toronto, Canada.

146. Goodman, N., Pammett, J., & Debardeleben, J. (2010, Autumn). Internet Voting: The Canadian Municipal Experience. Canadian Parliamentary Review, 33(3), 13-21.

148. Ansper, A., Heiberg, S., Lipmaa, H., Overland, T. A., & van Laenen, F. (2011). Security and Trust for the Norwegian E-voting Pilot Project. Oslo, Norway: Ministry of Local Government and Regional Development.

150. Beaucamps, P., Reynaud-Plantey, D., Marion, J.-Y., & Filiol, E. (2009). On the use of Internet Voting on Compromised Computers. Rennes, France: Equipe Carte-Loria and Army Signals Academy Virology and Cryptology Laboratory.

152. Bochsler, D. (2010, May 26). Can Internet voting increase political participation? Remote electronic voting and turnout in Estonian 2007 parliamentary elections. Central European University, Budapest: Centre for the Study of Imperfections in Democracies.

154. Chowdhury, M. J. M. (2010). Comparison of e-voting schemes: Estonian and Norwegian solutions. University of Tartu, Estonia.

156. Election Process Advisory Commission. (2007, September 27). Voting with Confidence. The Hague: Ministry of Interior and Kingdom Relations.

157. Science and Technology Options Assessment. (2011, March 23) Can E-Voting Increase Electoral Participation? European Parliament.

164. Joint Standing Committee on Electoral Matters. (2009, March). Report of the 2007 Federal Election Electronic Voting Trials. Parliament of Australia. Canberra, Australia.

166. Kripp, M. (2011, March 11). Internet Voting in Estonia – Necessary to Maintain Turnout and Integrate Voters. Retrieved July 24, 2012 from http://www.e-voting.cc/en/internet-voting-in-estonia-necessary-to-maintain-turnout-and-integrate-voters-archive-032011

167. Nestas, L. H. (2010, June). Building Trust in Remote Internet Voting (Master's thesis). University of Bergen, Norway.

173. Puiggali, J. & Castello, S. G. (2012). Cast-as-Intended Verification in Norway. Paper presented at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

174. Puiggali, J. & Castello, S. G. (2012). Cast-as-Intended Verification in Norway. Presentation at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

176. Driza-Maurer, A., Spycher, O., Taglioni, G., & Weber, A. (2012). E-voting for Swiss Abroad: A Joint Project between the Confederation and the Cantons. Paper presented at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

180. Budurushi, J., Neumann, S., & Volkamer, M. (2012). Smart Cards in Electronic Voting: Lessons Learned from Applications in Legally-Binding Elections and Approaches Proposed in Scientific Papers. Paper presented at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

184. Stenerud, I. S. G. & BULL, C. (2012). When Reality Comes Knocking: Norwegian Experiences with Verifiable Electronic Voting. Paper presented at the EVOTE 2012 conference, Lochau/Bregenz, Austria.

187. Beckert, B., Lindner, R., Goos, K., Hennen, L., Aichholzer, G., & Strauβ, S. (2011, November). E-public, E-participation and E-voting in Europe - Prospects and Challenges. Brussels, Belgium: European Parliament.

190. Krimmer, R. & Volkamer, M. (2006). Observing Threats to Voter's Anonymity: Election Observation of Electronic Voting. Paper presented at the EVOTE 2006 conference, Lochau/Bregenz, Austria.

191. Office for Democratic Institutions and Human Rights. (2012, January 30). Swiss Confederation Federal Assembly Elections, October 23, 2011: OSCE/ODIHR Election Assessment Mission Report . Warsaw., Poland: OSCE/ODIHR.

192. Chevallier, M. (2003). Internet Voting: Status, Perspectives and Issues. Presentation to ITU E-Government workshop, Geneva, Switzerland.

194. State Chancellery. (n.d.) Discover the Video [Video file]. Canton of Geneva. Retrieved September 24, 2012, from http://www.geneve.ch/evoting/english/welcome.asp

195. State Chancellery. (2013). The Geneva Internet Voting System. Geneva, Switzerland: Imprimerie genevoise SA.

197. State Chancellery. (2009, September). History and Results of the Tests and Official Ballots. Retrieved 13 August, 2013, from http://www.geneve.ch/evoting/english/historique.asp

203. Regenscheid, A. & Beier, G. (2011, September). Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters. Gaithersburg, Maryland: National Institute of Standards and Technology.

204. E-Voting Working Group. (2012). Record of Discussion, May 3-4, 2012. Canada.

205. Capital Region Partnership. (2012, February 1). Internet Voting Pilot Proposal for 2013 Municipal Election. Edmonton, Canada.

206. Clark, J. (2011). Democracy Enhancing Technologies: Toward Deployable and Incoercible E2E Elections (Doctoral dissertation). University of Waterloo, Canada.

207. Delvinia. (2004). Internet Voting and Canadian e-Democracy in Practice: The Delvinia Report on Internet Voting in the 2003 Town of Markham Municipal Election. Markham, Canada.

208. Delvinia. (2011). eDemocracy and Citizen Engagement: The Delvinia Report on Internet Voting in the Town of Markham. Markham, Canada.

210. Elections Ontario. (2012, October). Network Voting Research Summary. Toronto, Canada: Elections Ontario.

211. Elections Ontario. (2012). Network Voting Business Case. Toronto, Canada: Elections Ontario.

213. Clark, J. (2012, November). Security Risks Related to Internet Voting. Presentation to Citizens' Jury on Internet Voting, Edmonton, Canada.

214. Goodman, N. (2012) An Assessment of Internet Voting in Canada. Presentation to Citizens' Jury on Internet Voting, Edmonton, Canada.

215. Goodman, N. (2012, November). Issues Guide: Internet Voting. Edmonton, Canada: University of Alberta.

216. Pammett, J. (2012, November). Internet Voting in Comparative Perspective: Context and Issues. Presentation to Citizens' Jury on Internet Voting. Edmonton, Canada.

217. Delvinia. (2012). Internet Voting In Markham. Presentation to Citizens' Jury on Internet Voting, Edmonton, AB.

218. Scytl. (2012) Security of the Internet Voting Trial: Security Components. Presentation to Citizens' Jury on Internet Voting, Edmonton, Canada.

223. New South Wales Electoral Commission. (2011, December 9). NSW State General Election and Clarence By-election iVote presentation. Sydney, Australia.

224. Gosse, R. (2012, November 2). Staff Report on Internet Voting to Finance and Corporate Services Committee. Kitchener, Canada.

226. Office of the City Clerk. (2013, February 6). City of Edmonton Internet Voting. Presentation to City Council, Edmonton, Canada.

227. Huycke, S. & Tecsa, T. (2012, September 28). City of Markham Online Voting Experience. Presentation to the Union of British Columbia Municipalities - 2012 Annual Convention, Victoria, Canada.

228. Habkirk, A. (2012, September 27). Voter Turnout: 2011 B.C. Local Government Elections. Presentation to Union of British Columbia Municipalities, Victoria, Canada.

231. Coleman, S. (2005). Just How Risky Is Online Voting? Information Polity, 10, 95-104.

233. Town of Truro. (2012, September). Voter Newsletter: Your guide to Elections 2012. The Town of Truro, Canada.

235. Council of Europe (2011, February 16). Guidelines on Transparency of e-Enabled Elections. Strasbourg, France.

236. Halifax Regional Municipality By-Law A-400 Respecting Alternative Voting. (2008). Halifax, Canada.

238. Billett, J. (2012, December 10). Finance and Corporate Services Committee (Meeting minutes). City Kitchener, Canada.

240. Cybernetica AS. (n.d.) Internet voting solution [Brochure]. Tallinn, Estonia.

241. Elections Canada. (2008, February). Strategic Plan, 2008-2013. Ottawa, Canada: Elections Canada.

242. Barette, P. (2013, February) Interest of Canadians in Internet Voting (2004, 2006, 2008 and 2011) (Research Note). Ottawa, Canada: Elections Canada.

244. Elections BC. (2013). 2013 Elections BC Post-election Voter/Non-Voter Satisfaction Survey. Victoria, Canada: Elections BC.

246. National Post Staff. (2012, March 27). Cyber attack on NDP leadership vote involved more than 10,000 computers. National Post. Retrieved from http://www.nationalpost.com

247. Perlroth, N., & Sanger, D. (2013, July 13). Nations Buying as Hackers Sell Flaws in Computer Code. New York Times. Retrieved from http://www.nytimes.com

248. Davis, S. & Kennedy, L. (2011, December 14) Potential use of Remote Electronic Voting Options: Internet Voting. Edmonton, Canada.

249. Seccuris. (2012, December 10). Executive Summary: Business and Technical Threat Risk Assessment for Electronic Voting.

250. Whittaker, P. (2012, October 19). Letter to Capital Regional City Managers re: Joint Internet Voting Pilot. Alberta, Canada; Government of Alberta Ministry of Municipal Affairs.

251. City of Edmonton. (2013). Internet Voting. Retrieved July 19, 2013, from http://www.edmonton.ca/city_government/municipal_elections/internet-voting.aspx

252. Rodrigues, A. (2013, February 6). Edmonton City Council Shelves Online Voting Idea. Edmonton Sun. Retrieved from http://www.edmontonsun.com

253. MacKinnon, L. (2013, April 30). Elections Canada Drops Plan For Online Voting Due to Cuts. CBC News. Retrieved July 19, 2013, from http://www.cbc.ca

254. ERR News. (2013, July 12). E-Voting Source Code Made Public. Retrieved July 22, 2013, from http://news.err.ee/politics/0233b688-b116-44c3-98ca-89a4057acad8

255. Centre for Public Involvement. (2012, November). Citizens Jury on Internet Voting Expert Witness Information Package. Edmonton, Canada.

256. Elections BC. (2013, June 23) Voting Results Change History Report, Saanich North and the Islands, 40th Provincial General Election. Victoria, Canada: Elections BC.

257. Estonian National Electoral Committee. Statistics about Internet Voting in Estonia. Retrieved July 23, 2013, from http://vvk.ee/voting-methods-in-estonia/engindex/statistics

258. Office of the Chief Information Officer. (2013, June 18). BC Services Card: The Possibilities. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

260. Lychkovakh, O. (2012, March). Success Case: Norway Local Government Elections. Scytl.

261. State Chancellery. (2013). List of all eEnabled official ballots conducted in Geneva since the start of the Internet voting project. Geneva, Switzerland.

263. Neufeld, H. (2013, March). Compliance Review: Final Report and Recommendations. Ottawa, Canada.

264. Jefferson, D., Rubin, A. D., Simons, B., & Wagner, D. (2004, January 21). A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE). United States.

265. Department of Defense. (2007, May). Department of Defense: Expanding the Use of Electronic Voting Technology for UOCAVA Citizens. Washington, D.C.

266. Jefferson, D., Rubin, A. D., & Simons, B. (2007, June). A Comment on the May 2007 DOD Report on Voting Technologies for UOCAVA Citizens. United States.

267. Schwartz, J. (2004, January 21). Report Says Internet Voting System Is Too Insecure to Use. New York Times. Retrieved from http://www.nytimes.com

268. National Association of Secretaries of State. (2009, November). NASS Summary of the Military and Overseas Voter Empowerment Act (MOVE Act).

269. West Virginia Secretary of State. (2012, September 13). Tennant: West Virginia's Military, Veterans, and Overseas Citizens Have Several Convenient Voting Options. Retrieved on August 13, 2013, from http://www.sos.wv.gov/news/topics/elections-candidates/Pages/TennantWestVirginiasMilitaryVeteransandOverseas.aspx

270. West Virginia Secretary of State. (2010, May 21). West Virginia's Internet Voting Pilot Program Featured In Pew Center Newsletter. Charleston, West Virginia. Retrieved on August 13, 2013, from http://www.sos.wv.gov/news/topics/elections-candidates/Pages/WestVirginia'sInternetVotingPilotProgramFeaturedInPewCenterNewsletter.aspx

271. Moretti, M. (2010, May 20). Internet voting for military, overseas voters debuts in West Virginia - Clerks and secretary of state pleased with first use. Electionline Weekly.

272. Collins, B. (2012, May 18). NIST Activities on UOCAVA Voting. Gaithersburg, Maryland: National Institute of Standards and Technology.

273. Ministry of Local Government and Regional Development. (2012, December 17). Internet voting pilots announced for 2013 [Press release]. Retrieved from http://www.regjeringen.no/en/dep/krd/press/press-releases/2012/new-pilot-with-internet-voting-in-2013.html?id=710138

274. Joye, C., Smith, P., & Kerin, J. (2013, July 27). Spy Agencies Ban Lenovo PCs on Security Concerns. Australian Financial Review. Retrieved from http://www.afr.com/

275. Vassil, K. & Weber, T. (2009, September). A Bottleneck Model of E-voting: Why Technology Fails to Boost Turnout. Paper presented at the Annual Meeting of the American Political Science Association, Toronto, Canada.

276. Trechsel, A. & Vassil, K. (2010, January). Internet Voting In Estonia: A Comparative Analysis of Four Elections since 2005. Florence, Italy: European University Institute.

278. Mellett, C. (2013, July 5). Personal communication.

279. Mellett, C. (2013, February 8). Electronic Voting 2012: Municipal and School Board Elections. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

280. Office of the e-Envoy. (2002). In the Service of Democracy: A Consultation Paper on a Policy for Electronic Democracy. London, United Kingdom.

281. Halderman, J. A. (2013, January 25). Internet Voting: What are the Security Risks? Presentation to Independent Panel on Internet Voting, Victoria, Canada.

282. Rivest, R. (2013, January 25). Is Internet Voting a Good Idea? Presentation to Independent Panel on Internet Voting, Victoria, Canada.

283. Elections BC. (2012, November 7). British Columbia's Current Voting Model. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

284. Ministry of Community, Sport and Cultural Development. (2012, December 19). Local Government Election Model in B.C. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

285. Local Government Elections Task Force. (2010, January). Backgrounder on Local Government Elections. Victoria, Canada.

286. Volkamer, M. (2013, February 9). Electronic Voting. Presentation to Independent Panel on Internet Voting, Victoria, Canada

287. Elections Ontario. (2013, February 8). Elections Ontario's Alternative Voting Technology Review. Presentation to Independent Panel on Internet Voting, Victoria, Canada.

289. Butts, R. (2013, January 15). Review of the 2012 Municipal and School Board Elections. Information Report to Halifax Regional Municipality Council. Halifax, Canada.

290. Butts, R. (2011, September 27). 2012 Municipal and School Board Elections. Recommendations Report to Halifax Regional Municipality Council. Halifax, Canada.

291. Mellett, C. (2013, June 19, 2013). Personal communication.

292. Elections Ontario. (2013, June). Alternative Voting Technologies Report - Chief Electoral Officer's Submission to the Legislative Assembly. Toronto, Canada: Elections Ontario.

293. Huycke, S. & Tecsa, T. (2012, November 13). Markham Votes 2014 - Internet Voting Program. Presentation to Special General Committee Meeting, Markham, Canada.

294. Ernst & Young. (2012, October 23) Specified Auditing Procedures Report: Electronic Voting - Halifax Regional Municipality. Halifax, Canada.

295. Goodman, N. (2013, July 15). Personal communication.

296. Town of Truro 2012 Elections. Retrieved from http://www.facebook.com/pages/Town-of-Truro-2012-Elections/528265507199852

297. Kennedy, L. (2012, November 23). The Edmonton Jellybean Election Experience. Presentation to Citizens' Jury on Internet Voting, Edmonton, Canada.

304. Oostveen, A.-M. (2010, September). Outsourcing Democracy in the Netherlands: The Risk of Contracting Out E-Voting to the Private Sector. Paper presented at 'Internet, Politics, Policy 2010: An Assessment' conference, Oxford, United Kingdom.

305. Jacobs, B. & Pieters, W. (2009). Electronic Voting in the Netherlands: from early Adoption to early Abolishment. Netherlands.

306. Teague, V. & Wen, R. (n.d.) Problems with the iVote Internet Voting System. The Computing Research and Education Association of Australasia. Australia.

310. Ostvold, B. M. & Karlsen, E. K. (2012). Public Review of E-Voting Source Code: Lessons learnt from E-Vote 2011. Paper presented at the NIK-2012 conference, Bodo, Norway.

317. Letter to T.D. Rust and Virginia Joint Committee on Technology & Science. (2012, July 11).

321. New South Wales Electoral Commission. (2013, August). iVote Strategy for the NSW State General Election 2015 - Key Issues, Guidelines, Application Architecture and Voting Protocol. Sydney, Australia.

323. Mayrand M. (2012, June 24). Personal communication. Halifax, Nova Scotia.

324. Ministry of Local Government and Regional Development. (2013, September 5). Seminar on Internet Voting. Retrieved from http://www.regjeringen.no/en/dep/krd/lyd_bilde/nett-tv/seminar-on-internet-voting.html?id=735137

325. Kiniry, J., Morkan, A., Cochran, D. & Fairmichael, F. (2007). The KOA Remote Voting System: A Summary of Work To-Date. Trustworthy Global Computing, 244-262. Springer Berlin Heidelberg.

329. Ministry of Local Government and Regional Development. (2013, September 9). Decryption and Counting Ceremony of the Internet Votes, English Language. Retrieved from http://www.regjeringen.no/nb/dep/kmd/lyd_bilde/nett-tv/decryption-and-counting-ceremony-of-the-.html?id=735138

330. Ministry of Local Government and Regional Development. (2013, September 6). Protection of the Internet Votes. Retrieved from http://www.regjeringen.no/en/dep/krd/lyd_bilde/nett-tv/seminar-on-internet-voting.html?id=735137

331. Ministry of Local Government and Regional Development. (2013, September). How to Vote Via the Internet in the Parliamentary Election 2013. Retrieved from http://www.regjeringen.no/pages/597658/how_to_vote_internet.pdf

332. Brightwell, I. (2013, November 1). Personal communication. New South Wales, Australia.

333. Office for Democratic Institutions And Human Rights. (2013, December 16) OSCE/ODIHR Election Assessment Mission Final Report: Norway Parliamentary Elections 9 September 2013. Warsaw, Poland.

334. Statistics Canada. (2013, December). Canadian Survey on Disability, 2012. Ottawa, Canada.

335. Elections BC. (2013, December 18). Personal communication.

336. Elections BC. (2014, January 15). Personal communication.

337. Elections BC. (2014, January 17). Personal communication.

338. Elections BC. (2014, January 21) Statement of Votes for the 40th Provincial General Election. Victoria, Canada.

APPENDIX F - EXPERIENCE WITH INTERNET VOTING IN OTHER JURISDICTIONS

The use of Internet voting is not as widespread as some may think. Of the 11 countries to have used Internet voting for at least one binding governmental election, only jurisdictions in seven countries still do.[65] Most implementations of Internet voting are limited to local government elections or to subsets of the entire voting population (e.g., remote voters). The jurisdictions highlighted in this appendix were chosen by the panel to be the most prominent, or to have the most representative experiences with Internet voting to British Columbia (whether implemented or investigated and rejected). These summaries are examples and do not represent an exhaustive list of Canadian or global Internet voting experiences. The amount of detail provided in the summary for each jurisdiction varies, in part due to the amount of, and detail in, existing research available for those elections.

Canada - Implemented

Markham, Ontario[66]

Origins

Until the 2008 Local Government Elections in the Halifax Regional Municipality, Markham, Ontario was the largest jurisdiction in Canada to implement Internet voting. Markham conducted its first local government election using Internet voting in 2003 with a hope that it would reverse a declining level of voter turnout. While this goal was not realized, the city felt that Internet voting would prevent a further decrease in voter turnout and allow it to provide a convenient and cost effective voting opportunity. For these reasons, among others, Markham has since conducted two additional mayoral and councillor elections in 2006 and 2010 and is making preparations to include an Internet voting option for the 2014 elections. In each election Markham has only provided in-person and Internet voting opportunities – it does not permit telephone voting or voting by mail, though it is considering the feasibility of adding telephone voting in 2014 as well as increasing the number of days for Internet voting or expanding Internet voting up to and including general voting day. The city utilizes a Request for Proposals (RFP) process ahead of each election to select its Internet voting system.

Process

Registered voters in Markham must register separately in order to use Internet voting using a two-stage process. All registered voters are sent a package in the mail that contains a unique Personal Identification Number (PIN) that the voter can use along with the voter's date of birth (DOB) to log into Markham's Internet voting registration website. On the website the voter creates a personalized password and will use this password along with a new PIN sent to the voter in the mail in order to vote.

65 Reference #142
66 For more information about Markham's experience with Internet voting, see references #38, 48, 71, 142, 145, 146, 207, 208, 214, 215, 217, 227, 293

In Markham, Internet voting was offered twenty-four hours a day during the advance voting period. In 2003, the advance voting period was 5 days, and in 2006 and 2010 it was increased to 6 days. Ahead of its next election in 2014, Markham is considering the feasibility of increasing the number of days for Internet voting even further or expanding Internet voting up to and including general voting day. It is also planning to add expanded audit capabilities to both its Internet voting processes and technology.

Markham's implementation of Internet voting permitted under-votes,[67] but not over-votes.[68]

	2003	2006	2010
Population	~230,000	~260,000	~300,000
Eligible voters	158,000	164,000	164,000
Overall turnout (#)	42,198	61,948	65,927
Overall turnout (%)	28.0%	37.9%	35.5%
Internet voting registration (#)	11,708	16,251	17,231
Internet voting turnout (#)	7,210	10,639	10,597
Internet voting as % of eligible voters	4.5%	6.5%	5.7%
Internet voting as % of votes cast	17.1%	17.2%	16.1%
When offered	5 days during advance voting period; 24h/d	6 days during advance voting period; 24h/d	
Vendor	ES&S	ES&S	ES&S and Intelivote

Results

The introduction of Internet voting in Markham has not led to the increase in voter turnout once expected, but it does consider Internet voting to be a success. City staff point to its repeated use by voters and the high levels of voter satisfaction reported in post-election experience surveys. Convenience has become the primary rationale for continuing with Internet voting, though city staff also consider Internet voting to be a way to help maintain the election budget at current levels.

Analysis of the Markham voter turnout research shows that Internet voting is used primarily by middle-aged voters[69] (the age cohort that also has the highest levels of voting using traditional voting opportunities) and does not appear to lead to increased voting by younger voters.

67 Under-vote: Marking the ballot for no candidate, or fewer than the maximum number allowed in the race; where only one vote was permitted this results in the ballot being rejected; where multiple choices are permitted, the valid markings are still recorded; often this occurs on purpose to indicate a protest vote, but can also occur unintentionally

68 Over-vote: Marking the ballot for more than the maximum allowable number of candidates; this results in the ballot being rejected for that race and no vote recorded

69 66% of all Internet ballots in Markham were cast by voters aged 40-69.

While Markham has one of the longest histories with Internet voting in Canada and reports high levels of voter satisfaction with the system, Internet voting still only makes up approximately 16% of all votes cast in the election. Furthermore, the number of Internet ballots cast in 2010 did not change significantly from 2006 despite an increase of almost 4,000 votes overall from one election to the next.

Halifax, Nova Scotia[70]

Origins

At the request of the council, Halifax Regional Municipality (HRM) staff first began to examine alternative voting methods in 2004. In 2005, amendments to the Nova Scotia *Municipal Elections Act* allowed for alternative voting methods to be introduced at the local government level, provided that the local government passed an authorizing by-law. In 2007, HRM council approved Internet and telephone voting[71] for the 2008 HRM municipal and school board elections as an additional voting channel during the advance voting period. The council established a number of goals for the Internet voting system, including increasing convenience (particularly for Halifax's older voters), potentially increasing voter turnout, improving cost effectiveness, and reducing the time required for vote counting and reporting.

Based on the success of the 2008 election, it was trialled again in a 2009 council by-election, and from the combined experience council approved its use again for 2012. In both cases it was also limited to the advance voting period.

Following an RFP ahead of the 2008 election, HRM entered into a four-year contract with a vendor to conduct all Internet voting. Prior to the 2012 election HRM conducted another RFP process. Three proponents met the requirements and HRM entered into a contract with a different vendor to conduct that election.

Process

All registered HRM voters are sent credentials (PIN) by mail ahead of the election. The provided PIN plus the voter's date of birth (DOB) were used for authentication credentials in 2008 and 2009. In 2012, officials added a password as a third credential to be used along with the PIN and DOB. In all three elections, voters were also required to complete a CAPTCHA challenge as part of the log in process.[72]

70 For more information about HRM's experience with Internet voting, see references #38, 48, 76, 146, 236, 278, 279, 289, 290, 291, 294
71 All subsequent references will be to the Internet voting component only.
72 The effectiveness of the CAPTCHA technology to prevent automated logins is debated by researchers.

In 2008, Internet voting was offered twenty-four hours a day during the three day advance voting period, in addition to traditional voting opportunities. In the 2009 by-election, it was expanded to five days and in-person voting was reduced to one location only. In 2012, Internet voting was expanded to 13 days prior to general voting day and in-person voting during the advance voting period was eliminated entirely. On general voting day only in-person voting was available.

The Internet voting system in Halifax enables voters to spoil a ballot using a "decline to vote" button on the same screen as the candidate choices. Voters may choose to vote online at different times and via different devices (e.g., phone, work computer, home computer) for each race they are eligible to vote in (e.g., mayor, councillor, school board trustee), as opposed to having to complete all ballots in a single session. A voter is only entitled to vote once in each race and voters cannot vote online for some races and in-person for others.

Halifax also established voter registration sites in libraries during the advance voting period to enable previously unregistered voters the opportunity to register and become eligible to vote (including online).

Results

It is suspected that not requiring voters to pre-register to vote online (only to already be a registered voter) was one of the reasons for the higher level of Internet voting turnout in HRM than in Markham and other jurisdictions that required secondary registration.

The significant increases in Internet voting turnout in 2009 and 2012 are likely due in part to the reduced number of in-person voting opportunities in those same elections (only one voting place in 2009, and no advance voting places in 2012). Ninety percent of all electronic votes were cast online and only 10% were cast by telephone.

While turnout overall is not increasing, 60% of all ballots cast in 2012 were cast online. This suggests that Internet voting is widely accepted by voters in Halifax and may be considered to be more convenient for a majority of voters than in-person voting opportunities.

	2008	2009 (district by-election)	2012
Population	~385,500	~385,500	~390,000
Eligible voters	279,326	12,476	298,209
Overall turnout (#)	101,116	4,391	110,114
Overall turnout (%)	36.2%	35.2%	36.9%
Internet voting registration (#)	N/A	N/A	N/A
Internet voting turnout (#)	~25,000	3,258	66,272*
Internet voting as % of eligible voters	9.0%	26.1%	22.2%
Internet voting as % of votes cast	24.7%	74.2%	60.2%
When offered	Three days during advance voting period; 24h/d	Five days from beginning of advance voting period to end of general voting day; 24h/d	13 days during advance voting period; 24h/d
Vendor	Intelivote		Scytl

*These figures include Internet and telephone voting. Internet voting accounts for 90% of all electronic votes cast, or approximately 59,645 ballots.

Truro, Nova Scotia[73]

Origins

In December 2011 the Chief Administrative Officer (and election administrator) and a representative of an Internet voting vendor made a presentation to council recommending the use of Internet voting in the October 20, 2012, local government election. Council took it under advisement and in April 2012 approved a bylaw permitting Internet voting and establishing that there would be no voting with paper ballots.

The goals of Truro were to increase voter turnout, improve convenience and access, and to try to reach younger voters while promoting the progressiveness of the town.

Process

All voting took place online and was offered over a nine-day period. All registered voters were sent a PIN by mail ahead of the election. This PIN plus the voter's date of birth were used for authentication credentials. Truro used the list of voters for the town provided by Elections Nova Scotia.

73 For more information about Truro's experience with Internet voting, see references #214, 233, 295, 296

In an effort to replicate the traditional social experience, and to assist older voters in the community, the city set up computers for voting in four prominent locations. The city also appointed nursing home staff as election officials to assist elderly voters resident in long term care facilities.

Officials maintained a Facebook election page where they provided the public with regular updates of the number of votes cast. The page also contained encouragements to vote and links to YouTube videos demonstrating how to vote online.

Results

Turnout in the 2012 election increased from 19% of eligible voters to 47%. While this is a significant increase, it may not be attributed solely to the introduction of Internet voting. For the same election, Truro officials conducted a new comprehensive education and outreach program. The local returning officer wrote an election-administration column in the local newspaper for the six months preceding the election. Topics varied, but at least one column was written about the introduction of Internet voting. It is believed that this outreach contributed to the positive reception of Internet voting by the media and by voters.

	2012
Population	~12,000
Eligible voters	9,680
Overall turnout (#)	4,549
Overall turnout (%)	47%
Internet voting registration (#)	N/A
Internet voting turnout (#)	4,549
Internet voting as % of eligible voters	47%
Internet voting as % of votes cast	100%
When offered	9 days during Internet voting; 24h/d
Vendor	Intelivote

Canada - Investigated and rejected

Kitchener, Ontario[74]

Circumstances for its consideration and why it was ultimately rejected

In June 2011, City of Kitchener council directed staff to investigate implementing an Internet voting option for the 2014 municipal election and report back on the issue by the end of 2012. On November 2, 2012, the City Clerk submitted a report to council recommending that Kitchener not implement Internet voting and on December 10, 2012, a committee of council agreed with the Clerk's report not to implement Internet voting.

74 For more information about Kitchener's consideration of Internet voting, see bibliography references #224, 238

The Clerk's report was fulsome and reflected consideration of many of the most significant benefits and challenges to implementing Internet voting.

The Clerk's report claimed that the overall cost of the system, including the cost of ensuring the system would be secure enough for candidates and the public to have confidence in it, would be too great, particularly when added to the cost of the existing paper ballot process. Further, the Clerk wrote that research suggests it does not increase voter turnout (particularly among younger voters), that it cannot be adequately scrutinized, that there is not an established Canadian standard for evaluating Internet voting systems, and that its legitimacy hadn't been tested in the courts.

Edmonton, Alberta[75]

Circumstances for its consideration and why it was ultimately rejected

In 2010, Edmonton city council first asked municipal staff to look into the possibility of implementing Internet voting for city elections. In February 2012 the capital region communities of City of Edmonton, City of St. Albert and Strathcona County submitted a joint proposal to the provincial Ministry of Municipal Affairs requesting permission to conduct a pilot project for the 2013 Alberta municipal elections. These municipalities wrote that their proximity, experience with advanced voting techniques, and size (one large, one mid-sized, and one rural/urban municipality) warranted a joint project. The original objective of a pilot focused on convenience.

Funded by the Ministry of Municipal Affairs, the City of Edmonton conducted a mock election using Internet voting technology from Scytl to evaluate voters' readiness to use Internet voting and to test the technology to see if it met the city's requirements. To avoid political opinions influencing the pilot, the city asked voters to vote on their favourite colour of jellybean.

There were no eligibility requirements for who could participate, but all voters were required to register with the city by completing an online registration form and uploading a copy of their ID. While the city stated it had hoped for a large number of voters, fewer than 500 individuals participated in the pilot.

Edmonton contracted with a third party to test the security of the Internet voting system used. When another group of computer security experts[76] requested permission to attempt to compromise the system, they were denied permission. The city reported that thirteen attempts to compromise the voting system were made, but that all were repelled. Of the thirteen attempts, five were invited and eight were not.

Satisfied with the Jellybean Internet Voting pilot, the City Clerk developed a review process with the Centre for Public Involvement (a City of Edmonton and University

75 For more information about Edmonton's consideration of Internet voting, see bibliography references #205, 218, 226, 248, 249, 250, 251, 252, 255, 297

76 These experts included: Jeremy Epstein, Barbara Simons, Ronald L. Rivest, and David Jefferson.

of Alberta group created for public engagement projects) to further assess the receptiveness of the city for Internet voting. This review included a survey of residents, roundtable meetings with stakeholders and, most prominently, a citizens' jury process.

The Citizens' Jury was made up of 17 (originally 18) residents of Edmonton selected at random from the previous survey respondents. In November 2012, jurists participated in one weekend learning session where they heard about some Internet voting benefits and challenges from practitioners, academics and vendors. Presenters to the jury put lots of emphasis on the social benefits to the city (to be seen as a leader in the field, civic pride, keeping up with other cities) if it adopted Internet voting. Jurists were not expected to become experts on Internet voting, but based on what they learned during the weekend were to give their opinion as to whether Edmonton should adopt Internet voting as an option for future municipal elections. The City Clerk indicated during the weekend that she would only recommend to Council that the city implement Internet voting in 2013 if the Citizens' Jury also recommended so. At the end of the weekend the jury, by consensus, enthusiastically recommended the city implement Internet voting at the 2013 municipal election.

In January 2013 the Clerk reported to council she was recommending Internet voting be adopted as another option for voting in the 2013 Edmonton municipal election. However, at the February 6, 2013, council meeting, council decided not to proceed with Internet voting. Council stated that it was concerned at the cost and security of Internet voting and the Mayor stated that convenience was not enough of a reason to implement it.

Ahead of the council meeting, an individual reported to the media he had registered more than once and cast a ballot under each registration instance. Although the way in which the voter registered multiple times was unrelated to the Internet voting technology, based on the deliberations of the council, the panel suspects this announcement contributed to the security concerns of council.

In March 2013, the Minister of Municipal Affairs announced that the provincial government would not authorize Internet voting for any Alberta municipality for the 2013 elections, but would continue to monitor Internet voting for future use.

Canada (federal)[77]

Circumstances for its consideration and why it was ultimately rejected

Since 2004, Elections Canada has been surveying Canadians on the subject of Internet voting to learn of their interest and concerns. In addition to this polling and being a supporter of Internet voting research generally, in 2008 Elections Canada, in its five-year strategic plan, proposed trialing Internet voting in a by-election by 2013. By 2009 it had refined its plan to conduct such a trial after March 2013. Such a trial was dependent on Parliamentary approval and was to be limited in scope to voting terminals used in a controlled environment, such as by military voters using a military network. Limiting the scope in this way would allow Elections Canada to control many of the Internet voting security and authentication issues.

Despite the interest in the pilot, the Chief Electoral Officer did not believe that Internet voting would become a permanent channel for voting in federal elections for at least three general elections.

In April 2013, after budget cuts took effect at Elections Canada, the Chief Electoral Officer announced that Elections Canada had no immediate plans for a pilot before the 2015 general election. In addition to budget pressures, the issue of authentication and concerns over data security, it is likely that current initiatives focused on significant changes to the voting process at the federal level may have factored into the decision not to conduct the pilot as originally planned. The Chief Electoral Officer reported to Parliament that Elections Canada will continue to monitor the issue and consider an Internet voting pilot project again after the 2015 general election.

Ontario[78]

Circumstances for its consideration and why it was ultimately rejected

In the context of broader legislative changes to the provincial *Election Act* that placed an increased emphasis on the issue of accessibility, amendments to the *Election Act* in 2010 required Elections Ontario to review alternative voting technologies[79] and report back to the Legislative Assembly by June 2013. The new legislation also permitted Elections Ontario to use alternative technologies in a general election, provided it met three conditions: that it was first tested in a by-election; that the Chief Electoral Officer recommended it, having first been satisfied as to issues of security and integrity; and that the Legislative Assembly approve it after holding public hearings.

---

77 For more information about Elections Canada's consideration of Internet voting, see references #135, 241, 242, 253, 263, 292, 323

78 For more information about Ontario's consideration of Internet voting, see references #123, 132, 210, 211, 287, 292

79 Alternative voting technologies was defined by Elections Ontario as: "a means of both casting and counting votes electronically, involving the transmission of ballots and votes via telephones, private computer networks, or the Internet". Elections Ontario shortened this to "network voting" and established that it was meant to refer to Internet or telephone voting. For consistency, this report will describe Elections Ontario's work as related to Internet voting.

Elections Ontario initially announced it would use alternative voting technologies in a by-election pilot project in 2012 to inform its research. Elections Ontario developed a business case for Internet voting that established very detailed requirements for an Internet voting system and used those requirements to put together an RFP for an "off-the-shelf" system to be tested in a by-election. However, in the spring of 2012, Elections Ontario determined that a pilot would not be feasible in 2012. Elections Ontario "determined that it would introduce more complexity and security issues, operational challenges and risk than originally anticipated" and that the organization did not have sufficient time "to determine whether these risks could be adequately resolved."[80]

In June 2013 Elections Ontario submitted its report on Internet voting to the legislature. The report stated that none of the current technologies met all of its implementation criteria (accessibility, individual verifiability, one vote per voter, voter authentication and authorization, only count votes from valid voters, voter privacy, results validation, and service availability) and so would not move forward with Internet voting at that time; however, it would continue to monitor the systems and processes that come forward against those criteria so that it could make a recommendation for Internet voting "when it is warranted".[81]

Other jurisdictions - Implemented

Estonia[82]

Origins

After the creation of a secure national electronic ID card in 2002, the Estonian government began investigating Internet voting in 2003 and in 2004 decided it would be piloted in the 2005 Local Government Elections. After deciding to go ahead with Internet voting it contracted with a private firm for the system's development. The initial goals of Internet voting were convenience and increasing voter turnout, particularly among youth.

The Estonian president challenged the constitutionality of the Internet voting system implemented due to a concern that the decision to allow an individual to cast more than one ballot contravened the principle of one person, one vote. However the Supreme Court upheld the Internet voting legislation, ruling that although a voter could cast more than one ballot, this process was only going to be used to protect the secrecy of the ballot, and ultimately only one vote per person would be counted.

80 Reference #292
81 Reference #292
82 For more information about Estonia's experience with Internet voting, see references #48, 136, 142, 152, 154, 166, 240, 254, 257, 276

Process

Estonia mandates a national ID card with a digital chip for interaction with government services. Card readers are widely available in public terminals and home computers. This card plus a unique PIN is used by voters to authenticate themselves for all government services, including voting.

Internet voting has been used for the 2005 Municipal Elections, 2007 National Parliamentary Elections, 2009 Municipal Elections, 2009 European Parliamentary Elections and 2011 National Parliamentary Elections.

Estonian elections are guided by three principles:

- secure digital authentication;
- "re-voting" (casting a ballot multiple times, but only the final ballot is counted); and
- supremacy of the paper ballot (a ballot cast in person on general voting day supersedes any electronic ballots cast)

Internet voting is only available for a limited number of days prior to general voting day and uses an electronic "double envelope" system comparable to the secrecy/ certification envelope process used for absentee voting in B.C. provincial elections. The system does not use end-to-end verification methods and the voter cannot independently verify that their ballot was successfully cast.

Results

There were several key success factors to its implementation: a high level of computer literacy; high-level of computer access; the existing electronic ID card; political will; and a legal framework for Internet transactions. Access to the Internet is a social right of Estonians enshrined in legislation.

Use of Internet voting has increased significantly since it was first introduced, but after five elections it is still only used by less than 16% of eligible voters.

	2005 (municipal)	**2007** (national)	**2009** (local government)	**2009** (European Parliament)	**2011** (national)
Population	~1,346,000	~1,342,000	~1,340,000	~1,340,000	~1,340,000
Eligible voters	1,059,292	897,243	1,094,317	909,628	913,346
Overall turnout (#)	502,504	555,463	662,813	399,181	580,264
Overall turnout (%)	47.4%	61.9%	60.6%	43.9%	63.5%
Internet voting registration (#)	N/A				
Internet voting turnout (#)	9,317	30,275	104,415	58,669	140,846
Internet voting as % of eligible voters	0.9%	3.4%	9.5%	6.5%	15.4%
Internet voting as % of votes cast	1.9%	5.5%	15.8%	14.7%	24.3%
When offered	Three days; 24h/d	Three days; 24h/d	Seven days; 24h/d	Seven days; 24h/d	Seven days; 24h/d
Vendor	Cybernetica AS				

Norway[83]

Origins

In 2008, the Norwegian Parliament approved an Internet voting pilot at the request of the governing party. The pilot consisted of 10 municipalities offering an Internet voting option in addition to existing voting opportunities during the local government elections in September 2011 and was overseen by the federal Ministry for Local Government and Rural Development. The ten pilot municipalities were chosen by the Ministry to participate out of the 428 municipalities in Norway. Goals of the pilot project were to increase accessibility and convenience, improve efficiencies in election administration, and facilitate direct democracy. The Ministry contracted with Scytl to provide the Internet voting system for the pilot and with Norwegian technology company ErgoGroup (now EVRY) to provide an elections management system and integrate the two systems. The Ministry contracted with an independent auditor (Der Norske Veritas) to audit the software development process and with additional security auditors to review the source code.

Local government elections require a complex ballot due to the electoral system used in Norway (open list proportional representation)[84] and so potential efficiencies (time and resources) in counting and reporting were significant, as was the potential for a reduction in errors during counting. Each local government sets its own rules and procedures for counting (some count ballots by hand and others use vote tabulation machines). Each municipality involved in the pilot trialled the chosen technology in youth council elections and referenda six to twelve months ahead of the municipal elections.

83 For more information about Norway's experience with Internet voting, see references #38, 48, 82, 83, 84, 140, 141, 142, 148, 154, 173, 174, 184, 260, 273, 324, 329, 330, 331, 333

84 Open list proportional representation permits voters to express multiple preferences when marking the ballot.

Process

Ahead of the election, all voters in the pilot municipalities received unique verification codes by mail. Voters used their electronic national ID (MinID) to authenticate themselves prior to voting online. The online ballot was randomized and voters selected parties and candidates with a point-and-click interface. The system was designed to prevent over-votes, but did allow under-votes, including the casting of a blank ballot. Voters were shown their completed ballot before it was officially cast.

The voting system utilized E2E verification with return codes. Immediately after casting the ballot the voter received a verification code by SMS which could be compared against the unique verification codes mailed to the voter prior to the election. This enabled the voter to verify their votes were received as cast. Cryptography (digital signatures, hash functions and zero knowledge proofs) ensured each ballot was included in the counting and hashes of every ballot are published after the election to allow voters to verify that their vote was counted.

Voters were permitted to cast multiple ballots, but only the last ballot cast would ultimately be counted (maintaining the principle of one vote per person). Voters could also vote in-person at advance voting or on general voting day. Any ballot cast in-person superseded any ballots cast online. These two features meant that Internet ballots could not be counted until all in-person voters had been identified at the end of general voting day. Norwegian pilot municipalities used electronic strike-off systems in voting places to enable rapid identification of in-person voters and minimize delays prior to counting.

There were three phases of counting:

- **Cleansing:** removed duplicate ballots from a single voter and all ballots from an in-person voter, and removed personal identifiers associated with Internet ballot to enable the secret ballot
- **Mixing:** re-encryption of all cleansed ballots, which were then stored in a different order; this process severed any links with the state of the ballots during the cleansing phase and the order of ballots cast
- **Tallying:** decryption of the votes using keys distributed among multiple key holders (i.e. election administrators, stakeholders, etc.) and tallying the number of votes for each candidate

Results

Utilizing some of the more advanced options presented to them, over one thousand voters cast multiple ballots (the most any individual cast was five), and over 650 voters voted in-person after casting an Internet ballot. In all cases, the latter of the final ballot cast online or the in-person ballot was the only ballot considered for each voter.

Online turnout among youth (16-17 year olds) was found to be lower than other age categories.[85] Anecdotal evidence suggests that younger voters preferred to vote in-person for social reasons.

Contrary to expectations, researchers found no statistically significant reduction in the amount of time required to count ballots compared to control municipalities. Rather, experience from the previous municipal election was a stronger influence on the amount of time counting took. The number of counting staff in pilot municipalities was almost 70% lower than in control municipalities, however researchers could not attribute all this difference to the use of Internet voting.

At the national level, resources required to manage the Internet voting project in the ten municipalities were quite low – two staff for the entire pilot, with an estimate of three staff needed for all local government elections.

Norway considered the high level of use as an indication the Internet voting option was trusted by voters. Voter turnout and level of trust in Norwegian political institutions is already much higher than average. Researchers on behalf of the election administration conducted a survey of voters and stakeholders after the election. They found:

- Level of trust in counting was lower for Internet voting than traditional methods, but was still high ("85% indicated a great deal of trust or some trust" in Internet voting compared to 92% for hand-counting paper ballots and 94% electronically tabulated paper ballots)
- Receipt of verification code created confidence, even though the number of people who verified it was suspected to be low
- Most voters accepted the security as adequate, or didn't question it; researchers hypothesise that voters who were not satisfied simply used paper ballots
- Stakeholders from pilot municipalities expressed positive feedback, trust, and wanted it used again ("reserved optimism")
    - local officials expressed concern with the accuracy of hand-counting and machine-counting of ballots

85 Norway also piloted voting by 16-17 year olds in 20 municipalities during the 2011 local government elections. Four municipalities were involved in both the youth voting pilot and the Internet voting pilot.

- National stakeholders, including political parties and civil society organizations, were unanimously against future use of Internet voting:
  - felt it was not necessary (did not share local officials' concern regarding traditional counting methods);
  - felt that the average person could not understand or monitor the system; and
  - felt that confidence in electoral system could decrease if results are close

No official complaints related to Internet voting were filed during the pilot.

When no stakeholder stepped forward to conduct an independent audit into the Internet voting, the Ministry contracted with a third party to do so. The perceived conflict of interest regarding the audit being requested and paid for by the election administration was seen to be less of a risk than no audit at all.

The audit demonstrated that all votes received remained unaltered during the counting and reporting process, but it did identify a small number of technical issues. For example, nine ballots showed too many votes cast and so were not counted. This scenario should not have been technically possible. The vendor determined either that there had been a purposeful attempt by nine voters to forge an improper ballot, or an error had occurred whereby the same party or candidate was listed twice on the ballot. Due to the nature of the error it was impossible to distinguish after the fact which of the two scenarios occurred.

Parliamentary approval to conduct a second pilot of Internet voting during its September 2013 Parliamentary Elections was granted in April 2013. The same ten municipalities in the 2011 pilot were included in the 2013 pilot, as well as two additional municipalities, for a total of approximately 250,000 eligible voters. In leaving the decision to conduct the second pilot so late in the election cycle, the amount of time available to develop and test the updated system and document all of the new procedures was limited.

The 2013 pilot largely followed the same procedures used in the 2011 pilot. Improvements over the 2011 pilot included new voting software, a new encryption model, and the establishment of a results verification process. The Ministry also took additional steps to emphasize the transparency of the process. These steps included: publishing the source code and system documentation on the Ministry website; broadcasting a seminar for election observers on its website; and broadcasting the decryption and counting of Internet votes on election day.

A new Internet Election Committee was formed to supervise key aspects of the preparation and verification activities and had the authority to suspend or even cancel Internet voting in the case of irregularities in order to "enhance the transparency and accountability of the Internet voting".[86] However, observers found that the Committee members "were not conversant with the system and relied entirely on the Ministry's guidance and advice" and its ability to act as an independent oversight body was questionable.[87]

On the last day of Internet voting, the Ministry announced that a weaker level of encryption had been used for Internet ballots cast to date than was planned for. This meant that it was possible for system administrators with access to the electronic ballot box to decrypt the ballots without the need for the secret decryption key. To address this issue, the Ministry "tightened access restrictions to the servers holding the electronic ballot box by requiring a written authorization each time servers were accessed" and updated the voting client software with the proper level of encryption for votes cast after this error was identified.[88]

Like the 2011 pilot, the 2013 pilot also enabled voters to check that their ballot was cast as intended and recorded as cast by comparing a verification code sent to them by SMS after voting against the unique verification codes mailed to the voter prior to voting. In 2013, voters could also check that their vote would be included in the tally by comparing an encrypted version of the vote displayed to the voter after the ballot was cast with a record of all encrypted votes published to an Internet bulletin board. As voters were permitted to vote multiple times with only the last vote being counted, each vote would be recorded on the bulletin board. While the Ministry provided an opportunity for political parties and the media to verify the tally (universal verification), none chose to do so and the only body to do so was contracted by the Ministry.

In the 2013 pilot, 36% of registered voters in the pilot municipalities used Internet voting, up from 17% in the 2011 pilot.[89]

86 Reference #333
87 Reference #333
88 Reference #333
89 Reference #273

2011 Norwegian Pilot

	Bodo	Bremanger	Hammerfest	Mandal	Radoy	Re	Sandnes	Tynset	Vefsn	Alesund	TOTAL
Population											
Eligible voters	36,635	2,955	7,752	11,764	3,687	6,870	48,689	4,163	10,456	35,535	167,506
Overall turnout (#)	24,131	1,947	4,373	7,413	2,275	4,395	30,537	2,870	6,193	20,716	105,050
Overall turnout (%)	65.9%	65.9%	56.4%	63.0%	67.1%	64.0%	62.7%	68.9%	59.2%	60.0%	
Internet voting registration (#)	N/A										
Internet voting turnout (#)	7,014	408	1,132	1,466	771	987	8,246	907	1,334	5,473	27,738
Internet voting turnout as % of eligible voters	19.2%	13.8%	14.6%	12.5%	20.9%	14.4%	16.9%	21.8%	12.8%	15.9%	16.6% (avg)
Internet voting as % of votes cast	29.1%	21.0%	25.9%	19.8%	33.9%	22.5%	27.0%	31.6%	21.5%	26.4%	26.4%
When offered	31 days during advance voting; 24 hr/d										
Vendor	ErgoGroup & Scytl										

Geneva, Switzerland[90]

Origins

Swiss citizens are accustomed to voting remotely and often. Since vote by mail was first offered in the mid-1990s its use has increased to the point where 95% of all ballots cast in Geneva are now cast remotely. Swiss voters also have four to six opportunities a year to cast a ballot for various elections and referenda at the local, canton and federal levels, with the administration of all elections and referenda administered by the cantons. Switzerland also has a large number of overseas voters, for whom even vote by mail is not sufficiently convenient.

The cantons of Geneva, Neuchâtel and Zurich independently developed Internet voting systems with the financial assistance of the federal government.[91] Geneva began investigating Internet voting in 2001 and after a series of pilot referenda and non-governmental elections, a constitutional amendment was approved in a 2009 referendum[92] (using traditional voting methods) to allow for Internet voting in governmental elections.[93]

Internet voting is highly supported by the State Chancellor of Geneva. This is seen as contributing to the success of Internet voting's implementation and to the public's support of it.

The Internet voting system was intended to be "as easy, practical and safe as possible," reliable, include a voter verification capability and protect the secrecy of the vote.[94] The federal and state governments each set requirements for the Internet voting system and two ISO standards were also used as targets for information security management (ISO 27001 and ISO 27002). One of the federal requirements is that when Internet voting is available in federal elections it may not be used by more than 30% of eligible voters and must be approved by the federal government in advance.[95] In the canton of Geneva this means that Internet voting may only be available in selected municipalities or may only be available to overseas Swiss voters.[96]

When it authorized Internet voting, Geneva also established the Central Election Commission (CEC).

90 For more information about Geneva's experience with Internet voting, see references #38, 45, 48, 109, 142, 176, 191, 192, 195, 197, 261
91 While Geneva's system was developed and owned by the canton, Zurich contracted with Unisys and Neuchâtel contracted with Scytl for the development and operation of their systems.
92 February 8, 2009. 70.2% voted in favour of permitting Internet voting for Geneva.
93 Geneva conducted 11 votes using Internet voting during the pilot phase (2003-2008). After the 2009 referendum approving Internet voting for governmental elections, the pilot phase officially ended. Since this time, Geneva has conducted 20 more votes using Internet voting, though all but one have been for federal and cantonal referenda.
94 Reference #109
95 When Internet voting was introduced in Switzerland the cap was 10%, but over time it increased to 20% and in 2012 was increased again to 30%.
96 Internet voting has been used in 20 votes in Geneva, since 2009.

The CEC has oversight and inspection responsibilities related to Internet voting in Geneva. These responsibilities include the locking of the electronic ballot box and the generation of its encryption keys. The CEC also regulates the testing and auditing of Internet voting systems and controls access to the system and its source code by outside groups. It is required by law to conduct a full audit of its system every three years and to publish its results.

Geneva also hosts Internet voting for other cantons, including Bern, Lucerne and Basel-Stadt using its own Internet voting system. Under this model, the other jurisdiction provides its voters list to Geneva, which conducts the Internet voting and transmits the results back to the other jurisdiction for reporting.[97]

Geneva was not one of the four cantons chosen by the federal government to use Internet voting for overseas voters in the October 23, 2011, federal election. However, Geneva's Internet voting system was used in that election by voters in Basel-Stadt.[98]

Process

Under the Geneva system, all voters are mailed a card with authentication credentials. Voters use a PIN that is hidden under a "scratch-off" portion of the card (like a lottery ticket) along with their date of birth and city of origin (shared secrets) to log into the system. Geneva's system utilizes encryption and the double envelope method to prevent a link between the voter and the ballot, but does not use other security methods such as digital signatures.

To prevent voters from being able to sell their vote, voter verification methods only prove to voters that their vote was counted and does not include any indication on how it was marked.

Decryption of the voting results requires that representatives from the state chancellery, the CEC, the state election administration, the police and a notary are present. While the electronic ballot box is sealed, if the number of votes in the ballot box and the number of voters recorded as having voted do not match, an "integrity meter" will sound an alarm.

97 Zurich also offers its system to other cantons, but instead of administering the other canton's election itself, it provides a copy of its system to Unisys, the original developer, which administers the Internet voting for the canton.

98 The approved cantons were: Basel-Stadt, St. Gallen, Grisons, and Aargau.

Results

Geneva is one of the jurisdictions that believes Internet voting has had a positive effect on voter turnout. This is partially due to the high level of younger voters (18-39) who responded in a survey that they typically did not vote. Voters under 50 were also more likely to use Internet voting than any other channel, and 90% of voters who used Internet voting claimed they would likely use it again. Geneva has also reported a 20% increase in the number of registered overseas voters since Internet voting was introduced.

In its third report on Internet voting since 2006, the federal government stated that Internet voting would be expanded to the majority of overseas voters by 2015 and possibly to all Swiss voters at some point after its next report in 2017/18.

	May 15, 2011 (canton referenda)	November 4, 2012 (local government election)
Population	241,780	240, 484
Eligible voters	241,780	240, 484
Overall turnout (#)	~95,540	~67,336
Overall turnout (%)	39.5%	28%
Internet voting registration (#)	N/A	N/A
Internet voting turnout (#)	21,057	~10,100
Internet voting as % of eligible voters	8.7%	4.2%
Internet voting as % of votes cast	22.0%	15%
When offered	28 days during advance voting; 24h/d	28 days during advance voting; 24h/d
Vendor	State of Geneva	State of Geneva

New South Wales (NSW), Australia[99]

Origins

In March 2010, the New South Wales Parliament directed the New South Wales Electoral Commission (NSWEC) to investigate the feasibility of Internet voting for visually-impaired voters in the March 2011 State General Election. In July 2010, the NSWEC concluded that Internet voting would be technically feasible but difficult to implement for March 2011 State General Election. Legislation to provide Internet voting for this group of voters was introduced in November 2010, but was amended weeks later to expand the classes of eligible to include voters who would be unable to vote for reason of location (being more than 20km from a voting place or being out of the state on general voting day).

99 For more information about New South Wales' consideration of Internet voting, see references #99, 223, 306, 321, 332

The state's goals were to improve accessibility (allow independent voting by visually-impaired voters and improve convenience for remote voters), to reduce the likelihood of errors in marking the ballot (New South Wales uses a complex, preferential ballot and is legally obligated to provide Braille ballots for visually-impaired voters), and to reduce counting errors, cost and other issues associated with absentee voting.

Following a public tender process, NSWEC contracted with EeveryoneCounts to provide the iVote Internet voting system used in the 2011 State General Election.

Process

In order to register to vote using the iVote system, voters were required to call NSWEC, verify their identity and confirm their eligibility for Internet voting. While on the phone the voter creates a PIN, which the system uses to create a voting credential (a hash based on PIN and other items) on the voting server. A unique, random voter number was also created by the system and sent to the voter via mail, SMS, SMS to Voice, or phone (phone option available for visually-impaired voters only). A letter was mailed to the voter's registration address on record with NSWEC to confirm that they did in fact register for Internet voting.

The voter number and PIN are required to cast a ballot. After the voter casts a ballot, the system creates a unique random receipt number and displays it for the voter on the device they used to vote. This number and their voting credentials can be used after the close of voting to confirm that their vote was received. However, because the voter cannot verify their vote during the voting period, there was no opportunity to vote again if a problem was identified. Further, as the voting receipt is issued during the voting transaction through the same channel as was used for voting, if the security of the voting process was compromised, the verification process would be similarly compromised.

NSWEC chose not to use E2E verification in the Internet voting system it implemented in 2011 "due to the emerging nature of the technology at that time". In its iVote strategy document prepared for the 2015 State General Election, NSWEC wrote that "full E2E where anyone can verify that all recorded votes are properly tallied...increases the complexity [and] reduces the ability of [voters], stakeholders and [NSWEC] to understand the system and be confident in its results".[100] In the proposed new iVote system to be used in NSW in 2015, the NSWEC will use a partial E2E approach. This approach will allow a voter to verify that their vote was received and NSWEC to verify "in aggregate" that all votes were counted as cast. NSWEC felt that the verification of results (both individual and overall) should be simple enough for voters to understand and voters should only have to rely on the expertise of NSWEC and appointed experts to trust that the proposed new iVote system works.[101]

100 Reference #321
101 Reference #332

Results

The legislation required an independent audit be conducted before and after each general election to ensure that the system was secure and the results reflected the votes cast. However, results for the first audit were to be provided to the NSWEC only "at least 7 days" before voting began and several weeks after iVote registration had begun. While this audit is separate from security reviews of source code, cryptography, infrastructure and processes and penetration testing that took place a month prior to the election, conducting an audit only seven days prior to the beginning of voting is not very much time to make changes if risks are identified. In fact, some risks that were identified by the security reviews and the pre-election audit remained outstanding during the election.

According to the auditor, late legislation meant "incomplete documentation, restricted test case formulation and compressed testing activities".[102] The auditor recommended an expanded level of testing for future events.

Five incidents occurred during the voting period, including one incident affecting 43 ballots that was not discovered until after the close of voting.

The NSWEC deemed the 2011 state election experience with Internet voting a success and the legislature has approved the use of Internet voting for the next state election in 2015. Procurement of an Internet voting system for that election began in July 2013. NSWEC intends to publish procedures, system architecture, voting protocol, security and source code reviews and post-election audits for the 2015 election to its website. It also has plans for increased stakeholder consultation, including a technical consultative group made up of outside experts that apply to participate. These technical groups will have access to the system's source code, but its use and members' ability to comment publicly will be limited so that "expert reviewers do not diminish the trust placed in [NSWEC] and the electoral process through sensationalised public comment". Beyond the technical consultative groups, public access to source code will be limited to those individuals and groups that can prove their expertise and are willing to sign a non-disclosure agreement.

The version of the system to be used in 2015 will improve the verification process. Voters will be able to access the content of their vote online or via an automated telephone system that reads back their vote. If their verified vote does not match the voter's intent, the voter can re-register and vote again. Re-registering automatically deletes their previous vote. The receipt numbers are to be published after counting to allow voters to verify their vote is included in the count, and all votes will be anonymized and published online to allow anyone to verify the tally of results.

102 Reference #99

	2011
Population	~7,210,000
Eligible voters	4,635,810
Overall turnout (#)	4,290,595
Overall turnout (%)	92.6%*
Internet voting registration (#)	51,103
Internet voting turnout (#)	46,864**
Internet voting as % of eligible voters	1.0%
Internet voting as % of votes cast	1.1%
When offered	12 days during advance voting; 24h/d
Vendor	EveryoneCounts

* Voting is compulsory in New South Wales

** 44,605 by Internet and 2,259 by phone

Other jurisdictions - Investigated and rejected

USA (military and overseas voters)[103]

Circumstances for its consideration and why it was ultimately rejected

Election administration in the United States for all three levels of government (local, state and federal) is conducted at the county level with guidance from the Secretary of State. As such, voting procedures can vary widely from county to county and from state to state. While Internet voting has not been implemented in a large-scale, binding governmental election to date, it has been the subject of significant amounts of research and a number of smaller pilot projects.

Internet voting in the United States has largely been focused on providing increased accessibility of the electoral process for U.S. military and overseas voters – two groups that have traditionally had difficulty exercising their right to vote due to the amount of time required to send and receive ballots outside of the country and unreliable postal services. The Federal Voting Assistance Program (FVAP), on behalf of the Secretary of Defense, administers the *Uniformed and Overseas Citizens Absentee Voting Act* (UOCAVA), the legislation that governs the voting process for these two groups.

FVAP began investigating Internet voting in the late 1990s ahead of a pilot project in conjunction with the 2000 General Election. The 2000 pilot was conducted for eligible UOCAVA voters in South Carolina and four counties in Florida, Texas and Utah, up to a maximum of 50 voters per jurisdiction. Due to the various technical and administrative requirements for participation, including a requirement for the voter to be mailed a CD-ROM with the appropriate software and a request for voters to also mail a paper ballot as a backup, only 84 voters cast an Internet ballot.

103 For more information about the USA's consideration of Internet voting, see references #38, 48, 57, 94, 118, 120, 142, 264, 265, 266, 267, 268, 269, 270, 271, 272

Building upon the 2000 experience, the Secure Electronic Registration and Voting Experiment (SERVE) was intended by FVAP to be a larger scale Internet voting pilot for the 2004 General Election for UOCAVA voters in fifty-five counties from seven states. However, after spending $22 million on the pilot, the Department of Defense (DoD) cancelled the pilot ahead of the election due to a lack of public confidence in the system after security concerns were identified by computer scientists contracted to evaluate the system. The researchers concluded that there was "no good way to build [a secure, all-electronic remote voting system] without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough".[104]

The 2009 *Military and Overseas Voter Empowerment Act* (MOVE) required states to improve the voter registration and absentee voting process for UOCAVA voters, and authorized the DoD to conduct pilot projects to test technology that would assist UOCAVA voters. The MOVE Act also required the DoD to report to Congress on such tests with the assistance of the Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST).

Based in part on this legislation, West Virginia established its own Internet voting pilot for UOCAVA voters during the 2010 Primary and General Elections. The state qualified two Internet voting vendors which the eight pilot counties could choose between to provide the service for their voters.[105] After submitting an application, eligible voters were emailed a username and URL by either the election administrator or the vendor to access the system. Voters received a verification code that would enable them to confirm that their vote was included in the tally of votes cast, but did not identify the voter's choices. Of the 165 voters that applied, 125 voters voted online in the November General Election. While the counties did not report any technical issues with the voting systems used in West Virginia, based on concerns with Internet voting raised at a 2010 UOCAVA conference and the experience of Washington D.C.'s Internet voting test in September 2010, the Secretary of State recommended that further research into the issues related to Internet voting be conducted. West Virginia did not use Internet voting in the 2012 General Election.

Although its 2011 report on Internet voting security stated that "pilot projects should be encouraged,"[106] the most recent statement from NIST issued in May 2012 states that "additional research and development is needed to overcome [the challenges of auditability, malware and a lack of a public authentication infrastructure] before secure Internet voting will be feasible".[107]

104 Reference #264
105 Scytl was contracted by three counties and Everyone Counts was contracted by five counties
106 Reference #94
107 Reference #272

United Kingdom[108]

Circumstances for its consideration and why it was ultimately rejected

The UK has conducted three rounds of pilot projects involving Internet voting for local government elections – 2002, 2003, 2007. While the UK Electoral Commission does not administer the local government elections or the pilots, it is required by law to evaluate and report on them.

2002

In 2001, the UK Electoral Commission wanted to explore Internet voting, among other voting and counting innovations, in order to encourage voter participation and improve the efficiency and accuracy of how elections are administered. Five local governments agreed to participate in a pilot that offered multiple electronic voting opportunities that included Internet voting. Internet voting accounted for between 10 and 27 percent of all votes cast in these municipalities; however there was no substantive evidence that Internet voting led to improved turnout overall. Post-election research showed that Internet voting was more convenient to voters with disabilities. While voters and candidates expressed concern that Internet voting would be more susceptible to fraud, the Commission was not aware of any actual cases of fraud. The Commission's evaluation of this pilot was largely positive and its critiques were largely related to the management of the pilot scheme.

2003

In 2003, fourteen local governments piloted Internet voting as an additional channel for voting. Credentials were mailed by the local governments and were sent in either one mailing, or two (for added security), depending on the jurisdiction. Use of Internet voting ranged from 10 to 37 percent of all votes cast in these municipalities, with an average of 12.6%. The Electoral Commission's evaluation of this pilot was more technical and contained a number of recommendations related to security and reducing risk.

2007

In 2007, five local governments piloted Internet voting as an additional channel for voting. Voters were required to pre-register for Internet voting and the Electoral Commission believed that this likely contributed to a significantly lower use of Internet voting compared to the 2003 pilots. This time the Commission reported that while the pilots were broadly successful, there were concerns of accessibility, public understanding of the process and technical problems in one jurisdiction. The Commission also raised concerns about poor planning, rushed implementation and a lack of quality assurance and testing by the local governments that resulted in significant risk.

108 For more information about the UK's consideration of Internet voting, see references #38, 48, 60, 62

The Commission recommended that no further Internet voting pilots be conducted until a comprehensive strategy for Internet voting is developed and UK standards for evaluating Internet voting systems are set.

Netherlands[109]

Circumstances for its consideration and why it was ultimately rejected

Dutch citizens living outside of the Netherlands are entitled to vote by mail in Dutch elections provided they register their interest ahead of the election. Turnout among these voters abroad is typically low (~5% of 600,000 eligible voters). The Netherlands experimented with Internet voting in 2004 and 2006 as an alternative to vote by mail for these voters in order to improve accessibility and convenience.

2004

In 2004, the Kiezen op Afstand (KOA) (Remote Voting) system developed by LogicaCMG for the Dutch government[110] was trialed and used by 4,871 voters for elections to the European Parliament. Registered voters received by mail a unique login code and a list of candidates with a code for each candidate on the list. There were 1,000 variations of the list of candidates and codes. The voter would enter their login code and the candidate code when voting online to indicate their preference instead of seeing a visual representation of the ballot. Together, this meant that if the security of the voting system was compromised, an attacker would still not know how the voter intended to vote.

2006

In 2006, the government decided to test a different system for voters abroad. This system was created by the Rijnland District Water Control Board and known as RIES (Rijnland Internet Election System). RIES had been successfully trialed in a large scale pilot project and included vote verification elements. RIES also used cryptography and a traditional visual representation of the ballot instead of candidate codes.

109 For more information about the Netherlands' consideration of Internet voting, see references #102, 156, 304, 305, 325

110 The majority of the KOA source code was subsequently released by the Dutch government for use as an open source Internet voting platform.

Interested voters abroad were required to register to vote using Internet voting at least four weeks before the election. Voters were then mailed an instruction booklet and sealed authorization code with which to authenticate themselves. Dutch law permitted voters to request a replacement authorization code if the original was lost, but this process required the election administration to maintain a link between the codes issued and individual voters so that the original code could be deactivated, thereby compromising the secrecy of the ballot.

Further, it required more codes be created than eligible voters, meaning the election administration had to be trusted to protect extra codes and to only issue the extra codes in authorized circumstances.

Voters were given a receipt that they could use after voting closed to verify their vote was counted, though the receipt did not show how the voter voted. After voting ended, a codebook was published linking all potential receipt codes to candidate names, along with a list of all the receipts issued to voters. This process enabled anyone to tally the votes independently. However if a third party gained access to both the receipt and the voter's authorization code used to vote, they would be able to determine who the voter voted for. Similarly, if the codebook was not kept secure throughout the election, it also could have been used with receipts to compromise the secrecy of the ballot.

Although a much larger number of voters abroad (19,815) voted online in 2006, developers and critics of Internet voting agreed that RIES would not be a suitable system if Internet voting were ever expanded to all Dutch voters.

Public support of Internet voting dropped significantly after the 2006 election due to significant issues found with the reliability and security of the Direct Recording Electronic (DRE) voting machines used in Dutch voting places for in-person voting. These problems with DRE technology resulted in a very low level of trust in all voting technology. Also at the time of the 2006 election, it became evident that the Dutch government had become too dependent on the private sector companies that it relied on for the provision and support of the DRE voting machines. This dependency meant that the election administration could not exercise its responsibility over all aspects of the electoral process. In 2008 the Dutch government mandated that only paper balloting be used for the foreseeable future.

APPENDIX G - GLOSSARY

The definitions used in this glossary are intended to be plain-language explanations of the terms used throughout this report. The panel recognizes that the definitions provided may not be as comprehensive as those used by experts in the relevent fields.

Absentee voting	Voting other than in-person at a voter's assigned voting place; includes vote by mail.
Accessibility	The ease with which voters can exercise their right to vote.
Adjudication	A process for determining whether a ballot has been marked in an acceptable manner and for whom the ballot has been marked.
Advance voting	Day or days for voting prior to general voting day; the period during which vote by mail is offered is not typically referred to as advance voting.
Algorithm	A sequence of actions to perform to accomplish some task or solve a technical problem; the term is often used in the context of computer programming.
Audit	An independent pre- and/or post-election evaluation of an organization, system or process which includes quantitative and qualitative analysis.
Auditability	The degree to which the integrity of the overall system for voting and, ultimately, the results of the election, can be confirmed.
Authentication	The process of identifying an individual as an eligible voter (may include confirming whether or not an individual has previously voted in the same election).
BC Services Card	A form of government-issued photo identification that serves as a combination drivers license and government services access card. The card has an embedded chip and other security features that could potentially provide a secure voter authentication mechanism for remote Internet voting in the future. The BC Services Card was launched in February 2013.
Ballot anonymity	The inability to link a ballot with the individual who cast it.
Candidate representatives	Individuals appointed by candidates to observe voting and counting on behalf of candidates at a voting place. Candidate representatives make sure that election rules are followed and that the counting is done fairly. Also known as scrutineers.
Chief Election Officer	The senior election administrator responsible for the administration of the local government electoral process in a jurisdiction in B.C.
Chief Electoral Officer	The senior election administrator responsible for the administration of the provincial electoral process in B.C.
Certification envelope	An envelope used in administering absentee voting. Identifiable information about the voter is written on the outside of the envelope. A secrecy envelope containing a ballot is sealed inside the certification envelope. The certification envelope is used to ensure that the voter votes, and the ballot is counted, in the correct jurisdiction. Used as part of the double-envelope process.
Cleansing	A electronic process that removes duplicate ballots from a single voter prior to counting; used by some Internet voting systems as one of three phases of counting.
Credentials	Physical or electronic document(s) that proves a voter's identity; used in B.C. local and provincial government elections and most other jurisdictions to authenticate a voter prior to issuing a ballot.
Cryptography	The practice and study of encryption and decryption, whereby, for example, a message is encoded so that it can only be decrypted by those with one or more keys known only to the intended recipient(s).

Denial of Service (DoS)	An attempt to overwhelm a server's capacity with traffic so that it is unable to perform its usual duties and respond to its intended users.
Device	Any means by which a voter may cast a ballot for Internet voting (e.g., computer, tablet, smartphone)
Digital divide	Refers to the gap between those with regular, effective access to digital technologies and those without.
Digital signature	Encryption of a message using the sender's secret key which authenticates the identity of the sender.
Distributed Denial of Service (DDoS)	A Denial of Service (DoS) attack conducted by a large number of computers, typically controlled remotely through malware.
District Electoral Officer	The senior election administrator, appointed by the Chief Electoral Officer, responsible for the administration of the election in a provincial electoral district.
Double-envelope process	A process for authenticating a voter remotely while maintaining ballot anonymity.
Election administration	The organization or body responsible for the administration of elections in a jurisdiction; e.g., Elections BC, individual local governments.
Election administrator	An official within an election administration, such as the Chief Election Officer, Chief Electoral Officer, or District Electoral Officer.
Elections BC	The usual name for the Office of the Chief Electoral Officer. Elections BC administers the electoral process in B.C. This includes provincial general elections, by-elections and provincial referenda. Elections BC does not administer local government elections or referenda in B.C.
Electronic voting	A broad term encompassing Internet voting and any other electronic means of marking a ballot, casting a ballot, or vote counting. Includes optical scan counting machines and direct-recording electronic voting machines (touch screen voting machines).
Eligible voter	In B.C., an individual who meets the qualifications for voting; in some jurisdictions, an individual who is registered to vote, or registered for Internet voting.
Encryption	Any procedure used in cryptography to convert plaintext into an encrypted message in order to prevent any but the intended recipient from reading that data.
(Encryption / decryption) Key	In cryptography, a value which must be fed into the algorithm used to encode / decode a message.
End-to-end verifiability (E2E)	Cryptographic protocols that enable anyone to confirm that all ballots cast were correctly tallied, and to prove to an individual voter that their vote is included in the final tally; also known as universal verifiability.
Final count	The final consideration of ballots cast in an election. The results of the final count are the official results, barring a judicial recount. For provincial government elections, the final count includes a confirmation of initial count results as well as the counting of absentee ballots.
General Voting Day	The final day for voting; ballot counting and announcement of preliminary results typically take place at the end of this day; also known as voting day or election day.

Initial count	The preliminary counting of some or all ballots cast in a jurisdiction with results subject to final count; typically conducted at the end of general voting day; does not typically include the count of absentee ballots.
In-person voting	The traditional channel in B.C. whereby voters attend a voting place, get authenticated face-to-face by an election official, and cast a ballot on paper.
Internet voting	A voting method where votes are transferred via the Internet to a central counting server; also known as voting online.
Internet voting solution	Products or services provided to conduct Internet voting.
Internet voting system	Technology and processes used to conduct Internet voting.
Jurisdiction	A geographic location for which elections are conducted; e.g., Nanaimo, British Columbia, or Estonia.
Machine code	Code used by a computer to cause an operation. Machine code is converted from source code using an automatic translation program called a compiler.
Mail ballot voting	see *Vote by mail*.
Malware	Malicious software; software designed to interfere with a computer's normal functioning (e.g., viruses, trojan horses, spyware) (Merriam-Webster).
Mixing	An electronic process implemented prior to counting involving encryption and decryption which removes any links between a marked ballot and the identity of the voter who cast it; used by some Internet voting systems as one of three phases of counting.
Observe	The act of witnessing and assessing, but not intervening in, the proceedings of an election.
On-site Internet voting	A form of Internet voting that is conducted at controlled settings, such as voting places or kiosks established in high-traffic areas. Election officials may be available on-site to authenticate voters and ensure secrecy of the ballot.
Over-vote	Marking the ballot for more than the maximum allowable number of candidates; this results in the ballot being rejected for that race and no vote being recorded.
Paper balloting	Voting using tangible ballots made of paper; as opposed to electronic voting or Internet voting.
Personal Identification Number (PIN)	A number (usually secret) assigned to an individual and used to confirm identity.
Phishing	The practice of attempting to acquire authentication credentials or other personal information by posing as a trustworthy or legitimate entity.
Process validation	The requirement that the procedures, technology and documentation to be used for Internet voting be available to the expert panel for testing and review for an appropriate length of time before, during and after the system is to be used, and for policies and procedures to be in place to respond to issues that arise.
Protocol	A set of formal rules describing how to transmit data, especially across a network.
Receipt	A randomly generated code that can be used by the voter after casting a ballot to ensure the vote is received and processed correctly by the voting system.

Rejected ballot	A ballot that is rejected during the counting because it is unmarked, is marked in a way that does not clearly indicate the intention of the voter, or is marked in such a way that the voter could be identified.
Remote Internet voting	A form of Internet voting that allows voters to transmit their voted ballot from any Internet-connected device and location to which they have access, e.g., home/office computer, smartphone, tablet. For the purpose of this report, see *Internet voting.*
Scrutineer	see *Candidate representative.*
Secrecy envelope	In absentee voting, the envelope in which the ballot is placed prior to being sealed inside a certification envelope. The secrecy envelope ensures that the ballot cannot be linked to the voter whose information is on the certification envelope. Used as part of the double-envelope process.
Shared secret	A fact or idea that both the voter and the election administrator know, but that few or no other individuals will know.
Source code	The form in which a computer program is written by the programmer. Source code is written in a programming language before being converted into machine code for a computer to read and use.
Stakeholders	Individuals or groups with an interest or concern in the conduct of elections; e.g., election administration, voters, political parties, candidates, MLAs, council members, technology vendors.
Supremacy of paper	The principle in some jurisdictions that have implemented Internet voting, that a paper ballot cast in-person will supersede any ballot cast by the same individual by Internet voting.
Tallying	Counting the number of ballots for each candidate; takes place after they have been adjudicated.
Traditional voting	Voting channels currently used for B.C. local or provincial government elections; e.g., in-person, absentee, vote by mail.
Transparency	The ability of individuals, groups, or the general public to scrutinize the activities of election officials, voters, and other participants in the electoral process. Transparency is achieved when observers can see that the requirements of applicable laws are being followed and the process is seen to be administered consistently and fairly.
Under-vote	Marking the ballot for no candidate, or fewer than the maximum number allowed in the race; where only one vote was permitted, this results in the ballot being rejected; where multiple choices are permitted, the valid markings are still recorded; often this occurs on purpose to indicate a protest vote, but can also occur unintentionally.
Vendor	A company that provides Internet voting systems or services.
Vote by mail	A remote voting channel whereby voters receive their ballot and associated voting material by mail, mark the ballot independently, and return it to the election administration by mail (some jurisdictions permit the voter or a representative to pick up and/or return the ballot in person; also known as mail ballot voting in B.C. local government elections.
Voter verification/ Voter verifiability	Processes or protocols that enable a voter to confirm that their ballot was received, and in some cases, counted as cast; End-to-end verifiability (E2E) is an extension of Voter verification/Voter verifiability.

Voting channel	A method for voting; either in person, by mail, or Internet; also known as voting opportunity.
Voting opportunity	see *Voting channel.*
Voting place	A building or other location where in-person voting takes place.
Voting process	The series of steps involved in casting votes for an election. The voting process may vary between jurisdictions and between voting channels in the same jurisdiction.
Write-in ballot	A ballot used in voting for a candidate in an election where the voter writes the name of the candidate or the registered political party they wish to vote for in a large blank space on the ballot. Used in certain types of absentee voting in B.C.

Mailing address: PO Box 9275 Stn Prov Govt Victoria, BC V8W 9J6

Phone: 250-387-5305

Toll-free: 1-800-661-8683

Email: info@internetvotingpanel.ca

Website: internetvotingpanel.ca

Website: internetvotingpanel.ca
Email: info@internetvotingpanel.ca
Enquiries: 1-800-661-8683

8017 (14/02)

Internet Voting in the USA: History and Prospects; or,
How NIST has Misled Congress and the American People about Internet Voting Insecurity

A Discourse Analysis.

Abstract
Internet voting in the USA has a tragic history. It began in the year 2000. It worked so well that Congress approved a major project for the Department of Defense to provide website based Internet voting for overseas military. But the project was abruptly aborted, and the reputation of Internet voting suffered a blow from which it is yet to recover. In chronicling these events our discourse analysis shows how a coup d'état of the election administration function was executed through the control of Internet voting's meaning.

William J. Kelleher, Ph.D.
The Internet Voting Research and Education Fund
Email: Internetvoting@gmail.com

Paper prepared for the annual meeting of the Western Political Science Association, March 28 – 30, 2013. Los Angeles, California.
Comments are welcome.

Part I: A SHORT HISTORY OF INTERNET VOTING IN THE USA.

Introduction

The defining event for the history of Internet voting in the United States occurred early in 2004. Before then small trials of Internet voting were conducted by the Department of Defense for its overseas military, and by a few political parties, but these uses pale in significance to what happened in 2004. In that year the myth of Internet voting insecurity swept the nation in a matter of days, and has remained the prevailing social meaning of the technology since then. Using a discourse analysis, this paper will describe the emergence of that myth, how it has been sustained to this day, and why it is a myth with no basis in science or fact. But first some historical background is in order.

Remote Electronic Voting Before 2004

The idea of using the technology of electricity to vote has been around for a long while. Thomas A. Edison's first patented invention, in 1869, was an electronic vote recorder for use by legislative bodies. Although demonstrated to Congressional leaders, it was never used.[1] Early in the 20th Century the inventor R. Buckminster Fuller suggested that voting by telephone would be convenient for rural voters.[2]

During the 2006 election Connecticut, Maine, New Hampshire, Oklahoma, Oregon, and Vermont used vote by phone systems.[3] Telephone voting continues to be used in several Canadian provinces.[4] In 1990, during Operation Desert Storm, the Department of Defense (DoD) worked with some states to allow voters to receive and submit their ballots by fax.[5]

Ross Perot's Reform Party might have been the first US political party to employ online voting, in 1996.[6] The Republican Party allowed remote voters in Alaska to vote online in its straw poll in 2000. But a mere 35 votes were cast this way.[7] Also in that year, the Democratic Party offered the option of Internet voting for its members in its Arizona primary. Nearly 40,000 voters, about 46% of the total, used the system.[8]

Concerned about the difficulty of voting from overseas that US voters, especially those in the armed forces, had long complained of, in 1986, Congress enacted the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). The Act granted authority to the executive branch of the federal government to provide a way for US citizens to register and to vote in federal elections from overseas. States were left to their own devices. By Executive Order, the President assigned the Secretary of Defense the administrative responsibilities for UOCAVA. In turn, the Secretary of Defense assigned these responsibilities for implementing the law to the Federal Voting Assistance Program (FVAP), an agency within the Department of Defense.[9] FVAP broadened its vote by fax method in 2003 to offer voting by email to the military in Iraq and Afghanistan.[10]

In the year 2000, FVAP worked with several volunteer states on a pioneering "test of concept." The project was called "Voting Over the Internet" (VOI). The plan was to allow members of the overseas military to vote online in the November election. "Internet voting," is a distinct method of voting. Unlike fax or email voting, Internet voting is

website based; that is, the voter can use his or her own equipment to connect with a designated remote server by logging on to a secure website. The challenge for FVAP was to set up a website on which the voter could log on (with user name and password) and retrieve an exact copy of his or her local jurisdiction ballot, then cast votes for every candidate and other issue, and click to return the voted ballot. There were 50 counties presenting ballots among the five states in the trial. FVAP's server was accessed by the overseas voters to vote, and then by the local election officials to download the encrypted digital information. This was the first time any US citizens used true Internet voting to cast an actual vote in a US election.[11]

Of course, no government agency, perhaps in the world, understands security issues as well as the United States Department of Defense. Despite all their security experts knew of online voting threats and how to defend against them, FVAP invited outside "White Hat" hackers to probe the VOI system for weaknesses. In addition, the state of Florida insisted on independently testing the system by its own standards; which it did, and then it gave VOI official "certification."[12]

Although the number of votes cast over the system was tiny, a mere 84, the *concept* of Internet voting for overseas military had proven itself viable. After the election, FVAP conducted a thorough assessment study of the trial. According to Polly Brunelli, FVAP's voting program director, satisfaction levels were very high among local election officials, FVAP managers, and most importantly the voters.[13]

The assessment study compared the use of Internet voting to the vote by mail (VBM) system that the military generally used to date. Several important findings were made. These include that: users had more confidence in the VOI than in the VBM process (4, 2); only voters whose registration was authenticated voted (4, 30); only one ballot per voter was taken by the VOI system (4, 4); VOI provided greater voter secrecy, privacy, and protection against the alteration of ballots than does the VBM process (4, 5-7); VOI facilitated reliable audits and recounts (4, 8); voter enfranchisement was enhanced because many of the frustrations of VBM, which had often discouraged participation, were eliminated. These included delays in the mail, and the rejection of registration forms and/or ballots because they had inaccurate, incomplete, or unclear data (4, 12-15).

Recognition grew in the DoD that Internet voting would be the future of voting for its overseas military, and perhaps all UOCAVA voters. Indeed, though they did not know it at the time, in 2003 FVAP would receive "the Excellence.Gov award for the VOI project from the Federal Chief Information Officers Council and The Industry Advisory Council." Additionally, the computer science experts in the "Caltech/MIT Voting Technology Project rated the VOI voter registration application a best practice for elections."[14] Following the VOI trial, DoD sought authority from Congress to try a much larger test.[15]

The Beginning of SERVE

Section 1604 of the National Defense Authorization Act for Fiscal Year 2002 directed the Secretary of Defense to carry out an expanded demonstration project which would enable

uniformed service members to cast ballots through an electronic voting system by the 2004 general election.[16] Using the knowledge gained from the VOI proof of concept, FVAP began work on the Secure Electronic Registration and Voting Experiment (SERVE).

Fifty-five counties from seven states – Arkansas, Florida, Hawaii, North Carolina, South Carolina, Utah and Washington – volunteered to participate.[17] According to the EAC report on SERVE, "services for voters included: online voter registration and updating of voter information online; ballot delivery and vote selection; and review of their registration and voting status."[18]

The FAVP team that worked on setting up the SERVE system employed several members of the prior VOI team. Also, private companies were brought in, such as Accenture and VeriSign. These companies had technicians with experience building Internet voting systems, like the one that went so well in Arizona. (Indeed, Arizona adapted that system for its overseas military, and now has the longest running overseas military Internet voting program in the country.)[19]

The SERVE voting process was security conscious from end to end. Each voter had to apply to vote on the system. Once the registration was cleared, he or she was assigned a "digital certificate," or identity code kept in the system to verify the voter's identity when he or she logged on.[20] As with VOI, these controls would help to prevent voter fraud by ensuring that only registered voters voted, and that each voter only voted once.

The central server was located in a well-secured building on Accenture's corporate grounds in Reston, Virginia. System administrators had to use security badges to enter the premises. Access to the server was limited to certificated personnel, each with their own security codes. Reading encrypted data required the codes of at least two authorized personnel. Event logs would keep an exact record of who did what on the server. Regular reviews of these logs assured that if any irregular activity had taken place, it would not go unnoticed. The odds of any "insider attack" succeeding were extremely small.

Separate modules were set up in the central server for each participating local election jurisdiction. Only their authorized personnel could access the central server from their local office. To further tighten security, FVAP provided each jurisdiction with a lap top computer dedicated only to the SERVE project. Using these computers, local jurisdictions could download the encrypted voting data from the central system. The FVAP-issued lap tops were programmed to decrypt only the data for the particular jurisdiction. At least two authorized personnel in a jurisdiction had to log on to access voter data.[21] Here again, security measures made insider shenanigans highly unlikely.

Encryption also makes it impossible for any unauthorized person to know who voted or how he or she voted. Having all the encrypted voter data for each jurisdiction on one lap top, requiring at least two people to use the decryption keys, creates a far more secure situation than having stacks and stacks of thousands of mailed-in absentee paper ballots scattered around an election official's office.

During development, SERVE's operations and security precautions were held to standards already in use by DoD military departments, including the National Security Agency. A diversity of independent subject matter experts combed the SERVE system for security vulnerabilities, and, as with VOI, the State of Florida independently certified SERVE for use by Florida voters.[22]

FVAP plans were to continue its security vigilance throughout the process. As the EAC Report explained, FVAP plans included

> conducting a formal phased risk assessment throughout the system development cycle; monitoring and review of system development process; developing [additional] system security requirements [as needed] to be responsive to risks; collaborative development of system requirements with states and counties; conducting thorough certification and accreditation testing for conformance to both functional and security requirements and doing third party penetration [or, White Hat hacker] testing prior to deployment.[23]

After deployment, intrusion detection systems would immediately alert administrators to any hack attempts so that counter measures could be promptly employed. Third party penetration testing would be conducted at random, without notice to SERVE administrators. System operators would engage in "continuous monitoring of system performance audit logs [which also had] pre-specified alarm conditions, and random third party review of system audit logs were planned as mechanisms to maintain awareness of the threat environment."[24]

FVAP Director, David Chu, used the following table to illustrate, in a report to Congress, the security risks the SERVE team anticipated and the strategies they developed to defend against those threats. Here is that table:[25]

THREAT	MITIGATION
Network Security	- Encryption - Intrusion Detection Systems - Redundant Firewalls - Penetration Tests
Privacy	- Digital Signatures - Secure Socket Layers - Encryption - Voter Identity/Ballot Data Separation - Voter Ballot Data Verification
Virus, Worm, Trojan horse	- Anti Virus Scanning - Digital Signatures - Voted Ballot Data Verification

Spoofing	- Secure Socket Layer - Digital Signatures - Voted Ballot Data Verification
Denial of Service	- Large Quantity of Bandwidth, Multiple Carriers - Multiple Internet Service Provider Entry Points - Utilization Monitoring
Voter Fraud	- Digital Signatures

Voters would register and vote in their state of residence. SERVE empowered them to vote in their state's primaries and the 2004 general election.

The voting process would begin with the voter using his or her PC, or any other computer, from any place in the world, at any time of day or night. First, the voter would log on to the secure SERVE website, enter the PIN that was issued at sign up, and request a ballot. Next, his or her name would be automatically checked against the local election authority's registration records. If cleared, an appropriate ballot would appear on the voter's computer screen. He or she would mark the ballot, and click the "vote" button. But that was not the final step. SERVE had a voter verification mechanism. That is, a window would appear showing the vote, and asking the voter to confirm it. Once the voter had verified his or her vote, the vote selections would be permanently stored in the database on the central server for later download by the local election officials.[26]

SERVE would automatically separate the voter's name from the ballot. Then the name would be stored on a list of those who voted, so that there could only be one vote per registered voter. The system would store the vote separately. By storing the separate records of votes and voters, SERVE would act as a back up for the local election officials. This back up data could also be used as an auditing resource. That is, throughout the process state officials could compare their lists of how many persons had voted, and their vote tallies, with those of SERVE. Any discrepancies would be cause for investigation.

Of course, every voting process consists in a division of labor. In the SERVE process, Congress had a role to play by granting authority and funding. DoD and FVAP had roles in the development and supervision of the system and coordinating with the states and local jurisdictions, along with the private contractors involved. Voters also had a role. Besides, hopefully, casting an informed vote, the voters who signed up with the SERVE project had other responsibilities. These included keeping their own PCs free of malware, and protecting their electronic credentials against theft or fraudulent use (such as buying or selling).[27]

Presumably, SERVE voters would have been an especially conscientious and responsible group. Because they were military personnel, they were likely security conscious; and

since they had to make the effort to sign up for the SERVE Internet voting project, they probably had more technological user savvy than the typical civilian voter at the time. Nevertheless, FVAP had planned a voter education publicity program to be sure the voters understood the need to protect their machines from malware.

The SERVE system was designed to handle far more votes than the tiny 84 cast in the VOI experiment. SERVE was prepared to process the registrations and votes of up to 100,000 participants. Beyond that, the SERVE technicians aimed to create a show piece of a system, which could be expanded to accommodate roughly six million UOCAVA citizens in the future, without compromising accuracy, vote secrecy, or the voter's identity. Although it was not their mission to demonstrate how a secure, accurate, and convenient Internet voting system could be carried on domestically, the SERVE team understood that this possibility was implied in their work. By the end of 2003 the SERVE technology was ready to conduct the first large scale multi-state online vote in an actual US election. SERVE was prepared for the 2004 primaries, and the November presidential election.

Indeed, to be sure that they had left no technological stone unturned, and that this was no secret operation done by government elites but a fully open process, which is as it should be in a democratic country, the FVAP established a SERVE Security Peer Review Group (SPRG). This group was comprised of 10 members from academia and industry. Some of these specialists were chosen because they were *known critics* of Internet voting. Nothing was kept secret from them, and everything was open for their inspection.[28]

Of course, this was a very risky move. The SPRG members with a bias against the project did not share the enthusiasm of the SERVE team for the vision of all UOCAVA citizens one day voting over the Internet. FVAP was aware that a sharp eyed critic could expose any major flaws in the system. Just one vocal dissenter could become a real party pooper.

Apocalypse Now

As it turned out, there was not just one vocal dissenter, but four! And they didn't simply add their dissenting opinion to the final report, as Supreme Court Justices do when they write a dissenting opinion. These critics went public with a passion to kill the project! That the *potentials* they envisioned and the consequences they imagined *might* happen caused them such alarm that they broke from the protocol for SPRG that the FVAP management had suggested.[29] Rather than the ten members of SPRG filing a consensus report with FVAP, these four critics wrote their own report, and promptly published it in the New York Times. The Times led its story with the conclusions made by the four critics:

> A new $22 million system to allow soldiers and other Americans overseas to vote via the Internet is *inherently insecure* and should be abandoned, according to members of a panel of computer security experts asked by the government to review the program. … The system, they wrote, 'has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks, any one of which could

> be *catastrophic*.' Any system for voting over the Internet with common personal computers, they noted, would suffer from the same risks.[30]

That story came out on January 21, 2004. On February 6, 2004, just over two weeks later, Deputy Defense Secretary Paul D. Wolfowitz issued a memorandum ordering David Chu, to halt work on the SERVE project.[31] The New York Times reported the story with the lead,

> Citing security concerns, the Department of Defense yesterday canceled plans to use an electronic voting system that would have allowed Americans overseas to cast votes over the Internet in this year's elections. Paraphrasing the memorandum, a Department of Defense spokeswoman told the Times: 'The department has decided not to use Serve [sic] in the November 2004 elections. We made this decision in view of the inability to ensure legitimacy of votes, thereby bringing into doubt the integrity of the election results.'[32]

Thus, the dissenting report had its desired effect. Four computer scientists, albeit with the help of the New York Times, caused the termination of an expensive Department of Defense project before it could be put into use. So powerful an essay deserves examination, so that history might understand the reasons and reasoning behind shelving SERVE. What made the SERVE system "inherently insecure"? What potentials did the critics see in the system that might result in "catastrophic" consequences? What did the dissenting essay say that led Deputy Secretary Wolfowitz to doubt the ability of SERVE "to ensure legitimacy of votes"?

The Argument from Potential

The four critics refer to their essay as "The SERVE Security Report" (SSR).[33] In it they stated their mission, their methods, their observations and opinions, and their conclusions. Here is how they understood their mission as SPRG members: "Our task was to identify *potential* vulnerabilities the [SERVE] system *might* have to various kinds of cyber-attack, to evaluate the degrees of risk they represent to the integrity of an election, and to make recommendations about how to mitigate or eliminate those risks."[34] The key words for understanding the methods these four critics followed are "potential" and "might." As we will see, they gave those words a very broad interpretation.

The analysis of Internet voting security is often divided into two sections. One is the website server, its physical environment, and the personnel connected with it (the server side). The other section is the environment of the voters who will vote on the system. This includes the voters, their equipment, the Internet, potential attackers, and law enforcement (client side). In the SSR, the primary concern was with the security threats in the voter's environment, the client side. The four critics stressed that those who constructed the SERVE *server* understood

> the security problems we describe here, and we have been impressed with the engineering sophistication and skill they have devoted to attempts to ameliorate or eliminate them. We do not believe that a differently constituted project could do any better job than the current team. The real barrier to success is … that, given the current Internet and PC security technology, and the goal of a secure, all-electronic

> remote voting system, the FVAP has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough.[35]

A wide range of threats infest the voter's environment, according to the authors of the SSR, "any one of which could be *catastrophic*."[36] They added, "We can *envision scenarios* in which the computers of SERVE voters have been compromised on a large scale, calling into question all votes cast over the Internet. Regrettably, such a scenario is all too possible."[37]

As a window upon the methodology followed by those writers, this is a telling statement. First, anyone who is concerned with the integrity of the democratic process will surely find it alarming, as those authors did, to contemplate a proposed online election system which would be based on "compromised" computers the use of which would call "into question all votes cast." Deputy Secretary Wolfowitz likely had such a disturbing vision in mind when he ordered a halt to the SERVE project.

However, the quoted statement might also cause alarm to anyone who is equally concerned that public policy criticisms have some foundation in scientific studies, or at least actual experience. Unhappily, that foundation will be found missing throughout the SSR. The expression "We can envision scenarios" is a description of the primary method employed by this "Report." The steps of their method include that they "envision scenarios," and many of them; then they treat each as if it were a statistically demonstrated "possibility," which they in turn rely upon to substantiate their case for setting aside all hopes for Internet voting. As we will see, not studies, but only their subjective imaginations render their scenarios "all too possible."

The authors admit that it is "impossible to estimate the probability of a successful cyber-attack (or multiple successful attacks) on any one election."[38] So, as a substitute for probability studies, the authors use the subjective approach of deeming an attack "quite *easy* to perpetrate." They add that those are "the attacks we are most concerned about."[39] We will discuss how they use "easiness" as a methodological concept below.

Another term in their methodological vocabulary is "could." That word occurs 128 times in the 34 pages of text. (We will also see such variants as "can" and "might.") Because the term refers to possibilities, as opposed to existing conditions, its referent is in the subjective minds of those who use the word, and not in the reality around them. Hence, the attacks the authors envision

> could occur on a large-scale, and could be launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law. These attacks could result in large-scale, selective voter disenfranchisement, and/or privacy violation, and/or vote buying and selling, and/or vote switching even to the extent of reversing the outcome of many elections at once, including the presidential election**.** With care in the design, some of the attacks could succeed and yet go completely undetected.[40]

Surely, if Wolfowitz had read this paragraph he would have lost a lot of sleep before deciding to stop SERVE.

As if that parade of horribles was not enough to overwhelm every American reader with fear for the safety of their country, should Internet voting be implemented, the authors zone in on party identifiers and political minorities: "It is *possible to imagine* widespread attacks that targeted all voters in a particular party for disenfranchisement, leaving the other party unaffected. Such an attack would have serious consequences."[41] To be sure!

However, in the present essay, addressed chiefly to professional political scientists, we will question the usefulness for public policy analysis of such head-spinning discourse. Attempts at rational discussions about whether or not a public policy proposal is worthy of implementation are frustrated rather than facilitated by igniting trepidation with seemingly irrefutable claims of catastrophe should the policy be adopted. The use of the word "could," and its variants, in the SSR appears calculated more to end discourse than to engage in it. No further discourse is possible when a position is based upon arguments that are, to use Karl Popper's term, "unfalsifiable." Unfalsifiable arguments are impossible to disprove. Popper uses this concept to distinguish science from religion and superstition. Science continues as an enterprise of learning because it welcomes the refutation of hypotheses. Religions and superstitions reach for the intellectual security of Eternal Verities, which cannot be refuted (at least in the minds of Believers).[42]

One example of an unfalsifiable argument is the well worn admonition, "The End is Nigh," which has never been disproven. Indeed, one discussion of false Armageddon predictions has it that the first warning on record is found on an Assyrian clay tablet from 2800 BC.[43] Perhaps this exhortation has such endurance with its gullible and naïve adherents because it is impervious to both logical criticism and empirical disproof, thus creating the illusion of Indubitable Truth. By logic, just because the End has not yet occurred, does not mean it will not occur – and soon. Empirically, it is unfalsifiable because with each failure the prediction can simply be moved to "tomorrow."

The SERVE Security Report attempts to win its case by relying primarily on three unfalsifiable claims. These are:

1. **The Invincible Could**
We have shown some examples of how arguments turning on the word "could" can be unfalsifiable, and we will show more as we proceed.

2. **Success Predicts Failure**
The authors of the SSR write, "the lack of a successful attack [on SERVE] in 2004 does not mean that successful attacks would be less likely to happen in the future."[44] Here is the same form of argument as "The End is Neigh." Logically, just because the world did not end on 12-21-12 does not mean that the end would be less likely to happen in the future. On the assumption that it has got to end sometime, each new prediction will be more likely to come true than the prior failed prediction.

Likewise, a successful run of SERVE does not necessarily bode well for the future; "quite the contrary, future attacks would be *more likely*."[45] Thus, with each successful use of online voting, according to this form of imagining, the odds *increase* that a catastrophe will strike. Why would the odds increase? Its simple, "both because there is more time to prepare the attack, and because expanded use of SERVE or similar systems would make the prize more valuable."[46]

In other words, according to these four Ph.D. computer scientists, success is a sure-fire prediction of failure. Contrary to commonsense, each new success does *not* show that more success is possible. Instead, success increases the odds of failure. Lewis Carroll could not have stated the case more clearly than this: "In other words, a 'successful' trial of SERVE in 2004 is the top of a slippery slope toward even more vulnerable systems in the future."[47] Ergo: Internet voting should not even be tried, because it might succeed.

3. **Invisible Attacks**

SSR: "the fact that no successful attack is detected does not mean that none occurred."[48] Here, the argument is that not only does success predict failure, but success can be an invisible failure. With online voting, no one can ever know for certain that the winner of an election is really the one who received the majority of votes, in part, because a hidden code in the computer that tallies the vote could have elected the candidate who actually lost the popular vote.[49]

Logically, this "invisible fraud" argument is invincible. Just because P appears to have won the online vote does not necessarily mean for certain that Q was not the real winner. Armed with this unfalsifiable charge, the four Ph.D.'s, and their followers, can challenge the validity of every online election, and they do not need a scintilla of actual evidence of fraud; indeed, in their method of imagining, the lack of evidence just shows how well the fraud was pulled off.

It is true that in university computer science labs demonstrations have been made of well hidden codes, and even of self-erasing code. True, too, such code can be "extremely difficult to detect" in the tens of thousands of lines of code that online election servers need. However, that code must be installed by stealth to have an effect on an election. So this argument presupposes the failure of every security measure put in place, without having to demonstrate the actual failure. Unfortunately, such dogmatic discourse does not lend itself well to a mature deliberation about so important a public policy proposal as whether or not to implement Internet voting.

Harkening back to Popper, if you can't know the truth or falsity of a proposition, then it is no longer within the realm of scientific knowledge, but has become myth. To say that the security of Internet voting can't be determined because hacks can be done without detection, creates an unfalsifiable proposition. This takes the computer scientist out of the realm of "science," and puts him or her in the myth-making department.

In any large scale election, no one can know for certain that the results represent the will of the majority. Outside a room of 50 people, where everyone can see every raised hand, some *trust* in the process will be required. A large scale election that does not require some trust in the process by the electorate is not possible. US presidential elections draw well over 100,000,000 votes. These are counted in thousands of local jurisdictions. Each jurisdiction passes its count on to a small number of state authorities, which uses the totals to determine the slate of Electors for the state's Electoral College. No one on Earth can ever know *for sure* whether error or misconduct affected the reported results. Indeed, as we will argue again later in this paper, in a representative democracy, like that of the United States, even with checks and balances, some trust is essential to the operation of the system.

To deserve respect and consideration, then, the imaginary vision of an invisible attack in an online election must pass at least two tests of reasonableness. First, a realistic sketch must be made of how a cheater could install the malicious results-changing code without being either foiled or caught by existing security measures. Second, a creditable explanation must be given as to how that code could remain in the server, or a voter's PC, without being detected by existing security measures. But, as we will show, whether as to server-side attacks or client-side attacks, the mere claim of "easiness," and other arguments, made in the SSR fail to meet either of these two tests of reasonableness.

Easy Installation

In addition to its unfalsifiable claims, the SSR frequently comments on how "easy" it is to carry out the various forms of attack they reference. They write, for example, that "The terms Trojan horse, virus, and worm all refer to types of malicious code, differing only in the means by which they get transported to the computer and get executed. … Malicious code is one of the most serious security threats in any application, because it is so *easy* to install, and so difficult to detect."[50]

Despite the condescending praise the four dissenters gave the SERVE construction team, the SSR includes attacks on a SERVE server in its use of the term "easy." While certain that the PCs of voters cannot be relied on to be virus free, the authors caution their readers that the "threat of SERVE-specific viruses should not be discounted."[51] The authors warn with foreboding that the "ability of an arbitrary outsider to learn on a wide scale how voters voted is enough of a threat to democracy that we think this alone justifies canceling the SERVE project. The fact that the attack is relatively easy to mount only strengthens our claim."[52]

But when they say "easy," do they mean "easy" *despite* all of the security measures taken by the builders of SERVE to keep out malicious code, or "easy" if you do not consider those protections? As inspectors of the SERVE system they knew of the many threat mitigating defenses which we discussed above, and which would be in operation during the 2004 election. These would include decryption key management protocols being followed, security guards on duty, and the FBI Elections Division and other law enforcement agencies on high alert and monitoring SERVE's environment, as they would be during an actual election.[53] The authors of the SSR completely fail to engage the law

enforcement capacities of the FBI and other policing agencies, just as they pretend that SERVE voters had little or no security protections. How "easy" is it really to commit large scale voter fraud without detection by the FBI? While the SSR imagines that anyone with a computer could sway an election, they neglect to mention the risks to the would-be cheater. Knowing of the possibility that voter fraud can result in arrest, huge lawyer fees, costly fines, time in prison, and all the social and economic consequences of a felony conviction, how many people who are intelligent enough to figure out how to commit such a crime are really dumb enough to try? This supposed "easiness" of election malware installation seems to be solely a product of their method of "imagining."

The SSR creates the impression that voter privacy on SERVE's server could be easily violated. But, specifically to protect the privacy of voters against malicious spyware SERVE was equipped with "Digital Signatures, Secure Socket Layers, Encryption, Voter Identity/Ballot Data Separation," and the means for "Voter Ballot Data Verification." To protect specifically against Trojan horses, viruses, and worms, SERVE had the capacity for "Anti Virus Scanning," and used "Digital Signatures," and "Voted Ballot Data Verification." Thus, the authors of the SSR fall far short of intellectual honesty by proclaiming how "easy" it would be to install malware or spyware on a SERVE server without engaging directly and specifically the security environment and the defenses built into the SERVE system precisely to protect against malicious code in its servers.

The authors assure their readers, without further explanation, that once malware has been installed (magically?), "Even experts with access to the source code of a program may not be able to tell if there is malicious code in it, since it is relatively easy to disguise malicious code so that it is extraordinarily difficult to find."[54] Those authors fail to mention both SERVE's "Anti Virus Scanning" software, and its protocols for the regular review of event logs, which would catch any installation of malware by an insider.

To make it "easy" for themselves, the authors conveniently by-pass any mention of those protocols, and simply speculate generally that "New viruses almost certainly will not be detected by most current virus checking software. Moreover, it is not too difficult for attackers to build new viruses, or to modify existing viruses sufficiently that they will avoid detection."[55] But mere conjectures on the supposed easiness of installation dodge the responsibility of these critics to engage the total security environment, and to specify the short comings of SERVE's security protocols and anti-virus scanning capacity. In the opinion of this writer, no rational public policy discussion should tolerate the avoidance of this intellectual responsibility.

The Specter of DDoS

One of the threats to the convenient use of the Internet is that a website server can be overloaded with visitors, freeze, and become inaccessible to other visitors. This can happen accidentally, as when the server simply receives more visitors than it is equipped to accommodate. However, access to a website can also be slowed or stopped by a deliberate attack. Computer scientists call this a "denial of service" (DoS) attack. A special form of a DoS attack is often referred to as a "distributed denial of service"

(DDoS) attack. This occurs when one person, or group, controls many computers and directs them to a particular target.

The SSR correctly states that "the robustness of a website against network flooding attacks is determined largely by the network capacity available to that website."[56] In other words, website hosting servers are constructed to handle an anticipated amount of traffic. If the server is suddenly faced with significantly more visitors than it was built to manage, it will freeze and block further attempts by computers to connect with it. This capacity to handle traffic is also referred to as the server's quantity of bandwidth.

The FVAP anticipated both that it would need sufficient quantity of bandwidth to accommodate thousands of voters at one time, and that a denial of service attack was a threat to be guarded against. Thus, the SERVE builders took not one, but several measures to defend the system's operations under a DDoS attack. According to David Chu, the SERVE system employed a "Large Quantity of Bandwidth, Multiple Carriers, and Multiple Internet Service Provider Entry Points."[57] The system administrators also planned to monitor the utilization of the system so that DDoS attacks could be seen coming, and defensive action taken, before the attack could overload the system. These are standard defenses and strategies.

As members of the SPRG, the authors of the SSR were fully aware of all the security measures taken by the SERVE team. But, in an act of omission that can only be described as disingenuous, the authors of the SSR said nothing about these measures built into the SERVE system. Instead, they simply laid out the bald assertion that, "It seems unlikely to us that SERVE could withstand such a high volume DDoS attack."[58]

Consistent with their "we can imagine" methodology, the SSR writers conjure up a spectacular scenario, treat it as a fact, and base their conclusion that SERVE is defenseless on that "fact." They imagine that

> It is *plausible* that an attacker could gather a 'zombie network' of 10,000 slave computers, and each computer could initiate about 50 new SSL connections per second. Consequently, an attacker could generate 10 to 100 times more SSL traffic than the SERVE website is *likely* to be able to handle. Thus, a DDoS attack against SERVE's SSL web servers *could* render SERVE unreachable to voters and disrupt an election in progress.[59]

Of course, this kind of "reasoning" will always be irrefutable. No matter how many "SSL connections per second" SERVE is equipped to handle, the SSR writers will simply raise the "plausible" number of zombies needed to defeat it in their imaginary scenario. Pitted against imagination, SERVE can never win.

Here are some more "coulds:" "An attacker *could* mount a large-scale denial of service attack that renders SERVE's voting service unavailable on the day of an election. Those voting on Election Day would be unable to vote, calling into question the validity of the election."[60] Of course, the authors of SSR knew that Internet voting is typically spread

out over several days as an "early voting" option. So this scary scenario, assuming only one day of voting, is more easily refuted than some of their other imaginings.

DDoS attacks can be stopped by several different means. One is to switch servers, as SERVE was prepared to do. Another is to trace the attack to its source and block traffic from there. The servers being used by the attacker can also be shut down. So, this Election Day argument is weak. But, perhaps anticipating this refutation, they offer another alternative scenario.

Imagine this – a "last-day denial-of-service attack." The attacker cleverly lies in wait to disenfranchise all the procrastinators and late deciders. What "possibilities" are implied by this scenario? "With SERVE, there is the *possibility* that the disenfranchisement rate could rise to close to 100%."[61] Although this "possibility" is drawn from thin air, as opposed to any sort of research or experience, they recommend killing the project, because "we consider last-day denial-of-service attacks a significant threat to the security of SERVE's elections."[62] Of course, by demanding that SERVE be shelved, they become responsible for disenfranchising 100% of the UOCAVA voters who, for a variety of reasons, could not vote by mail.

Given all these "possibilities" and imaginings, one may wonder if there are any actual facts upon which rational people can assess the kind of threat that DDoS attacks really pose to elections using Internet voting. The SSR refers to only *one case* of an election being disrupted by a DDoS attack.[63] In 2003, the New Democratic Party of Canada (NDP) held its officer elections, and offered online voting as an early voting option along with other ways of voting. During one of the days of voting the online process was slowed, but not stopped, by a DDoS attack. The technicians operating the system blocked the attack within 45 minutes.[64]

There are only two other examples of an election using Internet voting being disrupted by a denial of service attack, which occurred after the SSR came out. Ironically, in another NDP officer election event access to the website was slowed. But the exact cause of the problem has not been fully determined. It might have been caused by a DDoS attack, or it might have been a result of too little bandwidth being clogged up by an unexpected surge of legitimate voters. Either way, the problem was resolved when the traffic slowed.[65] An Internet voting option has been offered in about 50 different municipal elections in Canada over the past decade, and *not one* instance of a DDoS attack, or other security issue, has been reported.[66]

The EAC "Survey of Internet Voting" repeated an allegation of a DDoS attack on an online voting trial for students in Austria, during the 2009 Austrian University Elections. However, no facts were given as to how long the voters were denied access, if at all.[67] In its survey of over 30 Internet voting trials around the world, the EAC Survey did not mention any other instances of a denial of service attack even being alleged.

When *facts* such as these are compared to the *imaginings* in the SSR, the threat of denial of service attacks appears less frightening. The facts indicate not that DDoS attacks can

be dismissed as insignificant, but that the professionals who set up the Internet voting systems can be relied upon to include effective defenses and mitigation strategies, such as they did with SERVE. Unfortunately, the myth of Internet voting vulnerability to DDoS attacks has other perpetrators, as our discussion of NIST will show.

E-commerce and Internet Voting

The New York Times quoted the SSR's claim that "e-commerce grade security is not good enough for public elections."[68] In support of that claim the authors of the SSR argue, *inter alia*:

> In a commercial setting, people can detect most errors and fraud by cross-checking bills, statements, and receipts; and when a problem is detected, it is possible to recover … In contrast, voting systems must not provide receipts, because they would violate anonymity and would enable vote buying and vote coercion or intimidation. [But] it is still vital for the system to be transparent enough that each voter has confidence that his or her individual vote is properly captured and counted, and more generally, that everyone else's is also.[69]

Here, again, those authors omit to engage what they knew to be the measures taken by FVAP to meet that criterion of transparency and voter confidence. As noted above, SERVE provided a method for voter verification. After marking the ballot, the voter would send it to the server, and the server would put up a confirmation widow showing the voter the vote that the system had for recording. The voter then had an opportunity to correct any errors.

Without elaboration the SSR simply dismisses SERVE's voter verification process with the contemptuous remark that "The mere presence of a confirmation screen does not prove that the vote was recorded correctly."[70] But, of course, the voter does not ask for "proof," but only reasonable assurance that his or her vote was counted as cast. For opponents of Internet voting like the SSR authors, nothing could ever satisfy their requirements of "proof." Because SERVE was never used, follow up studies on voter confidence in this verification method could not be conducted.

Another difference between e-commerce security and SERVE's security is that e-commerce websites are online 24 hours a day, seven days a week, and 365 days a year. This gives hackers an endless amount of time to poke at the systems for security vulnerabilities, and to experiment with different attack strategies. An online voting platform that is only up for two or three voting days does not offer such opportunities. Also, in such a lengthy time, the chances of disgruntled or greedy employees turning against their employers is greater than it would be with a small team of personnel who have had security clearances by the US Department of Defense, and who are working intensely on a very short term project. E-commerce employees working at routine jobs are also more likely to be distracted, or to make mistakes over the long haul, than are skilled technicians on high alert for a short time.

Like other opponents of Internet voting, the SSR reminds its readers of the multitude of news reports of alleged "hackings" of government and commercial websites. However,

the circumstances that enabled the hacks to happen are rarely examined, nor is light shed on the differences in the types of hacks. A superficial defacing of a commercial website's home page is given the same coverage as an unauthorized withdrawal from a victim's savings account. Thus the occurrences of really serious crime are inflated in the minds of the public.

Yet the explanation is rarely given that the victim may have enabled the crime by his own carelessness. People who open every email and uncritically click on the links they present, or who download free screen savers or other "freebies," visit websites with free music or porn, or who fail to purchase quality commercial virus protection systems are far more likely to fall victim to online crime than are the more prudent folks.

Recently, the New York Times gave prominent coverage to a report that the Chinese military was engaging in industrial espionage by hacking into the computer systems of US corporations.[71] But the 3000 word Times story was written in an upside down fashion. That is, it led with the sensationalistic announcement of all kinds of hacks on US corporations, but only towards the end did it introduce a little education. By far, most of the attacks were not cold hackings coming from out of nowhere. The Chinese sent trick emails to corporate officials who then clicked on links, which instantly let in the malware. For example, Coca Cola was in negations to buy a Chinese company. One email posed as part of the business communications, and Coke was hacked. But in other instances, sharp employees knew better than to click on links in email. They turned over the emails to security, and saved their companies from the headaches Coke executives had. If the Times had given as much attention, in this and other such articles, over the years to educating its readers on how to avoid being fooled by trick emails, perhaps many system penetrations could have been prevented.

Despite the stream of e-commerce hacker news, in the context of understanding Internet voting security issues, the SSR's references to common computer crime is a Red Herring. In addition to what has been said about the lack of public education about security self-protection, election officials cannot be held responsible for the victims of computer crime any more than they can be held responsible for the victims of purse-snatchings when these happen to voters going to and from polling places, or auto theft that happens while the voter is waiting in a long line to vote. Computer crime exists; but that is no reason to forgo online voting. If election officials make an effort to educate voters as to their responsibility to protect themselves, and to inform voters about how to protect themselves during the election process, the amount of online election crime could be significantly reduced, if not eliminated. Experts in computer security could help election officials to prepare such an education program.

While the New York Times eagerly printed the catchy quote, "e-commerce grade security is not good enough for public elections," its reporter made no effort to inform his readers as to how they can protect themselves, and he asked no questions challenging the comparison of online commerce and online voting, nor did he ask why the SERVE security measures could not be relied upon. Apparently, while cries of impending

catastrophe make a sensational story (news that's "fit to print"), educating readers about how the doom can be avoided is too dull an endeavor.

More of the specific claims of Internet voting insecurity will be examined in the discussion of NIST's unfortunate role in this propaganda war on that voting technology. But first some accounting will be given for how the myth of Internet voting insecurity, based on the claims in the SSR, swept the nation in the days that followed the publication of the allegations by the New York Times.

Part II. THE BIRTH OF A MORAL PANIC

Wolfowitz's order on February 5, 2004, to halt the SERVE project was the direct cause of SERVE's demise. The New York Times states what is known of that order: "Paraphrasing the memorandum, a Department of Defense spokeswoman said: 'The department has decided not to use Serve [sic] in the November 2004 elections. We made this decision in view of the inability to ensure legitimacy of votes, thereby bringing into doubt the integrity of the election results.'"[72]

However, there are unanswered questions about that order, to which a complete history of Internet voting in the US should have answers. For example, what factors weighed most heavily in Wolfowitz's reasoning? His order to Chu clearly implies a lack of confidence in SERVE's security measures. The focus on "legitimacy of votes" can entail several items. It might mean the concern that votes could be changed on the voter's machine, without the voter or the FVAP authorities knowing. Another concern Wolfowitz might have had is that the votes cast could be coerced or cast by someone who has bought or stolen the voter's credentials. He might have been worried that the final tally would be unreliable, both because the SERVE server could be hacked and the votes changed on it without detection, or because he did not trust the system's capacity for auditing. Besides the SSR, what other reports, studies, or publications, or who influenced him is not available in public records. The order was not made public.[73] Whether he was personally convinced of SERVE's supposed vulnerability, and based his order on that conviction, or he gave the order to quiet public outcry, is currently unknown. There was public outcry, and we will examine the main causes of it.

Unfortunately, Wolfowitz has not elaborated on his reasons for shutting down the SERVE project. Wolfowitz is reported to have also said in the memo that he would reconsider his decision only if researchers can prove that integrity can be maintained.[74] Apparently, that proof was never forthcoming. While the record is clear as to what the SSR arguments against SERVE were, there is no record as to what, if any, FVAP personnel pled to Wolfowitz in SERVE's defense. Indeed, while the press and other news media gave widespread coverage to many of the specific, and most sensational, charges made against SERVE by the four critics, there is no public record of any intellectually equivalent rejoinder in defense of SERVE.

The January 21st article in the Times, which originally announced the SSR's claims, gave several reasons why voting on SERVE "could be catastrophic."[75] The information the

Times publishes is, in many cases, all that the public learns of an issue. Thus, if the Times, and all the secondary publications following it, give a one-sided sensationalistic report, calculated to alarm and frighten readers, then that will likely be all that enters the minds of the public. The Times story included such emotionally weighted phrases about SERVE as:
"inherently insecure and should be abandoned;"
"Trojans, viruses and other attacks [are possible, and] could be carried out on a large scale;"
"unacceptable risks of election fraud;"
"malicious software [could] monitor the users' activities, scan them for private information;"
"introduces greater risks just to gain convenience;" and,
"How do we recover if an election is compromised?"
For many readers, these phrases might sound like a Paul Revere alarm that another government boondoggle is coming, and concerned citizens should demand it be stopped before the "catastrophe" of a corrupted election befalls the nation. (Indeed, a New York Times editorial says no less two days later.)

But in reply to such disturbing charges as those, and that using SERVE "could enable hackers to disrupt or even alter the course of elections," a FVAP spokesperson gave an arid and tepid response. Representing DoD and FVAP, Glenn Flood told the Times that the four critics were a "minority" of the 10 SPRG members, and that they "overstated" the security risks. An official for Accenture, the lead contractor on the project, said the critics drew "unwarranted conclusions." She also claimed that five of the other six SPRG members told her they would not recommend shutting down SERVE. The Times reporter quoted one of the six non-dissenting SPRG members as saying the four critics were simply reflecting "the professional paranoia of security researchers."

That's it. No energetic, hard hitting, blow-for-blow riposte from the SERVE side; at least nothing that made it into that report by the Times, or other public sources. While opinions can differ, considering the *emotional appeal* of the discourse presented in the Times story, one can understand why such a lethargic defense did nothing to slow the momentum set in motion by the alarming report in the Times. More on how that momentum of public opposition to SERVE was sparked and kept fueled can be learned from an insider's account.

Introducing Avi Rubin

About two years after Wolfowitz issued his February 5, 2004, halt order, Avi Rubin, one of the four SSR authors, published a memoir of that period.[76] He writes about how, before being invited to join the SPRG, he was a leading figure in the publicity campaign against the burgeoning use in the US of DREs, or direct recording electronic voting machines. The use of those machines was prompted by the passage of the Help America Vote Act of 2002.[77] Following the infamous "hanging chads" in Florida in the 2000 election, the Act, among other things, made nearly four billion dollars available to states as reimbursement for upgrading their voting technology. Rubin became a leading critic of the DREs when he published an essay exposing what he saw as numerous security

flaws in the source code of a popular DRE model built and sold by the Diebold Corporation.

An anti-e-voting activist, Bev Harris, discovered in 2003 that the source code was on a Diebold website, and unprotected. She posted the link for all to see on her blog as a prank. When Rubin heard this, he downloaded the source code to his office computer at The Johns Hopkins University. Once Rubin had written out his critique of the Diebold code, he devised a strategy for publicizing his exposé. Prior to teaching, he had worked for six years at AT&T, where he fortuitously underwent "media training."[78] Given this training, Rubin "sensed that his exposé was going to be a public relations hot potato."[79]

He put his PR training to good use. He writes,

> From the beginning, my plan was to break the story in the New York Times. I wanted this story in the hands of a reporter I could trust to get it right, someone who was … sensitive to the political ramifications. If the first story doesn't get it right, any misinformation it contains is likely to be repeated countless times. The reporter I trusted most was John Schwartz, who covered technical issues for the Times.[80]

Rubin had provided Schwartz with technical advice in the past. On July 24, 2003, the New York Times ran the Diebold story.

Rubin had learned from his media training that "the second day after a news release is the big day for media coverage. That's when all the stories that follow the original one appear."[81] Sure enough, the next day, his local paper, the Baltimore Sun, made his report "its lead story on the front page."[82] Not only that, to his delight the story was printed "above the fold," where readers could see it in vending machines. Beyond that, the following "Sunday the Sun put the story on the front page again."[83]

After making the deal with Schwartz, Rubin contacted "the vice president at the CNN national desk, Nancy Lane."[84] They arranged to interview Rubin "in a studio in Baltimore" on the day the Times broke the story.

A man of foresight and energy, Rubin made further preparations. He informs his readers that the day before the New York Times was to run the exposé, "I had prepped Adam and Yoshi," his two grad student research assistants.[85] The trio spent several hours in a Johns Hopkins classroom polishing, memorizing, and rehearsing the key phrases that Rubin wanted to feed the media (and, hence, the public).

He had learned from his public relations training at AT&T that the more complex a statement to the press is, the more likely they are to get it wrong when they present it to the public. To control the message, you have to keep it simple. "The main idea is to boil your information down to no more than three short, simple, and memorable messages … that will stick in the minds of readers and [TV] viewers."[86] Rubin writes, "we practiced ways to work these quotes into our answers, even if they didn't directly answer the questions asked. … I grilled them for hours." The effort paid off, and the trio was "amused and gratified" when "many of these quotes turned up verbatim in news stories over the next few weeks."[87]

Once the Diebold story came out, Rubin shot to celebrity status. His memoir is replete with detailed accounts of all his TV appearances. He writes, for example, "I was on The Today Show a couple of times and on NBC's and CBS's national evening news shows, and … on The Daily Show with Jon Stewart."[88] He also fully discusses his radio and press interviews, his speeches, and the articles he was asked to write for magazines and newspapers. He became so famous, according to his narrative, that one story on his blog, about serving as a voluntary poll worker, received "forty thousand hits," and became the subject of even more stories in the press.[89] Later, Rubin was called for a meeting with members of the House of Representatives, which he notes was covered by the "NBC Nightly news."[90]

Potential, not Experience

Rubin candidly reports receiving much criticism from other computer scientists about his methods for analyzing the security vulnerabilities of DRE voting machine code. For example, lawyer and Carnegie Mellon computer science professor Michael Shamos, conveyed to Rubin that "the lack of fraud in previous electronic elections made the concerns about it unrealistic."[91] But Rubin rejects this method of trying to assess the likelihood of fraud from the study of what happens in actual situations. He writes, "I believe in assessing *vulnerability*, not past performance. *Potential*, not experience."[92]

To further illustrate his methodological point, Rubin writes that he was questioned by Ohio congresswoman, Marcy Kaptur, about his claim that hacked DRE code could be used to the advantage of a political party. "Diebold's base of operations was in her home state."[93] He frankly admitted to her, a Democrat, that in his examination of the DRE code, "we had not seen even the slightest indication that the [Diebold] voting machines were rigged to favor one party over another. In fact, [he and his two assistants] hadn't seen any evidence of tampering at all. Our point had to do with potential fraud."[94]

Rubin saw his methodological approach soundly rejected in a Maryland court. In *Schade v Lamone*[95] an anti-e-voting group in Maryland sought an injunction to try to stop the state from using the Diebold machines in the 2004 November election, or at least to compel Diebold to make its machines print a paper record of the votes. Rubin submitted his Diebold analysis as evidence, and testified as an expert witness for the Plaintiffs. Michael Shamos testified as the expert witness for Maryland, the Defendants.

The court stated, in part, that while the witnesses for the Plaintiffs "indicate catastrophic, doomsday-type scenarios, nevertheless, the Court is impressed with Dr. Shamos's testimony this will not occur. The Court is confident the votes of Plaintiffs will be counted."[96] The court opined, "No system is infallible. No machine is infallible. Under oath, all experts agree systems such as these [DREs] are much more secure and less vulnerable than the paper ballot, and even the opt scan ballots."[97]

The court also observed that "the overwhelming factual evidence clearly shows there have been no verified incidences of tampering with these machines anywhere in the United States. The votes have been counted accurately. Recounts have occurred with

complete accuracy, and there is no reason to believe this will not continue."[98] During the hearing, said the court, in sworn testimony "All experts agreed the use of paper ballots is the least accurate of all systems and lends itself to the most chicanery. On the other hand, the experts seem to agree, if untampered, the Diebold-type voting machines are the most accurate in recording and counting votes."[99] The petition for an injunction was denied.[100] The decision was upheld on appeal.[101]

Rubin was stunned by his experience in the hearing. In his view, the lawyers were not there, as he was, to find "objective truth."[102] "I walked out of the courthouse and wandered the streets of Annapolis."[103] Showing his pique, Rubin contemptuously dismissed the lawyers, the expert witnesses who testified in favor of the DREs, and the judge as more of those "technically illiterate people" found "throughout the legal system."[104] Because of that experience, Rubin rejects the US legal system as a source of "objective truths," and says that only by funding research institutes, like the one he had just founded, can the truth be known.[105]

Rubin and his cohorts were unswayed by such criticism, whether from courts or colleagues. David Jefferson, a veteran anti-e-voting activist and one of the four SERVE critics, had also heard many similar criticisms from his colleagues. In an interview he said, "I think they believe our concerns are exaggerated – either that it's not really possible to undermine the election to the extent we say it is or it's all theoretical and academic."[106] Undaunted, they followed the same methodological principles in their estimations of SERVE's "potential" security flaws. In their SERVE Security Report, perhaps with some defiance, they listed many of their previous criticisms of DRE security vulnerabilities to hackers and insiders. "All of these criticisms, which we [still] endorse, apply directly to SERVE as well."[107]

The Election Integrity Movement

Judge Manck's characterization of Rubin's testimony in *Schade* as based on unrealistic "catastrophic, doomsday-type scenarios," coincides with much that has been said in the present analysis about the vacuity of the SERVE Security Report's fanciful methodology. The imagined dangers to democracy of DREs that Rubin divined were belied by the judge's finding of fact in *Schade* that "there have been no verified incidences of tampering with these machines anywhere in the United States."

Thus, one wonders whether the only intellectual foundation of the anti-e-voting "election integrity" movement in the US, informed by Rubin, consists of no more than Rubinesque divinations of *possibilities* that have never been realized. If so, such unreasoned hysteria would be sadly reminiscent of the socially unwise rhetoric of groups like the Anti-Saloon League prior to the ratification of the Eighteenth Amendment in 1919. Laws based on ill-reasoned foundations, like those prohibiting the sale and consumption of intoxicating beverages, and, worse, those permitting slavery, tend to have consequences that have proven antithetical to the public good. Since politics is their field of study, political scientists are well positioned in our society to carefully scrutinize activist demands for "election reform," and to alert law makers and the public when they find that those

demands are based on irrational Rubinesque foundations. By doing so, this profession might help public policies to stay the course of Reason.

The *Schade* decision was rendered in September of 2004. That was too late to lend any assistance to the defense of the SERVE project. Wolfowitz had ordered the project stopped in February of that year. But our digression into the *Schade* case helps to amplify our sketch of the kind of reasoning that lead to the demise of SERVE. We will continue using Rubin's memoirs of the period to further explain the original steps that resulted in the current widespread doubt about the security of Internet voting.

SPRG

Two weeks before the New York Times broke Rubin's Diebold "exposé" (which was done on July 24, 2003), the first Security Peer Review Group (SPRG) meeting was held to discuss the SERVE system. As we have said, SPRG was a 10 member group of computer scientists who were invited by FVAP to inspect the system. There was a second team, which included the CIA and the National Security Agency; but they made their suggestions privately, and did not call for terminating SERVE.[108] Still working furiously on his Diebold report, Rubin "was only able to attend by phone."[109] He writes that the SERVE team "seemed unafraid to share openly the details of the system. Those details, unfortunately, horrified me."[110] But he was too busy with the Diebold essay to do anything about SERVE at that time.

The second SPRG meeting was a two day affair held in Reston, Virginia in early November 2003. "After the second day of review, several of us determined that if we failed to act, SERVE would almost certainly be adopted and implemented."[111] That is when the four dissenters decided to write their exposé alerting the public. "We set at it immediately, working late into the night and continuing over the next couple of weeks, firing drafts back and forth to each other over e-mail."[112]

Having hit the news stands about six months before he and the other three started in on their SERVE Security Report, Rubin's Diebold exposé was still "a public relations hot potato." But Rubin had already learned many lessons from this experience about maximizing public exposure for his exposés. So he took the lead of his SSR co-authors. He writes, "I convinced the others to work again with John Schwartz of the New York Times."[113] As before, Schwartz was given the exclusive.

Rubin notes that he and his cohorts "had hoped to manage the release of the report to the media carefully, as had happened with the Diebold report."[114] Unfortunately, Schwartz failed to get the story on the front page of the New York Times. But that was not much of a set back, for, as Rubin understood, "the second day after a news release is the big day for media coverage." And so it was. The second day reports mimicked the Times's model of leading with the emotionally alarming allegations of "easy" to execute dangers to democracy, followed by a reserved response in defense of SERVE.

The Washington Post ran the story on their front page the day after it came out in the Times.[115] The Post headline was, "Pentagon's Online Voting Program Deemed Too

Risky."[116] Above the fold, the alarming lead sentence declared, "A Pentagon program for Internet voting in this year's presidential election is so insecure that it could undercut the integrity of American democracy and should be stopped immediately." The story quoted Avi Rubin and Barbara Simons as saying "their biggest fear is that this year's experiment would be a hit, leading to widespread Internet voting for the 2008 presidential election. That is when the kind of Internet attack they envision could emerge, possibly from foreign subversives."

Coming just two years after the 9/11 Al Qaeda bombing of the Twin Towers in New York City, many readers likely found the "vision" of "foreign subversives" attacking "American democracy" to be a credible scary scenario. Perhaps aiming for "balanced reporting," the Post quoted a couple of SERVE team members as pleading it's only "an experiment," and could yield useful knowledge. But to this rather pedantic defense, Barbara Simons countered, "calling the program an experiment ignores the fact that voters will be casting votes that will count. If there is a question about the legitimacy of those votes, she said, the election could be undermined. It is no favor to overseas voters to let them think they have cast ballots when they have been fleeced, she said." No defense matching the emotional punch of "fleeced" voters was given.

Also the day after the Times story broke, CNN reported the news.[117] On its web page CNN's lead sentence said, "A federally funded Internet-based voting system due for release in less than two weeks is inherently flawed and should be scuttled because of weak security, according to a report by a team of computer scientists." Then, "According to the report, the online nature of SERVE could easily allow a hacker to tamper with the voting results. … Among the type of hacks the researchers outlined are ones that would overwhelm computers with a denial-of-service attack."

For the appearance of balance: "The backers of the SERVE system downplayed the findings Wednesday, saying other experts disagree." Then the tepid Glenn Flood quote, "This is a minority report from one of the peer-review groups … of about 10 or 11 members, only four of them decided that concerns were warranted." This was hardly enough to calm the emotions aroused by the lead.

Computer World, a widely read print and online IT magazine, also reported on the SSR the day after the New York Times broke the story. The lead sentence: "A federally funded Internet-based voting system scheduled for use in the 2004 primary and general elections has several unresolvable security vulnerabilities that leave it open to widespread vote tampering and privacy breaches."[118] Quoting SPRG member David Wagner, who favors the methodological terms "easy" and "could," the article goes on,

> For instance, it would be relatively easy for malicious hackers to insert spoofed Web pages that appear to belong to the SERVE system but are actually designed to alter votes or prevent them from being cast. A voter using a PC infected with a virus or worm could easily jeopardize the integrity of the system … An attack on the main SERVE system or any of the PCs being used by voters, using any of these methods, could seriously compromise the results … And the particularly dangerous part is that

> … SERVE is susceptible to large-scale election fraud that could be launched from outside the reach of U.S. law and go completely undetected.

Then Avi Rubin added, "I think that a dedicated and experienced hacker could subvert the election rather easily … I don't think that Internet-based voting such as SERVE can be made secure enough for use until we can develop computer systems that are not vulnerable to viruses and Trojan horses, and until we can develop an Internet that is resistant to denial-of-service attacks." As usual, failing to challenge any of the "easys" or "coulds," or to respond to any of the specific charges, and completely missing the emotional punch their presentation carries, Glenn Flood is quoted as repeating his standard reply that FVAP "welcomes" the input, but these are only four critics out of the ten-member SPRG, etc.

For some semblance of balance, the Computer World article closes with a quote from the SERVE website (since taken down) explaining that to protect voter information and ballot integrity the SERVE system "uses the latest security technology available." But the article does not use this quote to challenge the critics of the system; instead, it criticizes the website for making such "claims without offering specifics."

Building Momentum

The reports by the Washington Post, CNN, and Computer World represent the scores of second day stories that came out in print, on the air, and on the World Wide Web. Like a fish story, the re-telling of the SSR allegations grew and grew. Just as an earthquake on the ocean floor can cause a tsunami that wreaks havoc on land dwellers in its path, so that combination of re-publications of SSR allegations sent a wave of meaning throughout the minds of the US public that wreaked havoc on the possibilities for Internet voting in this country. Without any rational challenges, the "ease" of hacking, and imminent likelihood of all the "coulds" became folk lore, accepted without doubt.

On January 23, 2004, the New York Times published an editorial designed to fuel the flames of opposition to SERVE ignited by its piece two days earlier.[119] The editorial singles out "Aviel Rubin" for special mention as among the "Four computer scientists brought in by the Pentagon to analyze a plan for Internet voting by the military." Then, as if they were heroic whistleblowers, rather than a dissident minority, the Times mentions that these four were the only ones to issue a report among the ten 10-member advisory committee. No mention was made of the second "committee."

Suspending all critical judgment, the editorial repeated the methodological terms of the report, such as "potential," "possibilities," and "could," to alert the world that

> the *potential* for hackers to steal votes or otherwise subvert elections electronically is too high. … the *possibilities* for compromising the secrecy of the ballot, voting multiple times and carrying out vote theft on a large scale would be limited only by the imagination and skill of would-be saboteurs. Viruses *could* be written that would lodge on voters' computers and change their votes. Internet service providers, or even foreign governments that control network access, *could* interfere with votes before

> they reached their destination. … the advantages of the Pentagon's Internet voting system would be far outweighed by the dangers it would pose. [Emphasis added.]

Although no science, nor actual experience, was cited in support of all its "coulds" and "possibles," the great newspaper righteously demanded that "Congress should suspend the program." Unhappily, for anyone who values a more balanced public policy debate, not one question was asked in this diatribe about the methods these four "scientists" used to arrive at their alarming conclusions. Only the conclusions were published. There was not a word about the opinions of the other experts and the entire SERVE team in defense of SERVE. Not even a tepid quote of Flood. Indeed, the editorial gave the impression that the frightening possibilities it enumerated was the one and only way to understand Internet voting.

Two weeks later, Wolfowitz issued his halt order, and SERVE was done for. Although it is not known exactly why he took this momentous decision, the unquestioning publication of the alarmist and sensationalist SSR by the New York Times, Washington Post, and other sources, plus the follow up editorial by the Times, no doubt contributed to his decision.

Once again, Rubin had hit another PR home run. He boasts that the SSR story took him on another round of celebrity appearances on TV, with more interviews by the newspapers and radio. He was called back to Congress, and invited to meet with the commissioners of the EAC.[120] Of course, in all this, the public only heard his divinations of all the dangers to democracy Internet voting invites. None of the pro-SERVE SPRG or FVAP members enjoyed such celebrity. Needless to say, there were no public debates or exchanges of opinion, and while Glenn Flood was occasionally quoted towards the bottom of printed articles, only the sensational allegations of the SERVE critics received widespread media publication.

In May of 2004, Rubin's PR insider, New York Times reporter John Schwartz, published an unabashed encomium on Rubin in the Times.[121] Completely oblivious to the lack of science or factual experience in Rubin's methods, Schwartz proclaimed that Rubin

> has become the face of a growing revolt against high-technology voting systems. … His critiques have earned him a measure of fame, the enmity of the companies and their supporters among election officials, and laurels: in April, the Electronic Frontier Foundation gave him its Pioneer Award, one of the highest honors among the geekerati.

Schwartz ends his plaudits by quoting David Jefferson's tribute to Rubin as "the most important figure in the United States in articulating the security problems with electronic and Internet voting."

Following Wolfowitz's order, a wave of "end of SERVE" news stories continued the public education about the issue. Given the fact that Wolfowitz had ended the project, the message to the public was that the allegations of security vulnerabilities were effectively confirmed by Wolfowitz's order. For example, the NBC report led with,

> Citing security concerns, the Pentagon has canceled Internet voting that would have involved as many as 100,000 military and overseas citizens from seven states in November, a Defense Department official said Thursday.
>
> The announcement comes two weeks after four outside security experts urged the program's cancellation in a scathing report. They said hackers or terrorists could penetrate the system and change votes or gather information about users. At the time, the Pentagon said it felt confident enough to proceed. … But Deputy Defense Secretary Paul Wolfowitz has since decided to scrap the system because Pentagon officials were not certain they could 'assure the legitimacy of votes that would be cast,' said a Pentagon official who spoke on condition of anonymity.[122]

In announcing the decision, the NBC report also enumerated some of the specific threats: "The experts specified these central risks, among others:
•There is no way to verify that the vote recorded inside the system is the same as the one cast by the voter.
•It might be possible for hackers to determine how a particular individual voted, 'an obvious privacy risk.'
•The system may be vulnerable to attacks from many quarters, some undetectable. Stealth programs as trojan horses that harvest data are sometimes installed on public computer terminals."

In Computer World's announcement, Barbara Simons was given a platform upon which to proclaim the most hysterical statement of this epoch. Simons was quoted as saying, "Our great fear is that there will be a major move to Internet voting, which I personally feel is a threat to our democracy. The bottom line is we could have our president selected by [hackers in] Iran."[123]

Nothing was said in SERVE's defense in this article. Apparently because "Polli Brunelli, director of the Federal Voting Assistance Program, wasn't available for comment."

By this time, of course, it was too late for anyone to try to defend SERVE, or to challenge the methods of those who condemned it. The public had its education on this policy issue. Internet voting was well on its way to "folk devil" status in the US. With one exception, Internet voting would go untried by any US election district or the DoD from 2004 to 2010.[124]

Internet Voting in the US After the Shelving of SERVE

The Michigan Democratic Party offered an Internet voting option to members for its caucuses in February 2004. The decision was made after a full debate over the issues of accessibility and security. This debate took place before the four SERVE critics burst into the public discussion on Internet voting. Times were different then. Writing prior to the publication of the SERVE Security Report, political scientists R. Michael Alvarez and Thad Hall observed that the consensus of the experts in the 2001 Cal Tech/MIT study, and "other studies," was optimistic. In their view, at the time, the rise of Internet voting seems "inevitable: Internet voting is the future of voting in the United States."[125]

Indeed, the Michigan experience bore out the optimism. Alvarez and Hall later studied the event. They found that there were more online voters in these caucuses than in any prior Internet voting trial. Of the 162,929 votes cast, 28.57%, or 46,543, were cast online. 14.41%, or 23,482 votes were sent in by mail, and 57.02%, or 92,904 votes were cast in person. Turnout was "much higher" in this year than in either 2000 or 1996.[126]

At a time when the "digital divide" was still considered a problem, and mindful of those who did not have a PC or access to a computer at the time, the party provided lap tops in public libraries, churches, and other places.[127] A CBS News survey of the online voters in the Michigan primary found that 67% said they used Internet voting for the convenience. 90% of these said they voted from home, and 8% from work. Despite the national media stock in trade predictions of doomsday and catastrophe, Alvarez and Hall report that "there were no successful attacks from pranksters and hackers."[128] The two political scientists did not find any voter disenfranchisement caused by offering online voting, but did observe that problems at polling places resulted in frustrating voters.[129]

After the successful use of Internet voting in Michigan, the behavior of government officials reveals how powerful the taboo on Internet voting had become. There were probably more violations of the incest taboo in the US between 2004 and 2012, than there were violations of the taboo against Internet voting. The temptation was there, the DoD and state governments did everything they could to tip toe up to the "sinful" act without actually committing it.

For example, in 2004, DoD's Federal Voting Assistance Program enabled overseas military voters to *request* ballots and *receive* blank ballots electronically. But it was not a streamlined process. First the voter had to apply to use the Interim Voting Assistance System (IVAS), and make a request for a ballot. Then FVAP had to check the voter's registration status with the local jurisdiction. If valid, the voter was notified by email. Then the voter would log on to the FVAP website to download and printout the appropriate blank absentee ballot. But after that, the voter had to use traditional mail to send the completed printed ballot back to the local election official.[130]

State participation and laws varied. Some states would accept the return of voted ballots by fax or email. But, of course, military personnel had to be located in areas where fax machines were available. To return the voted ballot via email, the voter had to have a scanner attached to his or her PC, or do the whole thing in an office that had the equipment. To comply with the taboo on using Internet voting, voted ballots would not be accepted via the FVAP website. Just to complicate the process, unlike SERVE, no voter registration could be done electronically from overseas through FVAP. The unregistered voter had to register with his or her jurisdiction through snail mail. FVAP provided a postcard, but no electronic means for voter registration.[131]

Returning voted ballots by traditional mail adds 5 to 10 days to the process. If the ballot arrives past the deadline, it is not counted. If the voter made some error on the ballot, it might be returned for correction. This can happen, for example, when the voter signs his

or her name in some way that varies from the signature on file (such as "W. Jones," rather than "William Jones"). If the soldier moves in the course of his or her service, the returned mail could be delayed and the voter disenfranchised.[132]

Of course, SERVE – the Secure Electronic Registration and Voting Experiment – was designed to reduce the cumbersome process of registering and voting for overseas military from days or weeks down to minutes. Who would have benefited from SERVE? By Election Day, in November of 2004, there were roughly 150,000 combat troops in Iraq.[133] Add to that another 150,000 Americans providing some kind of support to the troops, either logistical or diplomatic, in that war-torn country, and the result is roughly 300,000 eligible US voters in that country. The war in Afghanistan then was still in its infancy, with about a tenth as many Americans of voting age, or roughly 30,000.[134] The 100,000 Americans who had volunteered to vote online in the SERVE project included some of these folks in combat zones.

The needless problems for overseas military voters continued to fester long after SERVE's demise. In 2009, the Pew Center found that more than one-third of states did not provide military voters stationed abroad with enough time to vote.[135] FVAP estimates that of those who requested absentee ballots in 2010, "29 percent of active duty military voters — roughly 120,000 troops — never got their ballots."[136] Only tinkering with various forms of electronic ballot request and ballot return by fax, email, or snail mail has been done to try to contain the spread of the inevitable frustration and disenfranchisement of overseas military voters. The technology is readily available to end this persistent disenfranchisement once for all, but the courage to break the taboo on Internet voting is lacking in the DoD, FVAP, and throughout the entire nation.

In 2009, President Obama signed the Military Overseas Voter Empowerment Act (MOVE). Among other things, MOVE required states to provide absentee ballots to overseas military voters for federal elections at least 45 days before the election would be held.[137] States were also required to provide some form of electronic communication for overseas military voters to use to request and receive an absentee ballot. In compliance with the taboo on Internet voting, voting on a secure website, in the style of SERVE, was not required. Thus, the states were encouraged to tip toe up to the edge of Internet voting, like FVAP, but not to cross over into the forbidden zone. Under this taboo, online registration is allowed, online ballot request is allowed, even online marking of a ballot is allowed, but then the ballot must be printed out for sending by fax or snail mail, or in a growing number of cases, copy and pasted into an email format.

Ever vigilant for deviations from the taboo, the New York Times growls when it sees anyone getting too close to the edge, but it has not condemned the tip toeing like it did SERVE. Commenting on the MOVE Act, a Times editorial warned that allowing the email return of voted ballots is getting too close for comfort to violating the taboo the Times had helped set in place. The first paragraph reads,

> Internet voting is in its infancy, and still far too unreliable, but states are starting to allow it and the trend is accelerating because of a new federal law that requires greater efforts to help military and other overseas voters cast ballots. Men and women

> in uniform must have a fair opportunity to vote, but allowing online voting in its current state *could* open elections up to vote theft and other mischief.

The Times, like other opponents of Internet voting, sometimes stretches the meaning of the term "Internet voting" to include the use of email and fax, so that all the technologies can be criticized with the same charges of insecurity. For example, the Times writes, "Massachusetts recently enacted a law allowing service members to vote by e-mail overseas. According to Verified Voting, a group that works to ensure reliable elections, 16 states allow some form of Internet voting." But the differences in the technology compel the use of the distinct terms. The terms "email and fax voting" have referents that are quite distinct from that of website based "Internet voting." Morse code is sent over telephone lines, but no one calls it talking on the phone.

In the same article, the Times then considers the Rubinesque *possibilities* opened up by the MOVE Act: "E-mail *can* be intercepted, and voting Web sites *can* be hacked or taken down by malicious attacks." Nothing is said, of course, about the fact that none of these things has actually happened in an election using the technology. The Times worries that often "it is not possible to ensure a secret ballot when votes are cast online or by e-mail." But the editors ignore the fact that the same problem exists with the current method of marking paper absentee ballots and returning them by traditional mail.

Disregarding military law enforcement's capability of controlling crime, the newspaper editors warn that voter coercion "is a particular concern for military voting, where soldiers *could* come under pressure from commanding officers about their choice of a candidate." They do not mention that this has not been a problem using paper absentee ballots. While approving of electronic requests for blank ballots, and sending them to voters electronically, the editors remind their readers of where the taboo line is drawn, "Right now, those ballots should not be returned online."[138]

While the Times did not mention the finding made by the judge in the *Schade* case that no misuse of DREs has ever been shown to have occurred in the US, it did give a platform to law professor and anti-e-voting activist John Bonifaz to twist the truth, returning voted ballots by fax or email "basically takes the hazards we've seen with electronic voting [by DREs] and puts them on steroids." Opponents of Internet voting, with a little help from the Times, often deliberately try to stretch the worries Americans have been made to feel about DRE insecurities and fraud to include the return of voted ballots by fax or email. Continuing to conflate the distinct technologies, the Times article declares that the "coming election will be the first in which Internet voting will play a major role, now that 33 states [up from 16 in January] have passed measures to allow their voters to cast ballots over the Internet."[139]

Of course, if the Times does not trust military officers to respect the democratic process, then voting machine vendors are even less trust worthy: "Critics of the new guidelines say they are flawed because they allow voting machine vendors to do some of the performance and security testing themselves." For balance, the Times does quote election officials in three states (Florida and the two Carolinas) that have used email and

fax return of voted ballots without problems. One of them added that "those soldiers are real happy, too, that they don't have to lose their right to vote."

The New York Times holds special favor for Representative Rush Holt (D-NJ), because he introduces bills that require paper records of voted ballots, which "would in effect ban Internet voting." One of his bills in 2009,

> would require paper ballots to be used for every vote cast in November 2010. It would help prod election officials toward the best of the currently available technologies: optical-scan voting. With optical scans, voters fill out a paper ballot that is then read by computer — much like a standardized test. The votes are counted quickly and efficiently by computer, but the paper ballot remains the official vote, which can then be recounted by hand.[140]

The Times does not discuss the error rates or other reliability, or security, issues of optical-scan machines.

The editorial declares, "Electronic voting machines that do not produce a paper record of every vote cast cannot be trusted." But evangelizing for paper based voting technologies is something new for the great newspaper. Paperless lever voting machines were so well liked in the state of New York that they had been in use from the 1890s to 2010. Without objection from the Times, New York City used them for at least a half century. The state only gave them up and purchased DREs when the Department of Justice sued New York for being out of compliance with HAVA.[141]

In 2008, Florida crept the closest of any state to real Internet voting without quite crossing the taboo line. Okaloosa County has several military installations, and over 20,000 active duty service members and dependents registered to vote in the county, many are overseas voters. The County set up a trial program anticipating that about 700 military voters, from Germany, Japan, and the United Kingdom (not Afghanistan or Iraq), would cast their votes online. But the voters still had to go to a polling place on base, and use a dedicated computer in a special kiosk. They could not vote from just anywhere. Using those computers, they would log on to the County's secure website, mark, and send their ballots. Then the computer would print out a record of the vote, without the voter's name or identity, and he or she would check the paper and deposit it in a box.[142]

David Dill, founder of the anti-Internet voting lobbying organization, VerifiedVoting.org criticized the process for not disclosing the "full details of the system."[143] But the harshest criticism came from the New York Times; indeed, the Times wanted to kill the project for being too SERVE-like, and therefore "bad." "Florida's secretary of state should deny Oskaloosa's request [to set up the trial], and Congress should ban Internet voting in federal elections until a reliable and *fully tested* system is developed."[144] Of course, the standard they use, "fully tested," is a neat piece of trickery, because it is unsatisfiable. That is, no matter what test is done, the Times will simply move up its standard of "fully" another notch. Since that standard can never be satisfied, the Times will always have an excuse to condemn Internet voting.

Case in point: The entire Okaloosa County system underwent a lengthy and thorough inspection by an independent team of security experts, led by Alec Yasinsac, Dean of the School of Computer and Information Sciences at the University of South Alabama and co-director of the Security and Assurance in Information Technology Laboratory. They recommended some improvements, and these were made. Then the Florida Bureau of Voting Systems Certification tested the system completely before certifying it. It was studied and approved by the Florida Division of Elections. Testing was continuous. For example, before voting each day the tamper proof seals on the equipment were checked. Also, the integrity of the kiosk voting software was validated each day. Sensitive materials were kept under 24 hour watch.[145]

But this was not "fully" enough for the Times. Also, those editors knew that "a reliable and fully tested system" will never be "developed" if every trial is shot down before it is tried, as the Times would have it.

This Times editorial starts out with an irrelevant and mean slurring of the state's reputation: "The words 'Florida' and 'Internet voting,' taken together, should send a chill down everyone's spine. … Internet voting is fraught with problems, including the *possibility* that a hacker could break in and alter the results."

Upon what evidence does the Times base its claim for this alleged Rubinesque "possibility"? Upon the word of Prof. Rubin himself – "In 2004, a group of academics reviewed an Internet voting system that the Pentagon was considering. The system was scrapped after the group identified numerous security flaws. There was a very real possibility, the professors warned, that the system could be used to steal votes."

Reflecting what seems to be its annoyance at the nation's move towards a paperless economy and culture, the Times continued to present its readers with only one side of this public policy issue. It offered no discussion of the successful use of Internet voting outside the US. The Times does not mention that the four SERVE critics, like David Dill, had never built an Internet voting system, but only condemned such systems from their armchairs, while the experts who have actual experience have demonstrated by their successes that it can be done. Instead, the editors drag out the old Rubinesque "slippery slope" fear producer: "The issue here goes beyond a single county. If the Okaloosa experiment goes forward, other counties around the country may decide to implement their own programs, with just as little public scrutiny and debate."

Even though Okaloosa County did not cross the taboo line, because it came so close the New York Times did its very best to shame and embarrass County officials by name, as well as those in the rest of the state, by painting them as reckless. This is one way of enforcing the taboo across the nation. How many election officials, especially elected officials, want to risk a public scolding from the New York Times?

The efforts of the states to comply with both the MOVE Act and the taboo against Internet voting have had disappointing results. A recent Chapman University study of

how well the email/fax return of voted ballots is working concludes that the "absentee ballot data for 2012 paints a bleak picture for military voters."[146]

A Coup d'état

The perpetrators, and enforcers, of the taboo on Internet voting appear to have successfully executed a coup d'état over the election administration system in the United States. They now control how elections will be conducted; and, it won't be online. The cabal consists of anti-Internet voting lobbying groups like Dill's 501c4 VerifiedVoting.org and the 501c3 Overseas Voting Foundation (or OVF, which specializes in keeping Internet voting out of the military). Whenever a "public outcry" is needed to pressure Congress, or some state legislature, Verified Voting has several power houses waiting on call. These include the Electronic Frontier Foundation (which gave Rubin its Pioneer Award), Moveon.org, and Common Cause. Following their study of how public attitudes towards electronic voting were manipulated, political scientists Hall and Alvarez observe "These organizations were able to shape the debate over electronic voting quite successfully."[147] Of course, the ultimate power of the cabal comes from the New York Times, which can trigger a flood of secondary online and print press with its opinions. Without the support of the Times, those special interest groups would not be able to use fear mongering to counteract the public's desire for more convenient voting. The Times has been the single greatest force for instilling the Internet voting taboo in the minds of the American people and their elected officials.

Natalie E. Tennant: A Profile in Courage

Despite the powerful forces railing against Internet voting, our country has had at least one outstanding profile in courage. In 2008, Natalie E. Tennant was elected Secretary of State in West Virginia.[148] Having a husband who is a career officer in the military, she knew first hand about the problems members of the military have had voting from overseas. Determined to do something about it, Secretary Tennant persuaded the state legislature to approve a true Internet voting trial to include five volunteer counties. Two private companies, Scytl and Everyone Counts, offered their expertise for free, as a demonstration of what can be done. A system not unlike SERVE's was constructed. Overseas military voters could log on to the secure voting website with a PIN and password. Online voting was made available for the 2010 primaries. Overseas military voters could use their own PC, and vote any time during the three day voting period, from anywhere. The process worked so well that Secretary Tennant persuaded the legislature to approve expanding it to several more counties for the general election, which it did.

After the election, Secretary Tennant sent the legislature a reoprt on the project. In the counties where Internet voting was offered, of all the voters who requested that their absentee ballots be delivered electronically, 76% voted on the secure website. In the counties using standard mail as the absentee ballot transmission method, 58% of the requested ballots were returned. As the report observes, there was a higher rate of participation with Internet voting. Also, there were no reports of security breaches or voting fraud. Contrary to the ill-founded worries of the New York Times, there were no reported cases of military brass pressuring soldiers to vote one way or another. Indeed, a

survey showed extremely high voter satisfaction, and many said they would use the system again.

Based on her experience, Secretary Tennant has become an advocate for Internet voting in the USA.[149] However, she has had to pay a price for her courage and advocay. For example, she participated in a panel discussion in which there were several prominant anti-Internet voting activists and she was the only discussant who favored the technology – and, who had actual experience using it. After quite a bit of interrupting, badgering, and being accused by the OVF CEO of using her overseas military voters as "guinea pigs," Secretary Tennant declared in her closing remarks, that if this is what it takes, "I'll continue to sit up here and take the attacks, take the arrows ... and things like that!"[150] Of course, public humiliation for violaters is another means of enforcing the taboo on Internet voting.

Also Rans

In 2009 there were three noteworthy uses of online voting in public elections, but these were less significant than the West Virginia experiment. The New York City School Board conducted one trial. Website voting was open to parents for six days to cast "advisory votes for [unpaid] members of their community education councils." This was not for actual public officials.[151]

The City of Honolulu offered telephone voting and website based voting for its Neighborhood Board Election in May 2009. However, these are also only advisory positions.[152]

Another online voting project was held in 2009 for the Board of Supervisors of the King Conservation District in the State of Washington. While these elections were for paid elected officials, the system of online voting used fell safely short of violating the taboo on Internet voting. Voters had to find their way to voting kiosks distributed across the County, and vote on dedicated lap tops.[153]

The DC Hack

Much ado has been made of the one and only Internet voting system in the world known to have been penetrated by hackers. In 2010, the Washington DC Board of Elections and Ethics contracted to construct an Internet voting system with a nonprofit group that had no experience building such a complex system. Partly to reassure itself that the system would work, the Board held a practice mock election a month before the November election.

The Board publicly invited anyone to test the security of the system. Someone did. University of Michigan computer science professor, Alex Halderman, and a team of graduate students probed the system in every way they could think of. After 36 hours they found a way in. Once in, they discovered all the identities and passwords of registered voters. They found stored passwords for administrators of the system. They used these to access all the approximately 900 votes that had been cast on the system. They changed the votes and wrote in a variety of silly names, like "Bender," a robot

cartoon character. Then they installed the UM football team "fight" song, which played after someone voted. Of course, the penetration alert system failed. None of the responsible administrators noticed the hack, until fans of other teams complained in emails that their school's fight songs were not being played. Since Halderman and his team had taken control of the security cameras in the "secure" room where the server was kept, they were able to see the expressions on the faces of the administrators and security guards after they learned of the deed.[154] The myth of Internet voting insecurity had its most potent reinforcement.

Part III: ASSESSING THE PROSPECTS FOR INTERNET VOTING

Assessing the prospects for Internet voting in the United States requires an examination of the claims made about its security. For, if elites and public believe the technology is unacceptably vulnerable to manipulation and abuse, then its prospects are poor. But this can change if the claims of insecurity are publicly and authoritatively shown to be without intellectual foundation.

We have seen that the fears of insecurity have been aroused in elites and public by methods of opinion manipulation, which have lacked intellectual integrity. But because well respected institutions, such as the New York Times, are leading the campaign against Internet voting, and no equivalent force is opposing it, the prospects for moving to the new technology are, at present, nearly nil. If the prospects for Internet voting are to improve, an institution that can command a degree of respect like that given the Times, must come forth and, using Reason and the Scientific Method, counter the Times's strategy of stimulating unfounded Fear.

The Voice of Science

Article 1, section 8, of the US Constitution enumerates the specific powers of Congress. Among these are: "The Congress shall have power … To regulate Commerce … To coin money … and fix the standard of weights and measures." The Framers had learned from unhappy experiences under the Articles of Confederation that without uniform standards for money, the new nation's economy had little chance of thriving. They had also learned that without uniform "weights and measures," the growth of science and technology, industry, and commerce would be crippled by chaos. Out of its continuing efforts to exercise these powers responsibly, in 1988 Congress created the National Institute of Standards and Technology (NIST), which is currently a non-regulatory agency within the Department of Commerce.

Throughout the history of the US, NIST, and its predecessor agencies, have worked in close collaboration with industry, science, and the military to fulfill its mission. That mission is "to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." Without an agency to perform these functions, the United States might never have become the giant it is in science and industry; indeed, NIST has such a vital role in the progress of science that it can aptly be understood as the voice of science in the USA.[155]

Appreciating the importance of NIST as a research and standard setting institution, and respecting its past accomplishments and the professional competence of its staff of researchers and technicians, when Congress established the Election Assistance Commission (EAC), in the 2002 Help America Vote Act (HAVA), it mandated that the Director of NIST be the Chair of the EAC's Technical Guidelines Development Committee (TGDC).[156] In a display of foresight, Congress also mandated that among the responsibilities of NIST is to provide the EAC technical support on the research and development of, among other things, "remote access voting, including voting through the Internet."[157]

NIST, then, has the authority and power to set straight the New York Times, and all the other purveyors of irrational fear. Only NIST can present itself as having the confidence of the United States Congress to apply the highest standards of the Scientific Method to a particular problem, and to command respect for its pronounced findings. Were the Times to obstinately contradict the scientific findings of NIST, it would risk looking ridiculous, and chance the loss not only of prestige, but of advertisers, subscribers, and readers. Thus, if there is no science behind the Internet voting insecurity scares, as we allege, then NIST is singularly situated to falsify or to verify this claim.

NIST Speaks

NIST has, indeed, spoken on Internet voting; and we will now examine attentively the findings of this honorable Paragon of Science; for, surely, nowhere else will we see the methods of science and the application of Reason so well displayed. The main pronouncements by NIST on Internet voting are found in its 2011 report, "Security Considerations for Remote Electronic UOCAVA Voting" (NIST 7770).[158]

Unhappily, in NIST 7770 the agency has not performed its duties well. Indeed, the agency appears to have been captured by the proponents of the taboo on Internet voting. Although expected to conduct independent scientific research for Congress and the nation, this report reveals little or no research beyond their reading of the infamous SERVE Security Report (SSR). While the EAC, Congress, the states, and the people of the United States look to NIST to be a leader in the field of scientific research, the reality is that, in its election technology division, NIST is a mere sycophant to the leaders of the bloodless coup over our nation's election administration process. NIST 7770 has no scientific content, but mindlessly puppets even the most absurd Rubinesque divinations. An examination of this document will reveal it to be a model of misfeasance.

NIST 7770 advises Congress and the states against the implementation of Internet voting. This advice is based on the report's findings in three principle subject areas.[159] These are:

1. **Software Attacks**

"First, remote electronic absentee voting from personally-owned devices face a variety of potential attacks on voters and voters' personal computers. Since the voter's personal computer is outside the control of election officials, it is extremely difficult to protect

against software attacks that could violate ballot secrecy or integrity or steal a voter's authentication credentials. These are serious threats that are already commonplace on the Internet today."

2. **Voter Authentication**
"Second, remote electronic voter authentication is a difficult problem. Current technology does offer solutions for highly-secure voter authentication methods, but these may be difficult or expensive to deploy. Personally-owned computers may not be able to interface with these methods, such as having the necessary smart card readers for cryptographic authentication using Common Access Cards or Personal Identity Verification cards."

3. **Auditability**
"Third, it is not clear that remote electronic absentee voting systems can offer a comparable level of auditability to polling place systems. Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution."

1. Software Attacks: Voter Education and Responsibility
We will examine each of these points, starting with the first; Software Attacks. Software attacks can occur against the voter's PC or the voting website server. The SSR's primary argument was that because the voter's PC was too vulnerable to malware and spyware, those PCs could not be trusted to be used securely in Internet voting.[160] By putting its focus on PC "software attacks," NIST 7770 is in lock step with the SSR.

But the NIST statement contains an ambiguous phrase, which seems to go well beyond the SSR. The report states, "Since the voter's personal computer is outside the control of election officials, it is extremely difficult to protect …" Does this mean that if the PCs were within the control of election officials, they would be easier to protect? That was the case in Okaloosa County, when overseas military voters went to an office on base and voted on a dedicated lap top computer in a kiosk. But the statement might be hinting at more than what they did in Okaloosa County. It could be read as suggesting that unless the voter's PC is within the control of election officials, Internet voting cannot be trusted.

This could be accomplished, for example, by requiring every voter to submit his or her device to the remote access of the election officials so that they could scan the machine for malware. Of course, if this government intrusion into each PC was made a requirement of law for Internet voting, it would not likely be acceptable to defenders of the secret ballot, or of privacy generally. By setting up a standard that would be an anathema to the public and thus impossible to fulfill, NIST would be guaranteeing the results it appears dedicated to bringing about – preventing the implementation of Internet voting.

Also, a standard that makes election authorities responsible for the security of the voter's PC implicitly rejects the original policy of the Department of Defense and its agency for overseas military voters, the Federal Voting Assistance Program. When DoD's FVAP constructed the SERVE system, they understood the threats to voters, but their policy was to leave the responsibility of maintaining the voter's equipment to the voter. SERVE would be able to protect itself from penetration by malware in the voter's computer. The voter was responsible for protecting his or her machine from malware and spyware that could, in NIST's words, "violate ballot secrecy or integrity or steal a voter's authentication credentials."

But FVAP did not intend to simply leave the voters to the mercies of predators. FVAP planned to actively engage the voters in a program of security education, so that they would know that they needed to protect themselves, and how to do it. Such education could be enough to prevent all, or most, of the common computer crime that opponents of Internet voting worry about. Because they were fully briefed, the four critics of SERVE knew of FVAP's plans for voter education, but they deliberately kept it out of their discussion. The NIST report, like its parent the SSR, also does not consider the role of voter education as a security measure in the Internet voting process.

However, before Wolfowitz's order to shelve SERVE was issued in February 2004, the director of the SERVE project for FVAP, Carol Paquette, responded directly to the charge that the online environment of the voter's PC was too insecure to be trusted for voting online. She explained to Kim Zetter of Wired (a popular print and online magazine), "We absolutely understand that the Internet is insecure." She said of the voters, "If they're using computers at work [however,] in most instances those computers are going to have firewalls and protection [from viruses]." She assured Zetter that, "Election officials will advise home voters to install antivirus software and run a virus check before election day. After all, this is a pretty important thing they're going to be doing, *and the voter also bears some responsibility for the act of voting*."[161]

Paquette's statement, "the voter also bears some responsibility for the act of voting," is not only the policy set by FVAP for the SERVE project, it is a policy followed by the United States, and every state, for as long as we have had the Union. Voters have always been expected to make their own way to the polls, and back home again. Except in the most extraordinary Civil Rights cases, the government has not provided voters either with transport or with a safe escort to and from the polling place. The government does not provide protection against the elements for voters who must wait in long lines. Nor does the government, as mentioned before, accept responsibility for any of the common crimes that can befall a voter. No voting jurisdiction in the US accepts liability for the victims of purse-snatchings when these happen to voters going to and from polling places, or auto theft that happens while the voter is waiting in a long line to vote. Even the act of registering to vote must be performed under the voter's own initiative, and is not done automatically for him or her by the government. The individual voter bears these responsibilities for the act of voting.

To the extent, if any, that NIST's ambiguous phrase is hinting that the government should have the responsibility for the security of the voter's electronic voting device as a condition of allowing Internet voting, then the proposal should be rejected as a tactic for preventing the implementation of Internet voting. Such tactics are tried in other parts of the report, as we will see. NIST presents numerous specious arguments in support of its claims that "it is extremely difficult to protect against software attacks that could violate ballot secrecy or integrity or steal a voter's authentication credentials."

Software Attacks on Secrecy

NIST 7770 notes that, at least in theory, there are two primary categories of attack on voter secrecy; client side and server side. In other words, secrecy can be violated by attacks on the voter's PC or on the voting website server. As to the server side, NIST suggests the reasonable requirement that "Voting systems must protect the confidentiality of sensitive information stored on those systems."[162] The NIST report candidly acknowledges that servers can be made reasonably secure, especially compared to vote by mail systems. "Compared to mail-in voting, remote electronic voting systems have the potential to provide much greater technical controls for maintaining ballot secrecy."[163] While secrecy is protected somewhat in vote by mail systems by using separate envelopes within envelopes, small scale violations by misbehaving election workers are still possible.

But with properly organized online voting systems, server access "control mechanisms and cryptographic technologies can provide strong protections against [server side] attacks on ballot secrecy."[164] Using prudent decryption key management and carefully vetted personnel can protect against insider attacks that could violate vote secrecy and voter identification privacy.[165] The report recognizes that sophisticated servers have the capacity to keep votes and voter identity separate. In other words, Internet voting systems that are constructed by real professionals can be relied upon to protect the vote and voter data stored in the servers. The fatal secrecy problems are far more on the "client side" than on the "server side."

Credential Stealing

The NIST report states hypothetically that "an attacker can potentially steal the victim's authentication credentials (e.g., a password or PIN)."[166] As the authors of this report know, few elected policy-makers or citizens who are concerned about the integrity of elections would support an online voting process if that would enable widespread stealing of voter credentials, and the multiple voting by crooks that would follow. Thus, assessing the prospects for Internet voting in the US depends upon evaluating the likelihood that the alleged threats to the process would actually occur.

While the report asserts in Rubinesque fashion that this crime "can potentially" be done, one of the important facts it omits to mention is that there are *no known instances* of this election crime ever having been committed in any online vote around the world. Lacking such experience, small wonder that the report omits any estimation of the probability that this crime will be attempted; or, if attempted, how likely a wrongdoer would be to

succeed at using the credentials of other voters to cast multiple votes without being detected.

The NIST report is defective, in part, for its numerous omissions. For example, it fails to explain who would want to engage in credential stealing, why it would be done, or how the many practical difficulties could be overcome. It also fails to show how much damage this crime could cause an election. Could an online election outcome be determined by multiple voting resulting from credential stealing, or, assuming it could succeed, would it only be a potential nuisance factor?

We will argue here that there is no reason to believe that the threat of multiple voting by a credential thief, is any greater for an online election than in the current practices of absentee voting, or voting by mail. We will also reflect upon how easily this could be done on a large scale. To put the report's hypothetical propositions in a fuller and more realistic perspective, we will carefully consider the practical details the commission of this crime would have to manage.

We will see throughout this examination of the NIST report that once its Rubinesque "possibilities" are juxtaposed with practicalities, the likelihood of the possibilities is greatly reduced. Indeed, NIST's advice against Internet voting is based entirely upon unrealistic hypotheticals. The report suggests two major methods for stealing voter credentials in an online voting system. These are keylogging and phishing.

Keylogging

As the report says, there are several types of malware that can be installed on a voter's computer. One form of malware installs a keylogging program.[167] Keyloggers send the hacker every key tapped on the user's keyboard. As a voter logs on to the voting website, he or she types in the necessary password and PIN. Then the hacker has it, too.

Keylogging is sometimes used by thieves to steal banking information. With that information, the crook can log on to the bank account any time and execute unauthorized withdrawals. Such banking credentials are re-useable. However, the first practical problem a fraudster faces with keylogging voter information is that under some circumstances he cannot use the information he has collected. During an online election, the key strokes can only be taken while the voter is logging on to vote. If each voter is only allowed to vote once, then by the time the credential thief goes to vote, it will already have been done, and he will be refused ballot access by the website. Keylogging only works in systems that allow multiple uses of the credentials; otherwise, it is useless.

Some countries, such as Estonia and Australia, actually allow a voter to vote multiple times, and the system only counts the last vote. This provides some protection in cases of coercion and vote buying. Perhaps a credential thief could succeed in this type of process by using the credentials to "re-vote." But even here, if the official website has a re-vote challenge question, such as "in what year did you first register to vote," the crook will not have the information he needs to pull off the crime. Also, Australia uses an independent verification website. A voter can log on and see what vote is recorded under his or her

name. If a voter is alerted by email or SMS of a re-vote being recorded, he or she could promptly report the irregularity. Thus, while keylogging "can possibly" be done, the stolen voting credentials would be useless.

Phishing

A second way to steal voter information, discussed in the report, is through phishing.[168] Suppose a spammer sends out thousands of emails during the days in which online voting is being conducted. The email is made to appear to be from some trusted organization, such as the political party the voter is registered with, and states something like this: "Don't forget to vote. Our democracy depends on your participation. For your convenience, click on the link provided here and vote now!" Some gullible and unsuspecting voters will click on the link. Then they will find themselves on a web page that appears official. They enter their password and PIN, and cast a vote. Not only is the vote wasted, but the criminal has the information he needs to vote on the official website multiple times, once for each duped voter. But, while hypothetically it "could" be done, this tactic also has practical problems, which NIST failed to consider.

First, the crook must obtain a list of email addresses. Rather than buy a spammer's list of general email addresses, he will want to buy a list of email addresses for registered voters. Such lists are commercially available and legal to sell.[169] These lists can be tailored to various marketing requirements – voting districts, party membership, age, gender, etc. However, they are not cheap. Political campaign organizations pay several thousand dollars for this information. So, the prudent crook will have to balance the costs of committing this crime against the benefits he might derive from it.

If a crook has a lot of extra money, or wealthy backers, he can buy a custom email list; otherwise, he might have to shop around for a cheaper, and perhaps stolen, list. Shopping around for a cheaper list with the email addresses of registered voters could very well bring him to the attention of the FBI. Law enforcement authorities are well aware of phishing scams, and will be monitoring the sale of voter information carefully around election time. They might set up a sting operation by offering such lists for sale, to catch unwary crooks. A patriotic employee of a company that sells voter information might report a suspicious customer to authorities. However, whether making a legal or an illicit purchase, the cost of such a list will be a deterrent to most people who are thinking about phishing as a way to steal voter credentials. (Probably, the costs of conducting a phishing scam will eliminate most teenagers.) As we will see, those with the money will also be deterred, because the return on the investment is very poor, and the risk of being caught is very high.

Multiple Voting in a Local Election

To illustrate what NIST should have done to make a rational threat assessment, we will conduct a thought experiment. Suppose an online election in Los Angeles County is being held over a three day period, so that every one in the county will have time to vote. In this case, credential stealing could pay off because the crook has time to use the voter credentials.

Suppose that thousands of dollars is no obstacle for this crook, and that he obtains a list of emails for all the 4.6 million registered voters in LA County. His plan would be to make up a fake website that looked like the official one being used for voting in that jurisdiction. He will send out his trick email praising democracy, and giving a link for the voter's convenience. When duped people click on the link, and log on to the website, they will give him their PIN and password, and then waste their vote. Then he will use this information to impersonate voters and cast multiple votes. With this scheme, keylogging will not be necessary. But this crime is easier to speculate about than to commit in practice.

The villain will not know what the official website looks like until it goes online just hours before the voting is to begin. He will have to work fast to duplicate it. Another difficulty is that in LA County different precincts have different candidates for different offices, and different issues. For example, the LA County Board of Supervisors has five Supervisorial Districts; there are 18 Congressional Districts, and 88 cities.[170] When a voter logs on to the official website, it will know the voter's precinct and present an appropriate ballot. Our fraudster will not have time to set up so sophisticated a site, so he will have to use a more generic look-alike. A generic site would surely arouse suspicion among some experienced voters. To paraphrase Lincoln, you can only fool some of the people some of the time. Just one call or email to the authorities would be enough to end the scam.

Despite the risks, suppose that on the first day of voting the crook scrambles madly to construct his generic website and post it online. Once that is done, he sends out his 4.6 million emails. However, LA County will have a voter education program running in print in newspapers, and on billboards and buses, on TV and radio, and online. That publicity will state that the voter should never trust an email with a link to the County voting website, no matter what the source, and that the County will never send voters such an email. An email address for reporting suspicious activity to the FBI will also be provided.

In practice, then, many of the crook's trick emails will be disregarded or deleted by voters who paid attention to the County's voter education publicity. More importantly, not just one, but perhaps scores of voters will alert the authorities to the scam, many by simply forwarding the trick email to the FBI. Those officials will have the server hosting the fake website shut down within minutes of learning about it. The crook will have thrown away thousands of dollars on the list he bought, and the authorities will have enough evidence to track him down. The overwhelming odds of detection and capture are enough to stop any sane potential bad guy from attempting this foolhardy crime.

Nevertheless, let us pretend, as the NIST report would have us do, that this crook is somehow able to dodge the authorities. Imagine that by the end of the first day of voting he has suckered 10,000 voters to give him their PINs and passwords. Now what will he do?

Bars to Automated Multiple Voting

During the next two voting days he will work furiously to log on and vote as many times as possible. Although the cheater has all these sets of credentials, automated multiple voting is unlikely to succeed. It can easily be prevented by placing a simple security question on the voting web page, such as "how much is 2+2, or 3+9, etc." The challenge problem can be chosen at random by the server, so that it is unpredictable for each voter who logs on. Alternatively, a few letters randomly selected by the server, and scrambled so that malware cannot read them but are readable to humans, can be placed on the web page, and voters instructed to type them into a box. Voters can answer the question, or retype the letters, but not an automated program.

Another problem for the imposter voter using multiple voter identities is that the LA County official voting website server will likely be programmed to detect multiple votes coming from the same computer, or IP address. It can then present a challenge question, such as "in what year did you first register to vote," or "what is your current address." The crook will have to take the time consuming task of checking his voter registration list for that information, provided he paid to have such information included on the list. The more time he spends on log in, the less time he has to cast multiple votes.

Hypothetically, if all goes well, working alone, how many fraudulent votes could he cast in two days? To cast 1000 fraudulent votes in two days, he would have to log on and vote about 21 times per hour. But that would require, on average, nearly three votes per minute, which is not humanly possible. At one vote every five minutes, he could cast 12 votes per hour. Working without stop for two days, he "could" cast 576 fraudulent votes. If he had accomplices he could cast more votes.

What damage could he cause? The trickster would have limited control over which LA County candidates or issues he could vote on. Because he cannot select or control or predict who will be duped by his fake website, he can only vote in those elections for which he has randomly obtained the voter credentials. His tricks might or might not fool enough voters to give him a controlling number in closes races. All his expenses and risk taking could result in his having no influence on any close elections.

The only candidates that would be on all the LA County ballots would be those for a presidential or gubernatorial election. If there are state-wide initiatives or referenda to vote on, these would also be on every ballot. Otherwise, he would have a smattering or potpourri of randomly appearing propositions and local, state, and congressional races to vote on.

Thus, in this thought experiment, the very best a crook could do is cast a measly few hundred votes in a presidential or gubernatorial election. If one guy working furiously without stop for two days could cast 576 fraudulent votes, then five guys working furiously for two days might be able to vote 2880 times. Giving them a lot of generous assumptions, hypothetically, they "could" provide the winning margin for some congressional races or ballot measures, and an extraordinarily close gubernatorial election. But in a presidential contest, that is still an insignificant number when the total vote exceeds 130,000,000, and the winning margin, as in 2012, is over four million votes.

Since this crook cannot control which congressional or local elections he can vote in, but must accept randomly given opportunities, he might or might not be able to swing one of these elections.

How many rational persons would pay the costs, and incur the risks of fines and imprisonment, for such uncertain opportunities? And, why would any sensible person do this? Would any malware writer or website maker take pay to go on such a suicide mission? The NIST report does not answer these questions; indeed, it does not even ask them.

Even if Fortuna favored the bad guys, using electronic technology in the LA County election would not have enabled them to cast as many fraudulent votes as, for example, the organized effort did in the Miami mayoral election of 1997. There, a group of candidate enthusiasts, among other things, stole absentee ballots from mail boxes, and cast about 5000 votes. Their candidate won. But the scheme was immediately detected, and within four months the crooks were convicted, jailed, the bad votes subtracted from the total by court order, and the election set right.[171]

The fraudsters in the LA County example would need a gang of 8 to 10 operatives to cast as many fraudulent votes as were cast in Miami. But, the same rule of criminology would apply in this hypothetical as elsewhere; that is, the more members of a conspiracy there are, the more likely they are to be detected. Once detected, all the fraudulent votes and PINs of the victims will be on the computers of the crooks. A court can either order those votes deducted from the totals, as was done in Miami, or subtract the bad votes and let the victims cast their votes anew.

The report concludes its section on credential stealing by claiming that "it is difficult to estimate the likelihood of such attacks or how motivated potentials attackers would be to conduct these types of attacks."[172] No it's not. It's not difficult, if one bothers to think it through. While *possible* in an unselfcritical imagination, realistically the crimes of keylogging and of phishing for voter authentication credentials are highly unlikely to be attempted, and if attempted, nearly impossible to pull off without early detection by alert law enforcement. Such considerations as high risk and uncertainty of reward would dampen the motivation of any rational potential hacker. As to scale, the damage they can do to an election is no worse than existing threats to elections using paper mail-in ballots.

Therefore, the threat of these crimes is no reason to forego the convenience to voters and election administration as well as the enhancements to democracy that online voting systems offer. NIST has failed to fulfill its fiduciary duty to Congress and the American people by not fully analyzing the practicalities of carrying out the threat of voter authentication credential theft before presenting it as a reason to discourage the implementation of Internet voting.

Complex Thought Experiments

The practicalities of executing some types of election crimes in an online election can be extremely complex, and require a very high degree of technical sophistication. There are

numerous contingencies involved. But these practicalities must be considered if estimates of the likelihood of the crimes being successfully committed are to have any intellectual bases. Without this sort of exercise, the execution of the crimes could appear to naïve and unthinking persons to be as easy as writing the names of the crimes.

Ballot Integrity

NIST states correctly that a vote loses its "integrity" if it is "modified by unauthorized parties."[173] Also, as we have seen, the SERVE Security Report alleges that hackers can "change votes," and listed "vote switching" as among the types of attack that "could succeed and yet go completely undetected."[174] Seeming to take its marching orders from the SSR, the NIST report states that hackers "can potentially … even change the victim's vote without the victim noticing."[175] And later,

> Ensuring the security of personally-owned computers remains a very serious open issue. At this time, there is relatively little jurisdictions can do to ensure that voters' computers are free from malware capable of changing ballots cast from those machines. Attackers have demonstrated an ability to infect large numbers of machines with malicious software.[176]

We have already addressed the false and misleading statement that "there is relatively little jurisdictions can do to ensure that voters' computers are free from malware." Voter education around election time can do very much to reduce the number of infected computers. As to the phrase "large numbers," elsewhere the report provides a slightly more specific statement of what that might realistically be. It cites estimates that up to 15% of computers around the world are infected with some sort of malware.[177] That, of course, implies that 85% are uninfected.

If there were 130,000,000 voters in an online presidential election, and 15% of their computers were infected with malware, that would be 19,500,000 infected machines. If such an election can turn on four or five million votes, then maybe there is good reason for alarm. It would be terrible, indeed, if millions of votes in a presidential election, for example, could be changed on the machines of voters, "without the victim [or election officials] noticing." This hypothetical threat, of itself, would be enough to stop any prudent member of Congress, or other person, from agreeing to implement an Internet voting system – that is, so long as the scary story was not critically examined. We will do that now. What would it take to pull off this crime? How easy is it to infect in mass the computers of voters with vote changing malware? Also, once infected, how likely is it that their votes can be changed in mass so as to affect election outcomes? Can that be done without anyone, like the voter or law enforcement authorities, noticing?

First, this crime is not easy to commit. Writing vote changing malware requires a high degree of technical skill and training. Such programs cannot be written simply by typing in "change all votes for Obama to votes for Romney." This code writing is far more complex than that. The malware not only must hide its operation from the voter, it must trick the voting server into accepting its vote as that of the voter who has logged on to the official website.

So long as the ballot being used has uniform positioning for candidates and issues, the vote changing program can work automatically in the infected computers. However, there are other challenges the program must be able to overcome. For example, different jurisdictions have different offices to be filled and different issues to be voted on. So the vote changing program would have to be tailored to the voter's specific jurisdiction. Not only that, but in the interest of fairness, jurisdictions routinely shuffle candidate and issue positions on their ballots. They do this because the first place on ballots is slightly favored by voters, and "voting fatigue" sometimes results in voters disregarding candidates and issues at the end of the lists.

To work automatically on each voter's computer, then, the vote changing program would have to be sophisticated enough to "read" the individual voter's particular ballot. This means the malware would have to interpret all the incoming data to the computer and identify when a ballot was being presented and then intercept the voters returning data and change it to suit the malware writer. Suppose the voter votes for 'X,' but the bad guys want 'Y.' The bad guys intercept the 'X,' and send 'Y' to the server. If the website has a voter verification function, as SERVE had, then the malware will have to intercept the message "You have voted for Y," and change it to appear "You have voted for X." The voter will be fooled, and click 'send.' While extremely complex, writing a program that can do all of this is not impossible.

Although an important fact to consider in the current public policy discourse, the NIST report fails to mention that to date there are *no* documented cases of vote changing malware ever changing even one vote in any online election in the world. Nor does the report give any consideration to the practicalities of executing this type of attack. It does not offer any assessment as to the likelihood of such an attack occurring in any kind of US election, and does not try to estimate the actual damages that such an attack could cause, if attempted. The Rubinesque assertion of what "could" be done – votes changed in mass without voter or official knowing – can be read as implying that this is highly likely to be done with ease in any kind of election; local, state, or federal. We will show below why that implication is false, and that this type of attack is extremely difficult to carry out successfully, has a very uncertain pay off, and is thus highly unlikely to even be attempted by people with rational minds.

We agree that vote changing malware can be written and widely disseminated in a bot network. A botnet is a collection of computers under the control of one operator. An unlawful botnet can be aggregated by a bot master who tricks PC owners into letting his malware into their computer. This can be done when people download freebies or visit websites that have the malware in them. Botnets can consist of tens of thousands of machines. But the larger they are, the more likely it is that law enforcement agencies will be able to track down the crooks.[178] Assuming that botnets with vote changing malware are possible, we will consider the practicalities of two scenarios: one in which criminal conspirators want to change the votes in an election in a single jurisdiction; and, the other in which the crooks want to swing a presidential election their way.

A Single Voting Jurisdiction

Suppose the voting website for Los Angeles County goes online at 10 pm on Monday. Voting will begin at midnight, and continue through Tuesday, Wednesday, and end at midnight on Thursday. (An extended voting period is common practice with online voting. To keep the complexity to a minimum, we will assume that no re-voting is allowed in this example.) Without insider information, or prior access to a demo site or a previous implementation, the botnet master and his gang will not know what the official website looks like until 10 pm on Monday, and will not be able to try it out, to see how it communicates with voters, until after midnight. In order to get the changed vote accepted on the website, adjustments in the vote changing program might be required before it is installed into the slave computers. During this time, voting will already have begun.

Of course, this malware program could only be effective on those machines which were used for voting *after* the malware was installed. Obviously, the malware could not be effective on those machines that were used for voting before it was installed. So the opportunity to change the votes of the earliest voters will be lost.

Suppose these crooks want to increase the number of Republican winners of congressional districts on the ballot for LA County voters. To succeed, the plot will require sophisticated preparation and planning. It cannot be done by just anybody.

Currently, only three seats of the 18 districts to be voted on are held by Republicans.[179] So, how would clever crooks plan their attack? First, they will have to determine which of the remaining15 districts have a chance at being winnable by a Republican.

In 2012, Democrats won two districts by more than 70% of the vote. They won four other districts by 35% or more. If, as the NIST report says, only 15% of computers on average are infected by malware, then that number suggests the probable success the crooks will have at building up their botnets in the three LA County precincts. Indeed, 85% of the computers in the targeted districts might not be infected. Assuming the crooks could control 15% of the votes in a given district, they still could not win in these very safe districts. Clearly, political realities limit what vote changers can do. Few crooks, with their reason in tact, would risk fines and prison to attack safe districts, which they have no chance of changing. They would have to focus on closer contests.

Republicans lost by 30% or less in three LA County races in 2012. They lost by 4% in the 26th district, and by 26% in the 27th district. They lost in the 32d district by 30%. Suppose, then, that the vote changers reckon that with luck they have a fighting chance at cheating successfully in these three districts, if they can lower the Democrat's vote total by 15%, and raise the Republican's total by that amount.

In a perfect world, for them, they could make the margin of victory in the three targeted districts just large enough so as not to arouse the suspicion of pollsters or seasoned observers. But since the earliest votes have already been cast, the bad guys will not know what the voting trends are. They won't be able to fine tune their votes, but will have to

make all their slaves in the three districts vote for the Republican candidate for Congress. The uncertainty here is that this move could result in unexpected lopsided victories, no victory, or the ideal of a close victory.

Suppose that there are 300,000 registered voters in each of the three districts. The bot herders in the gang will have done all they could to build up their herd. They will have purchased email lists divided by districts, so they can focus their trick emails on the three particular districts. But they still have to work within severe constraints. They cannot force folks to take their bait.

Also, amidst the campaigning and election related publicity, County officials will have conducted a public education campaign. So along with other political information, the attentive public will learn about phishing, trick websites, untrustworthy freebies online, and the need to have professional security services scan their computers for malware before voting.

In some of the three congressional districts the voter education program will have been more effective than in others. That is, if on average 15% of machines are infected, then perhaps only 5% or 10% will be infected in one or two districts, while 25% or more are infected in another district. Whether the needed number of voters is fooled by the bot herder's ruses is a matter of chance, and luck. Just as you can lead a horse to water, but not make him drink, so spammers can try to entice email recipients to click on a link, or download their malware, but they cannot make them do it. The bad guys will have no control over which districts will have the requisite number of infected machines to assure victory for the Republicans. These contingencies render botnets an unreliable tool for election fraud.

Yet another contingency is that if the margin of victory is so far beyond what seasoned observers had predicted or expected, then the election's integrity will be cast in doubt. For example, if the vote changing in the 26th district gives the Republican a 25% margin of victory, when the experts were predicting a narrow win for the Democrat, protests will surely follow. The US Constitution, Article 1, section 5 states that "Each House shall be the judge of the elections, returns and qualifications of its own members." If the fraud is so obvious that local experts would protest, Congress might not accept the "winner." In that case, all the efforts, expenses, and risks taken by the crooks would be for naught.

In addition, the cheaters will have to reckon what their chances are of being caught. Of course, such an underhanded endeavor as vote changing cannot be undertaken risk free. The FBI will be on high alert for election fraud during the election. Botnet activity can be observed, and herders are often caught and prosecuted. In the course of tricking voters into going on websites loaded with malware, or luring them to download free videos, etc., containing malware, the FBI might be alerted for a variety of reasons. Security companies might be asked by customers to scan suspicious websites for malware, or the companies may notice their customers are being infected by one source, and the company alert the FBI. Anyone on the Internet can alert the FBI to suspicious activity. Thus, the FBI or other law enforcement agencies could investigate the bad guys, and arrest them

before they change any votes; or, wait until they do change some votes and arrest them for the more serious charges. Crooks never know when they are being observed, or about to be arrested. Even if the crooks are off shore, their servers can be shut down.

Finally, besides disregarding all the practicalities involved in committing this crime, the NIST report fails to ask why anyone with the skill and intelligence needed to launch this particular form of attack would do so. Would they do it as a prank, just for fun? How likely is it that a few technicians with professional level programming skills would take on such a task, with all the risks they would incur to their freedom and fortune, for their own amusement? On a scale of one to ten, ten being the most likely, would the likelihood of them doing this as entertainment rate a zero, or a .5? Clearly, there would have to be some other motive. Since no one enjoys any immediate gain from winning an election, except the candidate and his party, there would be no immediate gain for the crooks. How likely is it that non-candidate tricksters would be policy wonks, or party zealots, willing to risk everything just to see a like-minded candidate win? Would this possibility rate as much as a 1 or a 2?

If they did it for *money*, then the crooked computer technicians would receive an immediate reward for their efforts and risks. But who would pay them? If they were paid to target the three congressional elections, how likely is it that the three Republican candidates would conspire and pool their funds to pay the programming experts? Would even one candidate take such a risk? Would local party elites? Whoever pays them, there would have to be some shopping around to find corrupt yet highly skilled programmers and bot herders. What are the odds that the FBI would learn of such shopping around? Could that likelihood be between 8 and 10 on our scale? The FBI might even set up a sting operation for morally challenged candidates to get trapped in. Knowing of the risks involved, and having their rational faculties intact, how many candidates are likely to attempt such a crime? Probably no more than do in the current polling place process; which is very few.[180]

The price for such vote changing services would be very high. The more operatives involved, the higher the price. The more races to be won, the more money the programmers will demand. Even if there was only one technical expert, would he agree to win one seat for one Republican candidate for one million dollars? Or, three seats for three million? While there are plenty of candidates who can afford such a fee, how would the payment be made – half now, half after the victory? What if there was no victory? Would the programmer refund the money? How many sensible Republicans would make so risky an investment?

We have presented an abbreviated analysis of the myriad of practicalities involved in carrying out a vote changing scheme in just one jurisdiction. Considering the difficulty of the technical challenges of writing the program and adapting it to a county Internet voting server, only a few highly skilled technicians could do the work involved. Finding such talent that is also willing to conspire to commit numerous federal felonies would not be easy, and would itself be very risky. Why would any skilled technician engage in such a risky enterprise, and which is so uncertain of success? Raising the funds to pay such

criminal characters could be problematic, and risky. Of course, the more conspirators there are in a criminal conspiracy, the more likely it is to be detected. So a conspiracy to change three congressional elections in LA County is not only highly unlikely to happen, but if it did, its detection would be highly likely. The same would be true of any county.

The persons at NIST who were responsible for presenting the idea of a vote changing attack as if it were inevitable, and likely to go undetected, in an election based on Internet voting appear to base their claim on a Rubinesque divination, rather than upon any science or experience. That same divination can be seen in the SERVE Security Report. The four SERVE slayers imagined the breath taking fantasy that, "Such attacks [as 'vote switching'] could occur on a large-scale, and could be launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law … even to the extent of reversing the outcome of many elections at once, including the presidential election."[181] Since these mentors of the NIST writers mention a presidential election as being under imminent threat in an online election, we will do what NIST avoided doing, and test that hypothesis in a thought experiment.

A Presidential Election

If the difficulties of winning a congressional election by unlawful vote changing are formidable in the limited context of LA County, how hard would it be to swing a presidential election that way? Aping the four SERVE critics, the NIST report assures Congress and the American people that "Attackers have demonstrated an ability to infect large numbers of machines with … malware capable of changing ballots cast from those machines."[182] While no record of such an event is cited, presumably, such a "large number of machines" would be enough to sway a presidential election. Regrettably, however, while omitting to mention that there are no known cases of this attack ever having been done, the report also shirks its responsibility to discuss any realistic scenario of how this could be done. Why avoid that discussion? Perhaps because the NIST report writers know that no such scenario can pass the laugh test. Let us reflect on some realities.

To win a presidential election, one of the candidates must take at least 270 of the 535 electoral votes available. While there are over 4000 voting jurisdictions in the US,[183] the crooks know that they will not have to control the computers used by voters in all of those places. Indeed, most states are relatively safe for one or the other political party. Coastal states are likely to give their electoral votes to the Democratic Party, while the Republicans can usually count on receiving the electoral votes of several Midwestern and Southern states. As campaign managers know, the outcome of the contest will be determined by a few battleground, or swing, states.

Suppose that a presidential election is so close that whoever wins just four swing states can win the race. Let us say that Florida, with 29 electoral votes, Ohio, with 18, North Carolina, with 15, and Virginia, with 13 are at issue. Because these are winner-take-all states, the bad guys will just want to change enough votes to win each state's electoral votes.

Of course, online elections would not be conducted monolithically in any US state. The administration of elections is usually divided up among counties, or boroughs, parishes, townships, and independent cities. Many of these political units would have their own website hosting servers, and all would format their own ballots. In Florida there are 67 counties. Ohio has 88 counties. North Carolina has 100 counties. And, The Commonwealth of Virginia is divided into 95 counties and 39 independent cities. The crooks who want to control a presidential election have a lot of work cut out for them.

Suppose further that there are six or seven major companies that provide Internet voting services, and that each has various models of online voting servers. Within each state, there will be a variety of products and services among the political units. These wrongdoers will have to be prepared to adapt their vote changing malware to every different server model there is on the market.

As prudent crooks, they will want to focus on just the number of the most winnable counties in each state needed to secure the necessary electoral votes. So as not to waste their resources and efforts, they will need to know which of the 389 political units are so one-sided for one party that even with a vote changing operation, there is no way they could change enough votes to win. But since there are so many voting jurisdictions to consider, how will the criminals know which ones they are going to be the most likely to succeed in?

Perhaps they had better try to recruit a political scientist or two to advise them of the major swing counties in each of the swing states. Of course, shopping for corrupt political scientists might be even more difficult and risky for the crooks than shopping for corrupt computer scientists was for them in LA County. Just one report to the FBI by an honest political scientist could result in all the conspirators paying lawyer fees, fines, and losing freedom.

At this point in our analysis of the practicalities, it seems that to swing a presidential election there will have to be quite a crowd of co-conspirators involved. Besides political advisors, the bad guys will need a highly skilled malware programmer for each county they need to win. If they decide to attack just 10 select counties in each of the four states, then they will need 40 top notch malware writers to adapt that program to the particular server being used.

Barbara Simons's much publicized frightening vision of a lone hacker in Iran controlling the outcome of a US presidential election seems somewhat off the mark when the political realities are brought into consideration. Even if the Iranian crook were to assemble the team he needs to succeed, how could he do so and still fly under the radar of the FBI, the Department of Homeland Security, and the CIA?

As in the example of LA County, each of the malware writers will have to wait until voting begins to see how the server for that county communicates with voters as they log on, vote, and verify their vote. They will not have to hack the server, but just quickly adapt their malware program to the server in use. All the contingencies that applied in

the attack on LA County will apply to each of the 40 attacks required to swing a presidential election.

To build their bot herd, the attackers will have to buy lists of the email addresses for all the registered voters in the 40 counties. While selling such lists is legal, buying them could raise suspicions. The crooks will be praying that the companies selling the lists don't have patriots in them who would report their suspicions to authorities.

Whatever the odds are that the FBI would get wind of the conspiracy in LA County can be multiplied by at least 40 in the case of a presidential election. In other words, all the conspirators would understand that the enterprise upon which they are embarking will be 40 times as risky as was the vote changing project in LA County. The world might not have that many qualified technicians who were also so reckless and foolish.

How could the search for such recruits be conducted in secret? Every person who was offered a part in this plot, even if he turned it down, would risk later arrest as a co-conspirator who abetted the crime, unless he or she immediately informed the authorities of the offer. Co-conspirators who aid and abet a crime by not reporting it risk the same punishments as those who actually commit the crime. The old rule of criminal investigation applies here; that is, the more conspirators there are, the higher are the chances of being detected, caught, prosecuted, imprisoned, etc.

Now, as to the costs: whether forty million dollars, or fifty, or even one hundred million dollars, political campaigns often spend far more than that on presidential elections. But to estimate the likelihood of this crime being attempted, the point is not how much money is needed, but rather how could people who are such talented and worldly entrepreneurs, as to be able to raise amounts like that, be so foolhardy as to do it for so high risk a crime with such an uncertain outcome? Unless one's theory of human nature is based on a Batman movie, the combination of entrepreneurial talent and foolishness required for this crime seem contrary to human nature.

The NIST report fails to speculate as to who in the real world would attempt such a suicidal crime. Would the governments of Russia or China? Would a Mafia organization in one of those countries, or in the US, try it? If detected, the US would surely retaliate with severely damaging economic sanctions. It could insist that every one of its allies stop doing business with the offending nations. All trade with those countries, and all travel to and from them, and even communication, could be halted.

What could a rouge nation gain from such a high risk crime if they succeeded? Would they do it to have a Republican Party foreign policy rather than a Democratic one? Are the risks worth that? Surely, only a government gone as mad as Hitler's Third Reich in the 1930s would even consider such a crime. What could a Mafia hope to gain? Would a presidential candidate promise to call off the Department of Justice Organized Crime Unit if the Mafia wins his election for him? A president who tried that would enrage the nation, and be impeached in a minute by Congress. He might even be tried for treason.

Why would a terrorist group like Al Qaeda try it? Would they join forces with Iran to try and elect a Muslim president? Could that *really* be done "without detection"? Would Americans sit happily on their couches praising the wonders of democracy as a newly elected Ayatollah harangues them on Inauguration Day? Barbara Simons seems to think so. Should the Untied States of America forego the enhancements to our democracy offered by online voting, out of the fear that an Iranian band of religious extremists might try to change some votes?

As we have shown here, the chances of successfully controlling a presidential election are slim for any would-be vote changing attacker. While NIST researchers are paid from US taxes to do their own thinking and scientific research, this NIST report seems to be based more on memos from Avi Rubin and Barbara Simons. No public policy discourse can produce an outcome beneficial to the political system based on this kind of mindless input. Congress and the political science profession, both of which understand the needs of the political system better than any other groups, have extended NIST an unwarranted excess of deference by allowing the NIST 7770 to stand unchallenged. If the demand was made of NIST that it do better than this – surely it could.

2. Voter Authentication

Among its reasons for rejecting Internet voting is that "remote electronic voter authentication is a difficult problem." There are two major reasons for this problem. One is the condition of voter registration records. Currently, the states are converting their paper based records into digital form.

Section 303 of the 2002 Help America Vote Act (HAVA) requires that each state have a centralized electronic Statewide Voter Registration System.[184] This computerized list will contain the name and registration information of every legally registered voter in the state and assign a unique identifier to each legally registered voter in the state. This voter information must be cross checked with the records in the state's Department of Motor Vehicles, and all other record keeping state agencies, such as the welfare department, the department of corrections, agencies that keep vital records, and with the national Social Security Administration. Once this task has been completed, Internet voting servers will be able to instantly check a voter's registration status in the relevant state data base, and the results will be reliable.

The second problem is that it is difficult to know if a person who logs on to vote is really the voter he claims to be. Voter authentication credentials can be lost, stolen, bought or sold, or a voter can be under coercion, and the system server will not be able to know this. But this is a law enforcement problem in every form of election. We have argued above (see Credential Stealing passim) that there is no reason to believe that the threat of multiple voting by a credential thief, is any greater for an online election than in the current practices of absentee voting, or voting by mail. We also showed why the large scale use of stolen credentials is very difficult. Each use requires a time consuming log on, and protections exist against automated voting.

Large scale selling of credentials, like large scale coercion, is an unlikely threat. The more publicly visible the commission of a crime is, the more likely it is to be detected and stopped. Online offers to sell or buy would be spotted instantly by law enforcement. The large scale use of bought credentials is as impractical as it is for stolen credentials. Large scale coercion is not a realistic threat. Suppose the boss, or pastor, demands that all his employees or parishioners vote in his office, so he can see they are voting "right." Everyone is a witness to the crime, and the more victims there are, the more likely it is that one or more will alert authorities. Internet voting does not exacerbate the likelihood or the scale of these possible election crimes beyond that of current vote by mail systems.

3. **Auditability**

The four critics of SERVE wrote, in the SSR, that, DREs "have been widely criticized because they are essentially unauditable. First, there is no way that a voter can verify that the vote recorded inside the machine is the same as the vote that he or she entered and saw displayed on the machine's touch screen." And, "there is no independent audit trail of the votes."[185] Their demand for a voter verified paper audit trail (VVPAT), of course, led to the shelving of SERVE, and generally dooms Internet voting. If the online voter's device printed a VVPAT, it could not be deemed official, since anyone could print out anything at any time, and no one would know if it was the actual vote recorded in the website server. If the web server printed out a vote, no voter would be there to verify it. Ergo; the VVPAT requirement kills Internet voting.

On cue, the NIST report concludes with this discouraging observation (as we quoted above):

> it is not clear that remote electronic absentee voting systems can offer a comparable level of auditability to polling place systems. Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution.[186]

Our examination of these points will show their weaknesses.

NIST 7770 sets up the auditability of "polling place systems" as its standard of excellence. However, lacking thoroughness, if not intellectual honesty, the report says nothing about the known problems of auditing those systems in actual practice. Consider some examples.

Using a paper audit trail, such terms as "hanging chads," "pregnant chads," and merely "dimpled chads" were made known during the well publicized audit of the 2000 vote in Florida. Several audits of the paper ballots were required to settle the disputed Minnesota senatorial election held in November 2008. On first count of 2.9 million votes, incumbent Norm Coleman lost to challenger Al Franken by just over 200 votes. A costly and time consuming recount of the paper audit trail brought that up to 225 as of April, 2009. But Coleman found uncounted votes, and sued for a complete recount. Among the uncounted there were over 12,000 absentee ballots that had been rejected for little errors like a slight change in a signature. These had to be re-examined by the lawyers to determine which

votes were properly rejected. They found 351 that had been wrongly rejected. But this re-recount did not help Coleman. Instead, it boosted Al Franken's lead by 87 votes, to a grand total of 312 ahead. Finally, Franken was declared the winner on June 30, 2009 – more than six months after the election, and at the cost of hundreds of thousand of dollars.[187]

The problems of auditing votes on millions of pieces of paper can also include boxes of lost, misplaced, or stolen ballots. Errors in counting, made by bleary eyed clerks, are inevitable, too. Inefficiencies like those in Minnesota and Florida seem to illustrate that auditing paper based systems of voting leave something to be desired. The NIST report is remiss in not explaining why those systems are to be preferred to the well known rapid and accurate electronic counting technology, which has been tried and proven over many years of e-commerce.

The report's conception of "auditability" includes "validating and verifying software on remote electronic voting system servers *and personal computers*." Because these tasks are "difficult," the report gives them as reasons to forego the implementation of Internet voting. But by including "personal computers" as a component of the online voting system to be audited, the report makes another *sub rosa* attempt to doom Internet voting. This ruse assumes that the government is responsible for auditing the integrity of the software on the voter's equipment. NIST's own integrity is questionable for failing to defend this novel theory of election official responsibility. We explained above why we reject that theory as an unneeded government intrusion.

NIST is also disingenuous by claiming, in absolute terms, that there are "no current or proposed technologies offering a viable solution" to the problem of "validating and verifying software on … servers." Independent Testing Agencies (ITAs) can validate that the software on a server is what it is supposed to be by using "mathematical proofs" to test a system's algorithms. This is widely done commercially, and is regularly done by states prior to certifying DREs. It can be done for Internet voting system servers as well. But NIST gives a very flimsy and specious excuse for dismissing this well known technology: "Because of its considerable *cost*, formal verification of software or designs is likely not well-suited to mitigating risks of software defects or vulnerabilities in remote electronic voting systems."[188] Thus, when the report definitively states there is "no … viable solution," to the problem, it really means there is none within what it considers to be an affordable price range for the states. Hence, "cost," not capability, make "formal verification of software … likely not well-suited" to testing the software in online voting servers. But suppose states pooled resources, or Congress allocated testing funds through the EAC? Would that make such testing better "suited"?

Trust

The report also defines "auditability" as the capacity of a system to "provide evidence to auditors that the system functioned in the way it was supposed to. … In addition, the voting system and its supporting election procedures must provide assurances that the evidence provided by the system is trustworthy."[189] The word "trustworthy" is at the heart of the auditability problem. While server technology can be tested for integrity and

proper operation, the fundamental issue is whether the humans who are responsible for constructing and operating the online voting system can be trusted to do so honestly and competently.

Indeed, exercising such judgment is precisely what an elected official is elected to do. Our Constitution establishes a system of representative government. Thus, at least in some measure, that document assumes that citizens will trust their representatives to execute their duties with honesty and competence. Frequent and regular elections, plus the powers of impeachment, are ways for the citizenry to remove officials who violate that public trust. But without some measure of trust, representative government would not be possible.

To put a human face on this political theorizing, in 2011, West Virginia Secretary of State, Natalie Tennant, was invited to participate on a panel, which, as we mentioned above, turned out to be very one-sided. She was the only defender of Internet voting, while there were several high profile anti-Internet voting activists on the other side. The issues of trust and official responsibility soon came up. When a panelist demanded to know how her office vetted the companies that provided her state's Internet voting service, she replied that the vendors had to agree to several conditions. One of these was that third party experts be allowed to inspect the equipment and operating codes the vendors used. She said the companies not only agreed to these conditions, but offered to do the whole job for free, as a demonstration project. Given that situation, the Secretary decided not to exercise the right to bring in a third party inspector. She said she trusted the companies.

Another panelist insisted that the vendors could be corrupt and she wouldn't know it. She replied that election officials have to exercise their professional judgment as to when such trust is reasonable. When pressed by the moderator about possible insider wrongdoing as well as software rigging, Ms. Tennant stated that she trusted the workers in her department because it was like a small community in which everyone knew each other. She trusted the system because it used military grade encryption, had an intrusion detection function, and other security checks. She also pointed out that it was a serious felony to tamper with elections, and this law is a part of the security system.[190]

In a large and complex political system like the US, if election officials could not be trusted to carry out their responsibilities well, public elections would risk descending into anarchy, and the entire political order fall into ruin. Imagine the chaos if mobs of "election integrity" enthusiasts demanded to observe and perhaps photograph or film all voters, the voted ballots, and the officials as they sorted through high piles of paper trying to tally the vote. At least since the discovery of agriculture, the division of labor has made modern civilization possible. Having some trust in the other fellow to do his part has made the division of labor possible; for, if everyone felt that he or she could not depend on anyone else, nothing would get done, and humanity would have to live, like primates, as foragers. As Secretary Tennant understood, the formula for Internet voting success, then, is to combine the ancient, and Constitutional, principle of reasonable trust

in other people with 21st Century technology. From that, the further advancement of democracy will follow.

Conclusion

Article One, section 4, of the US Constitution states, in part, "The times, places, and manner of holding elections … shall be prescribed in each state by the legislature thereof." Thus, EAC guidelines for voting technology are voluntary. Every state is free to write its own legislation establishing website based Internet voting for both its overseas and domestic voters. However, as long as the existing irrational taboo on Internet voting is being enforced by strong armed extremists, there is little chance that any state will go it alone. But there is one institution in this country that can expose the irrational bases of that taboo, and thus free the states to choose 21st Century technology without fear of public relations reprisals. If only the election technology division of NIST would fulfill its duties as responsibly as have the other departments of that distinguished agency, the prospects for Internet voting in the USA would be excellent.

[1] Edison was issued U. S. Patent 90,646 on 1 June 1869. Rutgers University http://edison.rutgers.edu/vote.htm

[2] One mention of this idea can be found in, *No More Secondhand God: And Other Writings* R. Buckminster Fuller Southern Illinois University Press. April 1, 1967.

[3] Chu, David S. C. "Expanding the Use of Electronic Voting Technology for UOCAVA Citizens." Federal Voting Assistance Program. May 2007 www.fvap.gov/resources/media/ivas2007.pdf (hereinafter "Chu") page 25. At the time, Chu was the Under Secretary of Defense for Personnel and Readiness.

[4] See http://en.wikipedia.org/wiki/Electronic_voting_in_Canada

[5] "A Threat Analysis on UOCAVA Voting Systems." www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf page 4 (hereinafter "NIST 7551"); Cf. "DoD to Test Online Absentee Voting" by Paul Stone http://www.defenselink.mil/news/newsarticle.aspx?id=42801

[6] Election Assistance Commission "A Survey of Internet Voting" http://www.eac.gov/testing_and_certification/eacs_work_with_military_and_overseas_voting.aspx (hereinafter "EAC"), page 13. The EAC credits the Reform Party with offering online balloting in its 1996 presidential primary, but gives no other information. One announcement made before the Party's convention claimed that the Reform Party's "1.3 million … members will submit their votes for the Reform Party's presidential nominee by computer linkups, telephone, or the U.S. mail." But reports of what actually happened could not be readily found. http://archives.obs-us.com/obs/english/books/yellow/food/reformp1_00.htm

[7] EAC, page 14.

[8] EAC, page 15.

[9] NIST 7551, page 4 f. n21.

[10] NIST 7551, page 4.

[11] EAC, page 34; NIST 7551, page 5.

[12] EAC, page 38.

[13] "Voting Over the Internet Pilot Project Assessment Report." Federal Voting Assistance Program 2001 www.fvap.gov/resources/media/voi.pdf The following paragraph cites page numbers from section four of the Assessment.

[14] Chu, page 11.

[15] Chu, pages 10-11. RE: the similar security measures taken for the 2000 online primary vote in Arizona; see Mohen, Joe and Glidden, Julia. (2001) "The Case for Internet Voting," *Communications of the ACM*, 44:1, pp72-85. Made available to me from one of the authors at: http://www.21cconsultancy.com.

[16] See http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107EEmu4A:e876932

[17] EAC, page 29.

[18] EAC, page 30.

[19] EAC, pages 15-16.

[20] EAC, page 30.

[21] EAC, page 29-30.

[22] EAC, pages 30-31.

[23] EAC, pages 31-32.

[24] EAC, page 32.

[25] Chu, page 12.

[26] EAC, page 30.

[27] EAC, page 32.

[28] For more on SPRG see R. Michael Alvarez and Thad E. Hall, *Electronic Elections.* 2008 Princeton University Press, New Jersey, page 83 passim.

[29] Gillmor, Dan. "Paperless E-voting is a Threat." Computer World. February 9, 2004, "Four members of a team looking into the Internet voting idea became so alarmed at the prospect that they jumped the scheduling gun and issued an early report of their own." http://www.computerworld.com/s/article/89910/Paperless_E_voting_Is_a_Threat
This information probably came from Glenn Flood, DoD/FVAP spokesperson. But Rubin claims that "the FVAP agreed to our terms … to issue an independent report … to the public," page 164, "as a condition of

our [the four] joining the group," page 173. Rubin, Aviel. *Brave New Ballot.* 2006 Morgan Road, New York.

[30] Schwartz, John. "Report Says Internet Voting System Is Too Insecure to Use." New York Times. January 21, 2004 (emphasis added). http://www.nytimes.com/2004/01/21/technology/23CND-INTE.html

[31] Garamone, Jim. "Pentagon Decides Against Internet Voting This Year." February 6, 2004. American Forces Press Service. http://www.defense.gov/news/newsarticle.aspx?id=27362

[32] Schwartz, John. "Online Voting Canceled for Americans Overseas." New York Times. February 6, 2004. http://www.nytimes.com/2004/02/06/us/the-2004-campaign-voting-online-ballots-canceled-for-americans-overseas.html

[33] Actually entitled "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," January 21, 2004; Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, Dr. David Wagner http://www.servesecurityreport.org/paper.pdf (hereinafter, "SSR").

[34] SSR, pages 2, 4, 20 emphasis added.

[35] SSR, page 3.

[36] SSR, pages 2 and 20 emphasis added.

[37] SSR, page 14 emphasis added.

[38] SSR, page 2.

[39] SSR, page 2 emphasis added.

[40] SSR, page 2.

[41] SSR page 16 emphasis added.

[42] Popper, Karl. Conjecture and Refutation.

[43] See, http://www.lasvegasweekly.com/news/2012/dec/20/end-night-history-false-armageddons/

[44] SSR, pages 3 and 21.

[45] SSR, pages 3 and 21 emphasis added.

[46] SSR, pages 3 and 21.

[47] SSR, pages 3 and 21.

[48] SSR, pages 3 and 21.

[49] This argument is reminiscent of the US Electoral College. In 2000, for example, Gore won the popular vote, but Bush won the Electoral College vote and became president. (Although transparent, does that make the Electoral College a kind of virus?)

[50] SSR, page 31 emphasis added.

[51] SSR, page 14.

[52] SSR, page 16.

[53] RE: the FBI Elections Division, see http://www.fbi.gov/about-us/investigate/corruption/election-crimes

[54] SSR, page 31.

[55] SSR, page 14.

[56] SSR, page 19.

[57] Chu, ibid, page 12.

[58] SSR, page 19.

[59] SSR, page 19 emphasis added.

[60] SSR, page 19.

[61] SSR, page 20 emphasis added.

[62] SSR, page 20.

[63] SSR, page 18.

[64] Zitter, Kim. "Risky E-Vote System to Expand." Wired. January 26, 2004. "It took Election.com only 45 minutes to fix the problem…" http://www.wired.com/politics/security/news/2004/01/62041?currentPage=all

[65] See Munson, James. "NDP cyber attack a warning to stay away from Internet voting." April 14, 2012 http://www.ipolitics.ca/2012/04/14/ndp-cyber-attack-a-warning-to-stay-away-from-internet-voting-expert/

[66] Elections Canada has petitioned Parliament to allow the agency to make Internet voting available for national elections. EC Official Reports are available on-line at www.elections.ca

[67] EAC, page 40; Cf. Scytl report: "It was one of the most complicated Internet elections ever carried out: 230,749 students from 21 different universities were able to cast votes for 376 simultaneous elections with over 100 parties and 2411 candidates." No attack of any kind was mentioned in this report.

http://www.scytl.com/scytls-technology-successfully-used-in-the-first-binding-internet-election-in-austria/index.html. Also the EAC Survey lists "Projects not included in the Report," at page 13. Here are two factual items missing that favor Internet voting: 1) Gujarat, the largest state in India, held that nation's first election offering Internet voting as an option in 2011. Election officials reported that there were no known security breaches or other problems, and that "we fended off 4,000 attempted hackings from Pakistan, Taiwan and even China." Thus, professionals can conduct successful Internet voting operations even in the most hostile of environments. Ajay, Lakshmi. "Gujarat became the first Indian state to experiment with e-voting this April." Business Standard. July 23, 2011 http://www.business-standard.com/india/news/e-voting-for-it-land/443583/. 2) Based on past successes, the Parliament in Norway decided to continue Internet Voting in 2013. See http://internetvotingforall.blogspot.com/2012/12/norway-to-continue-internet-voting-in.html

[68] See Schwartz, note 30, and SSR, page 7.

[69] SSR, page 7.

[70] SSR, page 12.

[71] Sanger, David et al. "Chinese Army Unit Is Seen as Tied to Hacking Against U.S." The New York Times. February 18, 2013 http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html?_r=1& Google sought to increase its profits by going into the Chinese market. As a condition, they allowed Chinese engineers to censor searches on democracy and religion. Meanwhile, the engineers were sending all they knew to two Chinese universities, which reversed engineered Google's email security codes. That was not a cold hack, but poetic justice.

[72] New York Times, ibid, February 6, 2004.

[73] Hall and Alvarez, ibid, 2008, page 84f.

[74] Garamone, Jim. "Pentagon Decides Against Internet Voting This Year." American Forces Press Service February 6, 2004. http://www.defense.gov/news/newsarticle.aspx?id=27362

[75] See note 30

[76] Rubin, Avi. *Brave New Ballot*. Morgan Road Books, NY. 2006

[77] See http://ballotpedia.org/wiki/index.php/Help_America_Vote_Act

[78] Rubin Ibid, page 41.

[79] Ibid, page 28.

[80] Ibid, page 28.

[81] Ibid, page 45.

[82] Ibid, page 45.

[83] Ibid, page 45.

[84] Ibid, page 30.

[85] Ibid, page 41.

[86] Ibid, page 41.

[87] Ibid, page 41.

[88] Ibid, page 107. His wife said he "seemed more excited about being on The Daily Show than about getting tenure," page 234.

[89] Ibid, page 104.

[90] Ibid, page 46.

[91] Ibid, page 156.

[92] Ibid, page 156 emphasis added.

[93] Ibid, page 42.

[94] Ibid, page 42.

[95] SCHADE vs. LAMONE. Opinion available in pdf from Michael Shamos at euro.ecom.cmu.edu/people/faculty/mshamos/schade.pdf

[96] Ibid, page 6.

[97] Ibid, page 7.

[98] Ibid, page 7.

[99] Ibid, page 3.

[100] Ibid, page 7; September 2004, no date for the day available.

[101] Rubin, ibid, page 160.

[102] Ibid, page 158.

[103] Ibid, page 158.
[104] Ibid, page 149.
[105] Ibid, page 267. The National Science Foundation seems to have been in harmony with that opinion, because Rubin happily reports that in 2005 his foundation was "funded to the tune of $7.5 million," page 246.
[106] Zetter, Kim. "Risky E-Vote System to Expand," Wired. January 26, 2004. http://www.wired.com/politics/security/news/2004/01/62041?currentPage=all
[107] SSR, ibid, pages 2 and 20.
[108] Hall and Alvarez, ibid, 2008, page 83.
[109] Rubin, ibid, page 165.
[110] Ibid, page 165.
[111] Ibid, page 170.
[112] Ibid, page 170.
[113] Ibid, page 171.
[114] Ibid, page 170.
[115] Ibid, page 171.
[116] Keating, Dan. "Pentagon's Online Voting Program Deemed Too Risky." Washington Post. January 22, 2004. Archived at http://www.votersunite.org/article.asp?id=1061
[117] CNN.com. "Federal remote voting system called flawed" Thursday, January 22, 2004 http://www.cnn.com/2004/TECH/01/21/internet.voting/index.html
[118] Vijayan, Jaikumar. "Panel members find security flaws in Internet voting system." Computer World. January 22, 2004. http://www.computerworld.com/s/article/89290/Panel_members_find_security_flaws_in_Internet_voting_system?taxonomyId=17&pageNumber=1
According to its website, CW receives "over 3 million unique monthly visitors," http://www.computerworld.com/s/pages/about
[119]"The Perils of Online Voting." New York Times. January 23, 2004. http://www.nytimes.com/2004/01/23/opinion/23FRI1.html
[120] Rubin, ibid, page 175.
[121] Schwartz, John. "Who Hacked the Voting System? The Teacher." New York Times. May 3, 2004 http://www.nytimes.com/2004/05/03/technology/03vote.html
[122] NBC News. "Pentagon cancels Internet voting test - Too many concerns about ballot security, official says" May 17, 2004 http://www.nbcnews.com/id/4184803
[123] Weiss, Todd. "Pentagon Drops Web Voting Plans for Military Personnel." Computer World. February 9, 2004 http://www.computerworld.com/s/article/89950/Pentagon_Drops_Web_Voting_Plans_for_Military_Personnel brackets in original.
[124] The use of Internet voting has had more acceptance in the private sector than it has in the public sector. While there were just three uses of the voting technology in 2000 (Republicans in Alaska, Democrats in Arizona, and the VOI – the only true government use), a January 2000 article in Forbes said that Votation.com claims to have already conducted some 600 elections for clients such as the Sierra Club, the Pennsylvania State Employees Credit Union and the California Bar. Einstein, David. "Internet voting: A touchy issue." January 10, 2000 http://www.forbes.com/2000/01/10/feat.html. There has been little formal study of Internet voting in the private sector.
[125] Dismissing the critics of Internet voters as outliers, only a few months before the New York Times published the claims made in the SSR, Alvarez and Hall declared "Everyone knows that an Internet voting system can be built." *Point, Click, and Vote: The Future of Internet Voting.* Thad Hall and R. Michael Alvarez. Brookings Institute, Washington, D.C. 2004, page 146.
[126] See Hall and Alvarez, ibid, 2008, page 92, turnout page 93. Cf. EAC, ibid, pages 22-23.
[127] Ibid, page 97.
[128] Ibid, page 97.
[129] Ibid, page 97.
[130] NIST 7551, ibid, page 6.
[131] Ibid, page 9.

[132] Ibid, page 9.
[133] See the New York Times, http://www.nytimes.com/2005/01/07/international/middleeast/07military.html
[134] See Strips.com http://www.stripes.com/news/u-s-troop-presence-in-afghanistan-at-17-900-and-expected-to-hold-steady-1.21700 7-9-04
[135] "No Time to Vote." The Pew Center http://www.pewcenteronthestates.org/uploadedFiles/NTTV_Report_Web.pdf
[136] Serbu, Jared. "DoD personnel miss out on absentee ballots." Federal News Radio October 28, 2011. http://www.federalnewsradio.com/?nid=239&sid=2610686
[137] See http://ballotpedia.org/wiki/index.php/Military_and_Overseas_Voter_Empowerment_(MOVE)_Act
[138] "Internet Voting, Still in Beta." The New York Times. January 28, 2010 http://www.nytimes.com/2010/01/28/opinion/28thu4.html emphases added.
[139] Urbina, Ian. "States Move to Allow Overseas and Military Voters to Cast Ballots by Internet." The New York Times. May 7, 2010 http://www.nytimes.com/2010/05/09/us/politics/09voting.html
[140] "How to Trust Electronic Voting." The New York Times. June 21, 2009 http://www.nytimes.com/2009/06/22/opinion/22mon2.html
[141] Chen, David. "City Finally Poised to Give Up Lever Voting Machines." The New York Times. January 4, 2010 http://www.nytimes.com/2010/01/04/nyregion/04machines.html
[142] EAC, ibid, page 23.
[143] Sofge, Erik. "Internet Voting in Florida Raises Security Concerns: Geek the Vote." Popular Mechanics. October 22, 2008 http://www.popularmechanics.com/technology/industry/4288327.html]
[144] "A Bad Experiment in Voting." New York Times. September 5, 2008 http://www.nytimes.com/2008/09/05/opinion/05fri2.html
[145] Sofge, ibid; and, EAC, ibid, pages 23-27. And cf. Carol Paquette, "Response to New York Times Editorial." When Ms. Paquette spoke with the Times editor, he demanded to know why Avi Rubin wasn't on the inspection committee. She said he was invited but declined the invitation. http://www.operationbravo.org/Response%20to%20NYT%20Editorial%20Opinion.pdf
[146] Chapman University. "Military Voting Update: A Bleak Picture in 2012." August 27, 2012 PDF available at, http://mvpproject.org/. This apparent failure of the MOVE Act could be another lesson, like slavery and prohibition, that when irrational thinking is the dominant input into the policy making process, bad law is the inevitable output.
[147] Hall and Alvarez, 2008; see Chapter four, Moveon.org and quote from page 70. RE: Common Cause, see http://internetvotingforall.blogspot.com/2012/08/common-cause-caught-using-junk-science.html. Verified Voting is well funded, and intends to stay that way. It was awarded a $300,000 grant from the MacArthur Foundation on April 19, 2012. http://philanthropy.com/article/article-content/131598/. It appears that the money was used wisely: Hasen, Rick. "Verified Voting Hires Lobbying Powerhouse Patton Boggs." http://electionlawblog.org/?p=38991. Henry, Captain Chas U.S. Marine Corps (Retired) "Lots of Bullets, Not Enough Ballots." US Navel Institute. July 2008. The Overseas Voting Foundation received "a $100,000 grant from the Pew Center for the States." http://www.usni.org/magazines/proceedings/story.asp?STORY_ID=1525. And, cf. https://www.overseasvotefoundation.org/alliances-sponsors-and-supporters.
[148] The discussion about Secretary Tennant comes from the West Virginia Secretary of State website at http://www.sos.wv.gov; and http://internetvotingforall.blogspot.com/2011/08/natalie-e-tennant-internet-voting.html; http://internetvotingforall.blogspot.com/2011/11/cyber-bullying-in-connecticut.html; and, http://internetvotingforall.blogspot.com/2012/02/news-hour-internet-voting-story.html. Also see EAC, ibid, page 32f.
[149] See Tennant, Natalie E. "Making the Case for Online Voting." Government Technology. June 29, 2012 http://www.govtech.com/e-government/Making-the-Case-for-Online-Voting.html
[150] See http://internetvotingforall.blogspot.com/2011/11/cyber-bullying-in-connecticut.html. After the private contractors requested a fee for their services, in 2012 the state legislature declined to renew West Virginia's Internet voting program. Reports stated the decision was due to budgetary consraints.
[151] Roberts, Sam. "Parent Voting for School Councils Is Moving Online." The New York Times. March 15, 2009 http://www.nytimes.com/2009/03/15/nyregion/15voting.html

[152] EAC, ibid, page 21; and, http://www.dkosopedia.com/wiki/City_and_County_of_Honolulu_Neighborhood_Board_System
[153] See http://www.scytl.com/eng/news.php
[154] Pictures and full report by the UM hackers at http://www.washingtonpost.com/blogs/mike-debonis/post/dc-vote-hackers-publish-their-vote-hacking-exploits/2012/03/06/gIQArbG4uR_blog.html. Putting his new fame to good use, Professor Halderman went on a mission to India to spread his anti-e-voting gospel. But authorities wisely detained him at the airport, and held his plane while they did the paperwork for deportation. He narrowly avoided deportation by wilily promising to stay in India for tourism only and not for propaganda, or "educational," purposes. Williams, Kaitlin. "U prof. nearly deported from India for research on electronic voting." The Michigan Daily. January 17, 2011 http://tmd.pub.umich.edu/content/university-assistant-professor-nearly-deported-india-research-flaws-indian-electronic-voting
[155] See the National Institute of Standards and Technology website at http://www.nist.gov
[156] HAVA PDF available at http://www.eac.gov/about_the_eac/help_america_vote_act.aspx. TGDC at Section 221f.]
[157] Congress displayed a very clear understanding of the potential of the Internet for enhancing democracy in the US. As to Internet voting, Section 245 required NIST (as the research arm of the EAC) to
(1) … conduct a thorough study of issues and challenges, specifically to include the potential for [online] election fraud, in the Federal, State, and local electoral process.
(2) [Other research to include:]
(A) the appropriate security measures required and minimum standards for certification;
(B) the possible methods … to register voters and enable citizens to vote online, and recommendations concerning statutes and rules to be adopted in order to implement an online or Internet system in the electoral process;
(C) the impact … Internet technology … could have on voter participation rates, voter education, public accessibility, potential external influences during the elections process, voter privacy and anonymity, and other issues related to the conduct and administration of elections;
(D) whether … public availability of candidate information and citizen communication with candidates, could benefit from the increased use of online or Internet technologies;
(F) the implementation cost of an online or Internet voting or voter registration system;
(I) the impact of technology on the speed, timeliness, and accuracy of vote counts in Federal, State, and local elections.
[158] "Security Considerations for Remote Electronic UOCAVA Voting," available at http://www.nist.gov/itl/vote/nistir-7770.cfm (Hereinafter NIST 7770)
[159] Listed in NIST 7770, ibid, at page 59. Another outrage that both the SSR and NIST 7770 warn of, and which will shock the democratic conscience in members of Congress, and of the various state legislatures, is the potential for online "vote swapping." First stated in the SSR, at pages 10-11, and repeated, of course, in NIST 7770, at page 18.
[160] SSR, ibid, "The vulnerabilities we describe … are fundamental in the architecture of the Internet and of the PC hardware and software that is ubiquitous today. They cannot all be eliminated for the foreseeable future without some unforeseen radical breakthrough. It is quite possible that they will not be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet," pages 2-3
[161] "Risky E-Vote System to Expand," Kim Zetter, Wired 01-26-04 http://www.wired.com/politics/security/news/2004/01/62041?currentPage=all emphasis added.
[162] NIST 7770, ibid, page 12.
[163] Ibid, page 14.
[164] Ibid, page 14.
[165] Ibid, page 17.
[166] Ibid, page 29.
[167] Ibid, pages 52-53.
[168] Ibid, 50f.
[169] For example, Aristotle, Inc has a "nationwide voter file of over 165 million registered voters," http://www.aristotle.com/
[170] See http://lacounty.gov

[171] "Vote Fraud in Florida." http://ballotpedia.org/wiki/index.php/Vote_fraud_in_Florida
[172] NIST 7770, ibid, page 51.
[173] Ibid, page 23.
[174] SSR, ibid, pages 2, 13, 20.
[175] NIST 7770, ibid, page 29.
[176] Ibid, page 37.
[177] Ibid, page 19.
[178] Search "botnets" at www.fbi.gov; also see http://blog.fireeye.com/research/2012/06/stories-about-botnets-part-1.html
[179] This discussion draws its factual data from, Statement of Vote, November 6, 2012, General Election, California Secretary of State Debra Bowen, www.sos.ca.gov/elections/sov/2012-general/
[180] To see how little election fraud there actually is in the US, search "election fraud" at The Brennan Center for Justice at http://www.brennancenter.org/; and see Hall and Alvarez (eds), *Election Fraud*, Brookings Institute, NY 2008
[181] SSR, ibid, pages 2 and 20.
[182] NIST 7770, ibid, page 37.
[183] The EAC estimates that there could be up "to 10,000 depending on the how the reporting unit is defined. [It had] a jurisdictional count of 4,678 in 2010." See http://www.eac.gov/research/election_administration_and_voting_survey_faqs.aspx
[184] See note 154, and http://ballotpedia.org/wiki/index.php/Help_America_Vote_Act#SVRS-Statewide_Voter_Registration_System.
[185] SSR, ibid, page 9.
[186] See note 157.
[187] "Court Rules Franken has Won." The New York Times. June 30, 2009 http://thecaucus.blogs.nytimes.com/2009/06/30/court-rules-franken-has-won-senate-seat/?scp=3&sq=Al%20Franken%20wins&st=Search; more at http://www.nytimes.com/2009/01/20/us/politics/20minnesota.html?_r=1&fta=y
[188] NIST 7770, ibid, page 34.
[189] Ibid, page 24.
[190] See http://internetvotingforall.blogspot.com/2011/11/cyber-bullying-in-connecticut.html

NISTIR 7770

Security Considerations for Remote Electronic UOCAVA Voting

Nelson Hastings
Rene Peralta
Stefan Popoveniuc
Andrew Regenscheid

National Institute of Standards and Technology
U.S. Department of Commerce

[This page intentionally left blank.]

NISTIR 7770

Security Considerations for Remote Electronic UOCAVA Voting

Nelson Hastings
Rene Peralta
Stefan Popoveniuc
Andrew Regenscheid
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2011

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

[This page intentionally left blank.]

This document has been prepared by the National Institute of Standards and Technology (NIST) and describes research in support military and overseas voting for the Election Assistance Commission and the Technical Guidelines Development Committee. It does not represent a consensus view or recommendation from NIST, nor does it represent any policy positions of NIST.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by organizations even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, organizations may wish to closely follow the development of these new publications by NIST.

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 PURPOSE AND SCOPE 2
1.2 INTENDED AUDIENCE 2
1.3 ORGANIZATION 2

2 GENERAL ARCHITECTURE 4

2.1 SYSTEM COMPONENTS 4
2.2 AUTHORIZED USERS 7
2.3 THREAT SOURCES 8

3 OVERVIEW 12

4 CONFIDENTIALITY 14

4.1 POTENTIAL BENEFITS 14
4.2 PROPERTIES 15
4.3 THREATS TO CONFIDENTIALITY 17
4.4 CURRENT AND EMERGING TECHNICAL APPROACHES 19
4.5 OPEN ISSUES 22

5 INTEGRITY 23

5.1 POTENTIAL BENEFITS 23
5.2 PROPERTIES 23
5.3 THREATS TO INTEGRITY 27
5.4 CURRENT AND EMERGING TECHNICAL APPROACHES 30
5.5 OPEN ISSUES 37

6 AVAILABILITY 38

6.1 POTENTIAL BENEFITS 38
6.2 PROPERTIES 39
6.3 THREATS TO AVAILABILITY 40
6.4 CURRENT AND EMERGING TECHNICAL APPROACHES 42
6.5 OPEN ISSUES 45

7 IDENTIFICATION AND AUTHENTICATION 46

7.1 POTENTIAL BENEFITS 46
7.2 PROPERTIES 47
7.3 THREATS TO IDENTIFICATION AND AUTHENTICATION 49
7.4 CURRENT AND EMERGING TECHNICAL APPROACHES 53
7.5 OPEN ISSUES 57

8 CONCLUSIONS 59

REFERENCES 60

This page intentionally left blank.]

1 Introduction

The Election Assistance Commission (EAC) requested that the National Institute of Standards and Technology (NIST) research technologies to improve uniformed and overseas United States citizens' ability to vote, as required by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) [1]. Additionally, the Help America Vote Act of 2002 (HAVA) requires the Technical Guidelines Development Committee, with technical support from NIST, to study remote access voting, including voting over the Internet [2]. This report contains the results of NIST's research into threats and security technologies related to remote electronic voting for overseas and military voters.

In December 2008, NIST released NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems* [3], which documents the threats to UOCAVA voting systems using electronic technologies for all aspects of overseas and military voting. NISTIR 7551 considered the use of postal mail, telephone, fax, electronic mail, and web servers to facilitate transmission of voter registration materials, blank ballots, and cast ballots. It documented threats and potential high-level mitigating security controls associated with each of these methods. The report concluded that threats to the electronic transmission of voter registration materials and blank ballots can be mitigated with the use of procedures and widely deployed security technologies. However, the threats associated with electronic transmission, notably Internet-based transmission, of cast ballots are more serious and challenging to overcome and the report suggested that emerging trends and developments in that area should continue to be studied and monitored.

While NISTIR 7551 looked at a variety of technologies for all aspects of the UOCAVA voting process, this report takes a deeper look specifically at the issues associated with remote electronic voting over the Internet. It identifies and defines desirable security properties of remote electronic voting systems and major threats faced by these systems that could violate those security properties. It also discusses the current technologies that could be used to mitigate some of those threats and open issues that may still need to be addressed.

In August of 2010, the EAC posted their *UOCAVA Pilot Program Testing Requirements* document [6]. This document defines requirements for remote electronic voting systems using a supervised-kiosk architecture that is intended for use in a UOCAVA pilot program. However, this report considers all remote electronic voting systems, with particular attention to the threats and technologies for remote voting from personally owned and operated devices. Depending on how it is used, the supervised kiosk model mitigates

many of the threats identified in this document, particularly those related to software integrity, coercion, vote-selling, and voter identification and authentication.

1.1 Purpose and Scope

On April 26, 2010, the EAC submitted their *Report to Congress on EAC's efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems* [7], detailing a roadmap intended to be used by the EAC, NIST, and the Federal Voting Assistance Program (FVAP) to create and implement guidelines for remote electronic absentee voting systems for overseas and military voters. The initial phase of this roadmap calls for a report describing security issues related to remote electronic absentee voting system for UOCAVA voters. This report, along with NIST's initial report on threats to UOCAVA voting systems, NISTIR 7551, *A Threat Analysis on UOCAVA Voting Systems* [3], is intended to meet this need.

This document is part of a series of documents that address the UOCAVA voting. In addition to NISTIR 7551, NIST has released drafts of NISTIR 7682, *Information Systems Security Best Practices for UOCAVA-Supporting Systems* [4] and NISTIR 7711 *Security Best Practices for the Electronic Transmission of UOCAVA Election Materials* [5]. In addition to NIST's research on security issues associated with remote electronic UOCAVA voting, NIST is also researching usability and accessibility topics. A report documenting this research, *Accessibility and Usability Considerations for Remote Electronic UOCAVA Voting,* will be released in early 2011.

1.2 Intended Audience

This document is intended for election officials, technologists, advocacy groups, UOCAVA voting system vendors, and other members of the elections community that will be working with the EAC, NIST, and the FVAP on improving the UOCAVA voting process with the use of electronic technologies. While this document assumes familiarity of the UOCAVA voting process and a high-level understanding of information system security technologies, it is intended to be accessible to a wide audience.

1.3 Organization

The remainder of this report is organized as follows:

- **Section 2** provides a high-level description of the remote electronic voting system architectures that are analyzed in the remaining sections this document. The primary architecture considered is remote voting over the Internet from personally-owned devices.
- **Section 3** provides an overview of the structure for the sections containing the subtopics: Confidentiality, Integrity, Availability, and

Identification and Authentication. Each subtopic contains a discussion of the potential benefits, properties, threats, current and emerging technical approaches and open issues.

- **Section 4** discusses issues related to confidentiality of remote electronic voting systems. Confidentiality refers to the concept of ballot secrecy, and also to protecting sensitive voter information and system data from unauthorized disclosure. This section discusses desirable properties of remote voting systems to deal with confidentiality issues, threats, and possible mitigating technologies.
- **Section 5** discusses issues related to integrity of remote voting systems. This includes data integrity, aimed at safeguarding important election records, including cast ballots and audit logs, as well as software integrity. It describes desirable properties of systems intended to support data and software integrity and identifies threats and possible technical approaches for dealing with these issues.
- **Section 6** describes properties, threats and technologies related to availability of voting systems. Availability refers to the ability of the system to be ready for use when needed by voters and election officials in the face of malicious and incidental threats.
- **Section 7** discusses issues related to the identification and authentication of voters, system operators, election officials, and system components. It identifies threats to the authentication process and discusses various technical methods for authenticating users and components.
- **Section 8** summarizes the important findings report.

2 General Architecture

The following section provides an architectural view of remote voting systems in order to provide a reference from which to discuss security considerations presented in the rest of the document.

2.1 System Components

The general architecture of electronic remote voting systems, as shown in Figure1, is composed of several different components. The following subsections detail the components that may be found in an electronic remote voting system.

2.1.1 Voters' Platforms

Figure 1 shows three different platforms that may be used by a voter to request, receive, and cast their ballot: personal computers, public computers, and kiosks.

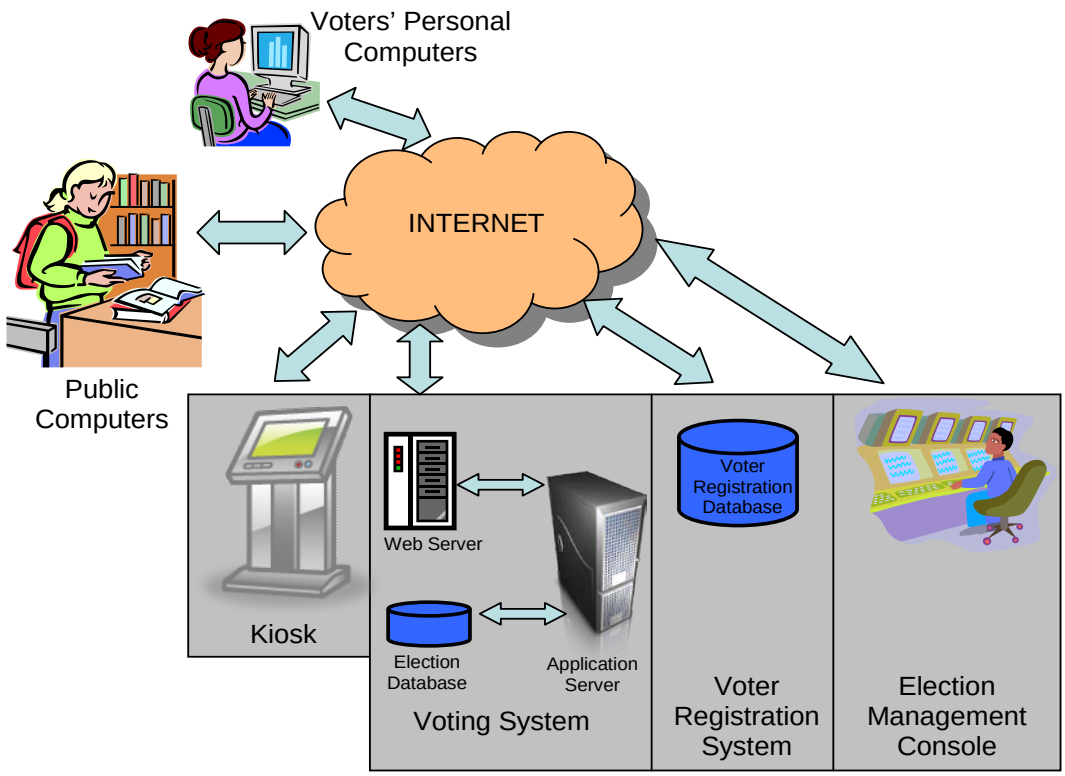


Figure 1- General Architecture for Remote Electronic Voting

Personal computers refer to general purpose computing systems a voter may have at home for their personal use, including desktop and laptop computers, tablets, and smart phones. Voters may also use general purpose computer systems found at public locations such as libraries, schools, and Internet cafes and are referred to as public computers. Finally, voters may use dedicated devices called kiosks that may or may not be under the control and supervision of poll workers and/or election officials. In general, the voter's platforms will have a connection to the Internet in order to complete the voting process.

The voter's platform is not under the control of election officials except in a supervised kiosk voting system architecture. This means that there may be no poll worker or election official to ensure the voter's privacy has not been compromised or that voters have not been coerced into casting their ballot differently than they desired. In addition, the platforms not under the control of election officials may be poorly protected and vulnerable to malware, phishing, and denial of service attacks. These platforms may be the target of attacks to monitor and/or modify voter choices, capture personal information, or prevent a voter from accessing the voting services.

2.1.2 Voting System

Figure 1 shows the voting system consisting of three subcomponents: web, database, and application servers. This is a simplified representation of the three subcomponents since they may include other hardware and software not shown in the diagram to ensure system reliability and availability.

The web server provides the interface that voters use to interact with the remote electronic voting system. The web server interface may have the voter use a general purpose browser or a voting-specific client application to obtain voting services from the voting system. The web server has a connection to the Internet so voters can interact with the remote electronic voting system. In addition, the web server will interact with the application server that provides the voting services to the voter.

The application server contains the logic for the services provided by the remote electronic voting system. The services provided by the application server may include the ability for the voter to: register to vote, request a blank ballot, return completed ballots, tally the ballots, and generate election reports. The application server has an indirect connection to the Internet via its interactions with the web server. This provides the voter interface to the remote electronic voting system. In addition to interacting with the web server, the application server will interact with election database and possibly the voter registration system.

The election database contains the ballots for the different jurisdictions serviced by the remote electronic voting system. When a voter requests a ballot, the application server queries the election database to find the appropriate ballot for the voter based on their information. In addition, the election database server may store completed ballots when they are not stored on the application server. The election database server usually does not have a direct connection to the Internet. Access to the database takes place through the application server.

In general, the web server, application server, and election database are housed in one location, such as a data center managed by a jurisdiction or commercial third party. The locations that house the servers and database will need to provide the physical storage space, communication connections, and physical and logical security measures.

2.1.3 Voter Registration System

Voter registration systems are run by states and contain a repository of eligible voters who can participate in elections. The voter registration system assembles the repository of eligible voters using information from different sources such as department of motor vehicle records, judicial records, and possibly the remote electronic voting system. States provide jurisdictions with the registered voter information when elections are held. Jurisdictions can use the information to ensure that only eligible voters are allowed to cast ballots and that only one ballot is cast per voter. Figure 1 shows the voter registration system being accessed directly via an Internet connection or a more limited connection such as a state or military operated network. The jurisdictions may use their connection to the voter registration system to access the voter information in real-time during the election or to make electronic copies of the information they need at a given point during the election.

2.1.4 Election Management Console

Election officials that administer elections use the election management console. The election management console provides an interface to the voting system so administrative task, such as the configuration of ballots, defining the time and date to cast ballots, setting up the tallying rules for the election contests, and the generation of election reports, can be completed. The election management console can be located in the same place as the voting system or may be at some other location (such as the office of the election officials).

2.1.5 Component Connectivity

In general, the components that voters interact with (e.g., voters' personal computers, public computers, and kiosks) use the Internet as their connection to the voting system.

Remote electronic voting system servers and other backend system components may be on the same local network or connected to one another over the Internet.

2.2 Authorized Users

Each of the components of a remote electronic voting system is under the control of one or more different people called users. The users that control the different components are authorized to perform certain, but possibly not all, actions on the component. Although the users are authorized to perform actions on the components, they have the potential to attack the remote election voting system. This section will describe the different users found in the remote electronic voting system but will leave the description of the potential threats which these users present for Section 2.3 Threat Sources.

2.2.1 Voters

The basic voting functionality required by a voter is to: (a) submit voter registration information, (b) request and receive blank ballots, (c) complete a ballot, and (d) return a completed ballot. Voters may use their own personal computers, public computers, and/or kiosks to interface with the remote electronic voting system. In general, voters only have limited capabilities on public computers and kiosks.

Kiosks typically do not have general-purpose applications, such as word processors or email clients, so voters do not have access to these types of applications when voting from a kiosk. However, public computers may provide voters with access to applications other than voting, such as word processors, email clients, and web browsers.

When using their own personal computers, it is the responsibility of the voter to install, configure, and protect their personal computers and the applications that reside on the computer. The different platforms voters use to interface with the voting system have different security and function advantages and disadvantages when considering remote voting system architectures.

2.2.2 Election Officials

Election officials require the capability to administer an election, including adding or removing voters from the voter registration database, configuring ballot styles, defining the time and date to cast ballots, setting up the tallying rules for the election contests, and the generation of election reports. Election officials may interface with the remote electronic voting system via the election management console. As described in Section 2.1.4, the election management console may or may not be co-located with the voting system.

2.2.3 System Administrators

System administrators will require the capability to install, configure, and protect the different components of the remote electronic voting system. In addition, the system administrator will ensure the components they are responsible for can connect to other components of the remote voting system as needed. The system administrator will monitor the components they are responsible for to look for signs the components are operating improperly or are under attack. The system administrator will vary from component to component. Depending on how the architecture is implemented, third party service providers may make up the system administrator for all the components except for the voter's personal computers. Voters are the system administrators for their personal computers. Election staff will serve as system administrators for the kiosk, voting system, voter registration system, and election management console.

2.2.4 Auditors / observers

Auditors and observers will need access to information generated or observed during an election in order to perform their functions. In general, auditors and observers will have limited information collected through observation due to the distributed nature of remote electronic voting systems. Most of the information auditors and observers will have access to will be electronically generated by the remote electronic voting system with a possible exception when paper ballots are used or a voter verified paper audit trial is produced. The integrity and accuracy of the information used by the auditors and observers will greatly impact the effectiveness of their functions.

2.3 Threat Sources

Threat sources are groups or individuals that could feasibly attack a voting system. Some attacks on voting systems could be conducted by almost any dedicated individual, while others may require significant resources, knowledge or access to voting system equipment. Threat sources can be

broken down into two classes: internal and external sources. Internal sources are individuals or groups with some level of authorized access to the voting system equipment or the supporting infrastructure (e.g. the communications network). External sources are individuals or groups that do not have any special level of authorized access to the voting system equipment or supporting infrastructure. This report considers the following examples of threat sources.

2.3.1 Internal Threat Sources

In general, internal threats come from individuals or organizations with privileged and authorized access to the remote electronic voting system required to support or carry out use of the system in an election. Threats from inside sources may be more dangerous and more difficult to protect against since they have some level of access to the system.

Voters: Voters' access to the remote electronic voting system is limited through the voters' platform used: their own personal computers, public computers, and kiosks. In general, voters will not have direct access to the voting system, voter registration system, or election management console. Voters are allowed to submit voter register information, request and receive blank ballots, complete a ballot, and return a single completed ballot. However, voters may use their voting platform to try to cast multiple ballots using multiple credentials, prove how they voted to sell their vote, expand their access to damage the voting system, change the results of the election, or harm the credibility of the election results.

In addition, the voting platforms may pose a threat to the remote electronic voting system without the voters' knowledge or cooperation. When voting platforms contain malware, the voting platform may try to inhibit a voter from casting his or her ballot, alter a voter's choices, monitor how a voter votes, use the voter's credential to gain and expand access to damage the voting system, change election results, or harm the credibility of the election results. Although the voter is not actively participating in attacking the remote electronic voting system, the platform they use to interact with the voting system poses a threat that appears to be from the voter.

Election Officials: Election officials access the remote electronic voting system via the election management console and possibly voting system equipment as authorized users on the voting system component. Election officials are allowed to add eligible voters to the voter registration database, remove ineligible voters, configure ballot styles, define the time and date to cast ballots, set up the tallying rules for the election contests, and generate election reports. However, election officials may not need to be able to

install and configure applications or have unrestricted access to the remote electronic voting system equipment. Election officials will have access to election data, such as cast ballots and system event logs, on the remote electronic voting system that most other authorized users may not. Access to the election data may allow a malicious election official to modify the results of the election, monitor how people vote, and provide incorrect ballot configurations.

Similar to the voter and voters' platform, the election official and election management console may pose a threat to the voting system without the election official's knowledge. If the election management console contains malware, the console may try to prevent ballots from being cast, alter ballot configurations, monitor how voters vote, and use the election official's credential to gain and expand access to damage the voting system, change election results, and harm the credibility of the election results. Although the election official is not actively participating in attacking the remote electronic voting system, the console they use to interact with the voting system poses a threat that appears to be from an election official.

System Administrators: System administrators access the remote electronic voting system equipment via a remote connection or a terminal directly connected to the equipment. In addition, system administrators have physical access to the equipment. System administrators are allowed to install, configure, and monitor the remote electronic voting system equipment to ensure the equipment is functioning properly. System administrators may directly administer the components of the remote electronic voting system or the supporting infrastructure used by the system. For example, network technicians at telecommunication companies or Internet Service Providers (ISPs) are system administrators of the infrastructure used by the remote electronic voting system. Election IT staff are system administrators for the election management console when it is located at the election official's office. System administrators have a level of access to the system that no other authorized user has in order to configure and maintain the system. Given this level of access, system administrators may try to prevent ballots from being cast, alter ballot configurations, monitor how voters vote, damage the voting system, change election results, or harm the credibility of the election results.

Other insiders: There are other internal individuals or organizations that may have access to the remote electronic voting system equipment before, during, or after an election cycle. For example, voting system manufacturers will have access to the software source code and hardware designs used to implement their remote electronic voting system. This level of access provides an opportunity for errors to be introduced, maliciously or not, into

the components of the remote electronic voting system. Voting system integrators have similar access as voting system manufacturers, but without access to the software source code or the designs of hardware components. This level of access provides the opportunity for known software and hardware errors to be exploited, and for third party, non-voting specific software and hardware to be integrated into the remote electronic voting system components containing errors; malicious or not. The support staff of different organizations, including but not limited to jurisdictions, voting system manufacturers, voting system integrator, and third party service providers, may have access to the remote electronic voting system equipment and that provides an opportunity for the system to be exploited. Examples of support staff include administrative assistants, package and mail delivery personnel, and warehouse personnel.

2.3.2 External Threat Sources

In general, external threat sources come from individuals or organizations not needed to support or carry out use of the system in an election.

Hostile Individuals: Individuals and affiliated individuals may attempt to inhibit ballots from being cast, monitor how voters vote, damage the voting system, change election results, and harm the credibility of the election results. These individuals rely on their technical knowledge and ability to deceive legitimate users and administrators. In general, attacks from hostile individuals are limited based on resources – time, money, and people – they can accumulate or control as required for a given attack scenario.

Hostile Organizations: Like hostile individuals, hostile organizations that may not have legitimate access to the remote electronic voting system in order to attempt to inhibit ballots from being cast, monitor how voters vote, damage the voting system, change election results, and harm the credibility of the election results. Hostile organizations can marshal more resources, particularly money and people, to conduct an attack on the remote electronic voting system than an individual. Given these added resources, a hostile organization can recruit, hire, and train individuals, as well as obtain more costly technology to conduct an attack on the system. Hostile organizations can take many forms including civilian, foreign-sponsored, or terrorist organizations.

3 Overview

The remainder of this report discusses security issues that need to be considered when developing, deploying, or using remote electronic voting systems. The discussion divides the issues into four topic areas:

- ***Confidentiality:*** Confidentiality refers to the concept of ballot secrecy and also the protection of sensitive voter information and system data from unauthorized disclosure. Issues related to confidentiality are discussed in Section 4.

- ***Integrity:*** This includes data integrity, aimed at preventing important election records, including audit logs and cast votes, from being improperly modified, as well as software integrity. Issues related to voting system integrity are discussed in Section 5.

- ***Availability:*** Availability refers to the ability of the system to be accessible to voters and election officials in the face of malicious and incidental threats. Issues related to voting system availability are discussed in Section 6.

- ***Identification and Authentication:*** Identification and authentication includes the identification and authentication of voters, system operators, election officials, and system components. Issues related to the identification and authentication of voting system users and components are discussed in Section 7.

These areas were chosen to break the discussion of security issues into closely related topic areas. Issues related to any one of these topic areas are closely bound to those associated with other topics. For instance, an insufficient authentication mechanism could allow an unauthorized individual to access sensitive information (a confidentiality violation) or modify key voting system records (an integrity violation).

For each topic area, this report discusses the following:

- ***Potential Benefits:*** The move from the current mail-in absentee voting process to a remote electronic voting system can provide some benefits to security, such as in the areas of automated forms of strong authentication, timeliness of delivery, and ballot secrecy. For each of the topic areas, this report will describe the advantages of remote electronic voting.

- ***Properties:*** In order to facilitate discussion of threats to remote electronic voting systems, this report provides lists of desirable security properties. In general, threats identified in this report are actions that can violate one or more of those properties. The security properties identified in this report are based on properties and requirements identified in other electronic remote voting system documents including the Secure Electronic Registration and Voting Experiment (SERVE) Project documentation [10], the Common Criteria Protection Profile for online voting systems [8], and the Council of Europe's standards for online voting systems [9]. Policymakers ultimately must decide which properties must be met by voting systems to be acceptable in their jurisdictions. This report provides notes with each property that can help policymakers decide which properties are realistically achievable with current and emerging security technologies.

  This report provides definitions for the identified desirable security properties. While definitions may be written in absolutes, readers should recognize there are always tradeoffs that have to be made. For example, the extent a security property can be met versus the cost and usability of implementing the property. Acceptable tradeoffs must be made when deploying systems which often necessitates compromising strict interpretations of some of the proposed properties.

- ***Threats:*** This report describes some of the major threats to remote electronic voting systems. However, this document is not intended to be a thorough threat or risk assessment on remote electronic voting systems. This document describes some of the more serious threats to remote electronic voting systems. It does not attempt to enumerate all threats. Readers should consult other resources, such as NISTIR 7551, for information on additional threats.

- ***Current and Emerging Technical Approaches:*** This report identifies and describes some existing and emerging technologies that can be used to mitigate some of threats faced by remote electronic voting systems.

- ***Open Issues:*** Some security issues associated with remote electronic voting do not have complete solutions at this time. In some instances, advances in technology are needed to address threats, while in other cases the technology is developed, but is not widely deployed.

4 Confidentiality

Voting systems must protect the confidentiality of sensitive information stored on those systems. Notably, remote electronic voting systems have unique concerns about protecting ballot secrecy compared to polling place systems. While an electronic voting machine in a polling place typically does not learn the identities of voters interacting with it, remote electronic voting systems typically must identify and authenticate voters in order to verify their eligibility and provide them with the proper ballots. In some jurisdictions, local or state election procedures dictate that the identities of overseas and military voters must be able to be linked to cast ballots, a property usually forbidden in polling place systems. Despite this, remote voting systems must protect their information from being used illegitimately.

Remote electronic voting systems must also protect the confidentiality of other sensitive information on those voting systems. Remote electronic voting systems may include an online voter registration database containing sensitive personally identifiable information. They must also protect sensitive system information that could be used to compromise the security of the system, such as secret cryptographic keys or passwords.

4.1 Potential Benefits

Compared to mail-in voting, remote electronic voting systems have the potential to provide much greater technical controls for maintaining ballot secrecy. With mail-in voting, ballot secrecy is protected by procedural means: identities of voters are physically separated from cast ballots prior to viewing the contents of the ballots. Small-scale ballot secrecy violations are still possible if colluding election workers handling mail-in ballots do not follow proper election procedures. Access control mechanisms and cryptographic technologies can provide strong protections against attacks on ballot secrecy. Technical measures can be taken so an arbitrarily large number of trusted officials must collude to violate ballot secrecy.

Furthermore, remote electronic voting systems can also provide some protection against unsophisticated attempts to coerce voters. For instance, systems may allow voters to cast multiple ballots and only count the final ballot issued by the voter. If voters feel pressure to vote a particular way in one instance, they would be able to cast a new ballot at some other time or location free from improper influence. While it is significantly more difficult to block coercion attempts from more sophisticated or determined attackers, this is still a useful benefit offered by remote electronic voting systems.

4.2 Properties

This section discusses high-level properties aimed at assuring confidentiality of the vote and of the voter. Confidentiality is necessary to protect the autonomy and privacy of the voter as well as the secrecy of the vote.

A strong form of enforced confidentiality, called receipt-freeness, is also discussed. This property makes it impossible for the voter to prove to a third party how he or she voted. This property addresses the threats of coercion and buying/selling of votes.

Property: Ballot Secrecy

The voting system protects the secrecy of cast ballots.

Notes:

All voting systems leak some information about voters' choices. Such information can usually be derived from data made public during the election (e.g., partial tallies, lists of voters). The remote electronic voting system should not add to this loss of secrecy in any meaningful way. In particular, a voter should not lose plausible deniability regarding his or her vote. Protecting ballot secrecy does not necessarily mean that it must be impossible to link individuals to cast ballots; state law regarding ballot secrecy differs from jurisdiction to jurisdiction. While the general public should not be able to perform this linkage, election officials acting in accordance with state and local election law and procedures may be required to have the capability to link voters to cast ballot. For these cases, voting systems should implement protections to ensure that ballot secrecy can only be breached when proper procedures are followed. For example, the system could force multiple trusted election officials to jointly interact with the system to violate ballot secrecy, and the system could only provide mechanisms for linking single ballots, not all ballots at once.

Property: Protection of Personal Information

The voting system protects voters' personal information from unauthorized disclosure.

Notes:

The voting system should not needlessly store voters' personal information. Any personal information that is stored should be protected against unauthorized disclosure. Use of encrypted storage is recommended in order to minimize the damage caused if storage media is lost or stolen, and access control mechanisms should be used to limit access to sensitive information.

Property: Receipt-freeness

Voters are not able to provide convincing evidence of their ballot selections to third parties.

Notes:

The threat of vote selling and coercion attacks becomes more serious if voters are able to give attackers evidence of how they voted. This information could be used to reward the voter for voting correctly in a vote-selling attack or as evidence that the voter met the demands of a coercer.

Notably, remote voting systems should not increase the likelihood of large-scale buying and selling of votes compared to current mail-in voting methods. They also should not increase the likelihood of large-scale coercion of voters. Coercion is different from vote buying in that the voter is not a willing participant.

Property: Protecting sensitive system data from improper disclosure or use

All sensitive system information handled by the voting system should only be readable by authorized administrators or election officials.

Notes:

Examples of sensitive system data are: passwords or keys used by the election officials to access, configure, and run the voting system; and timestamps recording when voters authenticated or cast ballots.

Property: Minimal storage

The voting system only stores sensitive information necessary to ensure the correct functioning of the voting system.

Notes:

While there are many safeguards that can be put in place, online systems are at risk for unintended data breaches. Internet-accessible systems should not store sensitive information that is not needed by the system. Notably, voter registration databases may contain sensitive voter information, such as identification numbers, that may not be needed by the voting system. When the voting system operates its own voter list or database, sensitive data fields should not be copied over from the primary voter registration database unless the information will be used by the voting system.

Property: Limited communication

Only necessary communications traffic is passed between entities participating in the voting process.

Notes:

As a general rule, there should be limited communications between voting system components. Passing extraneous information, even information that may look benign, increases the chance that this information could be combined to violate confidentiality goals, such as ballot secrecy.

4.3 Threats to Confidentiality

This section discusses some of the more significant threats to confidentiality that are either unique to remote electronic voting systems or that may be more severe in this context. This is a high-level classification that addresses generic threats for all remote voting systems. It does not address threats to individual voting system implementations.

4.3.1 Central System Data Breaches

A data breach is an unintentional release of secure information to an unauthorized party. In the context of voting systems, data breaches can cause loss of vote secrecy as well as loss of private voter information. The potential damage of private information exposure may be less severe in voting systems than in some other systems, such as financial databases or health databases, since voting systems do not need to store as much sensitive private information.

Storage of unencrypted sensitive information carries increased risk and should be avoided when possible. Connection to the Internet also increases the risk of a data breach. Failure to properly secure encryption keys and passwords can result in granting unauthorized access to malicious (or simply curious) third parties. Poor key management can result in insufficiently vetted personnel (e.g., temporary workers) obtaining decryption keys that they are not supposed to have. This can lead to serious data breaches. Additionally, compromised keys can harm the integrity of stored or in-transit data.

A remote electronic voting system may use an external database (e.g., a vehicle registration database). In this case, the voting system could become a route for exposure of private information contained in the external database. Standard database security practices should prevent sensitive information from being exposed. However, the scenario in which two

database administrators each assumes the other is responsible for preventing data breaches is a concern.

4.3.2 Coercion

Voting systems that allow the voter to vote more than once can make it harder to effectively coerce voters (since voters could vote again at a later time). On the other hand, if the secrecy of the vote is not secured, then coercion can be a more serious problem than in non-electronic voting. The reason is that electronic coercion attacks can scale easier and impact more voters and ballots. In particular, coercion that takes the form of reprisals long after the election has ended could be a serious problem, should the secrecy of the vote be compromised on a broad scale. If the voting system has a capacity to link cast ballots to voters (say, under a court order or a voter challenge), then it may be desirable to implement a mechanism for permanent removal of this capacity. In principle, this would occur via destruction of secret keys after a prescribed amount of time has elapsed. Keys that are meant to be eventually destroyed could be split into electronic components and tamper-evident physical components to help ensure the keys are destroyed. In modern information systems, it is very difficult to fully ensure the destruction of electronic data.

4.3.3 Buying and Selling of Votes

A concern with remote electronic voting is the possibility of a market for voting credentials could emerge. A similar threat exists in the case of mail-in voting, in which the unfilled ballots could be bought and sold. However, the scalability and increased anonymity inherent to remote electronic voting potentially makes this a more serious concern. We do not know how to gauge the likelihood of this threat in the presence of law-enforcement deterrents. We note that, in most cases, this threat requires the willingness of both buyer and seller to commit a crime. This should serve as a significant deterrent to vote selling for most of the voting population. On the other hand, any change in voting technology implies a corresponding change in the cost/benefit equations that determine the extent of illegal practices such as vote selling.

A related concern is vote swapping (i.e., vote pairing). This occurred in the 2000 and 2004 elections in the US. It is conceivable that the deployment of Internet voting could cause a surge in this practice if there is an easy mechanism to exchange credentials to voting systems or verify how individuals voted.

Since long-lived voter credentials may increase the likelihood of these types of threat, it may be advantageous to have voters obtain at least part of their voting credentials in the days or weeks prior to the election.

4.3.4 Malicious Software on Client Systems

An emerging threat to computer systems over the last few years is that of malicious software infecting computers, giving attackers control of these systems. Researchers from the Georgia Tech Information Security Center have estimated that attackers may control 15 percent of online computers in this way [12]. What "control" means here is that the machines have been infected by malware that allows some level of access to them. The level of access is typically enough to steal private information and tap communications. Compromised machines could potentially violate the secrecy of the vote. Votes could be linked to machines or, depending on the voting protocol, even to voter identities. While this is clearly illegal, it is unclear what value this information might be to criminals. Unlike credit card numbers, there is no clear financial gain from knowing how a person voted. This is particularly true if such knowledge cannot be verified by a third party (as anyone can claim to know how someone else voted). Furthermore, this type of information is typically only valuable in bulk (as a reference, a single stolen piece of credit card information sells for between $0.85 to $30 [14]). Bulk voting information has two principal uses: tying demographics to voting and large-scale voting coercion. The former is easily obtainable from statistical analysis. The latter seems to be a low-likelihood threat on two accounts: i) it necessitates verifiable information; and ii) it appears hard to do without getting caught.

If compromised machines are able to steal verifiable voting information, then another threat scenario is plausible: vote buying and selling. Opinions vary regarding the severity of the vote buying and selling threat.

4.4 Current and Emerging Technical Approaches

This section discusses the main tools at our disposal for secure implementation of remote electronic voting systems. Some of the tools are standard IT security mechanisms, whereas others are of special applicability to voting.

4.4.1 Cryptographic Protections

Cryptography can protect any data that is communicated from one system to another as well as stored data. For example, the data which travels through the Internet between the voting system and the voter's computer can be efficiently protected from unauthorized access via protocols like

Secure Socket Layer (SSL) or Transport Layer Security (TLS) [15]. SSL and TLS are widely-deployed encryption mechanisms that are often used to protect communications between a web server and browsers. When used with mutual authentication, these protocols provide end-to-end security.

When used to protect data at-rest, cryptographic keys can be split between several people, requiring an arbitrary number of key holders to come together to decrypt data. Such mechanisms offer protection against insider attacks, as long as a small number of insiders can be trusted to not collude in an attack.

Proper cryptographic key management is very important to achieving protection using cryptographic techniques. Keys must be generated, stored, used, and destroyed in specific ways to ensure there are not ways to bypass the cryptographic protections.

4.4.2 Advanced Cryptographic Voting Techniques

Modern cryptology provides several possible solutions for securely conducting secret-vote online elections. These solutions provide very good properties in idealized scenarios where voters make no mistakes, have complete control of their computers, and communication lines are reliable. The scenarios typically allow for fraudulent voters attempting to sabotage the election and for attackers having unimpeded read access to all communication lines. The result of these idealized protocols is that a tally of the votes of all honest voters is obtained and is publically verifiable without compromising the secrecy of the votes.

Despite there being an abundance of voting protocols with the above properties ([16][17][18][19][20] are just a few), the problem of remote voting using the Internet is far from solved. This is because the Internet is not the idealized scenario assumed by that body of work. Voters make mistakes and their computers may be partially under the control of malware. Communication lines may not be reliable. Also, there have been no formal usability or accessibility studies of current cryptographic voting schemes yet, but researchers anticipate that such studies would identify issues that would need to be addressed. Further research may lead to dramatic improvements, but current cryptographic voting techniques do not solve many of the challenges associated with remote electronic voting.

4.4.3 Access Control Mechanisms

Access control mechanisms can be used, in conjunction with identification and authentication mechanisms, to restrict access to data, applications or

actions to particular users. Different levels of access can be granted to different users; a relatively common set of access levels include read, write, and execute permissions, and modern access control mechanisms often provide more fine grain control over permissions. Access control can be implemented in many different ways. On computer systems, access control mechanisms are most often enforced by operating systems, and, in the case of voting systems, voting applications.

For example, access control mechanisms could provide only a designated election official with the access rights to write, modify or delete ballot definition files, but give a much wider set of users access rights to only read those files.

Access control mechanisms could also implement things such as dual-person control, whereby the system requires two or more users to authenticate to the system before providing access to a particular resource. However, such functionality is often not provided by modern operating systems or applications. When used, dual-person control is often implemented with a combination of technical and procedural means.

Depending on how access control mechanisms are implemented, it may be possible to bypass those protection mechanisms. For example, if access control mechanisms are enforced by an application, users may still be able to access resources through the operating system. If the operating system enforces access control mechanisms, an individual with physical access to the system may be able to access resources by booting from a different operating system. Furthermore, in many modern operating systems, the system administrator, or root user, often has nearly unlimited control over the system. For these reasons, it is important to also use cryptographic protections to restrict access to sensitive data, rather than solely relying on common operating system or application-level access control mechanisms.

4.4.4 Separation of Duties

With a combination of procedural and technical means, operators of remote voting systems can enforce separation of duties to limit the capabilities of any single user or computer system. For instance, important information or tasks could be split between several election officials or system operators, requiring them to collude to conduct an attack. One example of how this could be implemented is that one official could be given a key to a locked room with voting system equipment, while a second official is given a credential for administering the voting system equipment.

4.5 Open Issues

Achieving a very strict notion of ballot secrecy remains a challenging issue in remote electronic voting systems. While polling place voting systems do not store, or even learn, the identities of voters, remote electronic voting systems need to authenticate voters before allowing them to cast ballots. Cryptographic protocols exist to protect the secrecy of ballots even from those with unrestricted access to voting system equipment, but these technologies may not be ready for immediate use with remote electronic voting systems. For technical, procedural, and legal reasons, it is likely that any deployed voting system for UOCAVA voters would still have access to, and probably store, sufficient information to violate ballot secrecy. Depending on policy decisions at state and local levels, this issue may not require a technical solution beyond what is already practical.

Advanced voting-specific cryptographic protocols have highly desirable properties in idealized models, but in practice, systems based on these protocols are often difficult to use and require that cryptographic keys be distributed to voters before an election. These systems also do not protect against many types of attacks, particularly if the computer used to cast votes and the voting environment are not secured.

Current techniques for remote electronic voting do not solve the problems of coercion and vote selling that are inherent to unsupervised voting. Variations on these attacks are possible with mail-in absentee voting, although in that voting method, it is difficult for a single individual to impact many voters. When moving to remote electronic voting, election officials and technologists should consider whether the move makes it easier to scale these attacks. In particular, there appear to be ways that attackers could coerce or buy votes remotely. A simple attack involves selling or transferring the credentials that voters use to log into the remote voting system. This particular issue and threat will be discussed further in the Identification and Authentication section (Section 7).

Despite IT professionals' and users' best efforts, data breaches continue to occur, releasing personally identifiable information (and other sensitive information) to attackers. This problem is not unique to voting systems. For the time being, it may be impossible to guarantee the secrecy of voter information stored on voting system equipment from determined and technically sophisticated attackers. However, there appears to be very little reason to store potentially valuable sensitive information on these systems. Depending on the type of information stored by the voting system, there may be very little motivation to attempt to illegitimately access this information.

5 Integrity

This section discusses security issues associated with voting system integrity. Integrity refers to the trustworthiness of the system, including both the data on the system and the functions provided by the system's software. Maintaining integrity involves implementing safeguards to ensure data and software on a system are not modified by unauthorized parties. It is typically preferable to have these safeguards block unauthorized attempts to modify data or software, but in some cases, it is only possible to detect integrity violations.

Integrity includes the concept of the origin or source from which the integrity is based upon. In other words, the origin or source of the integrity for data or software functionality can be traced back to a particular trusted authoritative entity. Tracing integrity back to a particular entity is closely related to identification and authentication, which is covered in Section 7.

5.1 Potential Benefits

5.1.1 Authenticity of Electronic Records

A cryptographically signed record of each cast ballot can be issued by the voting system components and transmitted for tallying and auditing purposes. The signed record can be easily and exactly replicated to reduce the likelihood of data loss. Assuming adequate key management, the signed record cannot be forged. Authenticity can be verified using public key cryptography.

5.1.2 Strong Integrity Protections In-Transit

It is a common misconception that the greatest threat associated with conducting transactions over the Internet is the modification of information as it is being transmitted. While this is a potential threat that must be mitigated, in fact there are very good technical solutions for protecting information during transmission. Cryptographic protocols, such as TLS or Internet Protocol Security (IPSec), are very effective at providing integrity protection in-transit.

5.2 Properties

There are two main categories of properties for integrity: data integrity and software integrity. Data integrity is related to the integrity of the election records, especially those records directly used to derive the final election tallies, as well as those necessary for meaningful audits. Software integrity refers to the correct, unmodified software running on the electronic

components of the voting system. Faulty or malicious software may directly affect election data integrity.

5.2.1 Data Integrity Properties

Property: Accuracy

The election outcome properly reflects the choices of participating voters.

Notes:

The voting system must: (a) record votes consistent with voters' selections, (b) accurately store the collection of cast ballots, (c) protect the cast ballots from unauthorized modification, deletion or insertion, and (d) accurately count the votes.

Property: Auditability

The voting system provides evidence of its behavior before, during and after an election.

Notes:

It is not enough for a voting system to merely function correctly. The voting system must also provide evidence to auditors that the system functioned in the way it was supposed to. The evidence could include system event logs, public voting system reports, voter-verified records, and, in some cases, mathematical proofs. In addition, the voting system and its supporting election procedures must provide assurances that the evidence provided by the system is trustworthy. Auditability is a high-level security property of a voting system with more specific sub-properties listed and described in this sub-section.

Property: Privileged verifiability

The voting system provides evidence that allows the election auditors to independently check the outcome of the election.

Notes:

In general, verifiability is a voting system property where an observer is able to check the election outcome produced by the voting system is correct. That is, the system should produce ample evidence allowing auditors to verify the results of an election. In the case of privileged verifiability, the evidence provided could be secret or sensitive information that could only be made available to, or authenticated by, election insiders.

Property: Public verifiability

The voting system provides evidence that allows the general public to independently check the outcome of the election.

Notes:

Public verifiability is a property offered by emerging cryptographic voting protocols. In this case, sufficient evidence is made publically available by the voting system so any individual can verify the outcome of the election. Generally this requires some assumptions about the behavior of other entities (e.g., other voters, poll workers, administrators, etc.).

Property: Traceability

The voting system maintains all the necessary information so that if a problem is found in a particular election, then it is possible for the election officials to trace the problem to one or more root causes.

Notes:

If there are any problems during an election, it is important to be able to trace problems back to their root causes. The voting system should log or otherwise track sufficient events on the voting system to determine which activities failed or succeeded.

Property: Recoverability

The voting system maintains necessary information to allow it to recover from a loss of integrity. If the integrity of election records is lost in a way that is irrecoverable, then the extent to which the problem affects the final tally is measurable.

Notes:

If a voting system fails, then it should fail in a graceful manner. A minor problem should not necessarily call into question the integrity of the entire election. When possible, the voting system should be able to recover from minor problems. In some instances a voting system will not be able to recover from an error. In these instances, it should be possible to measure the extent of a failure so appropriate remediation can be carried out.

Property: Prevention of data alteration

The voting system prevents the unauthorized modification, deletion or insertion of election or voting system records.

Notes:

A voting system contains a great deal of data (e.g., system files, election records, and event logs) that must be protected from

unauthorized manipulation. To the extent possible, the voting system should prevent unauthorized manipulation and detect any manipulation that takes place.

Property: Logging data alteration

The voting system keeps a secure log with the information about who created/modified/deleted data which may influence the outcome of the election.

Notes:

Secure audit logs can help to increase accountability of system administrators and other insiders with privileged access to the machine. The log should be secure against modification by anyone, and should only be readable by authorized users.

Property: Data authenticity

Election auditors are able to verify the authenticity and provenance of election records.

Notes:

While protecting ballot secrecy, the voting system should provide sufficient evidence to allow election auditors to determine what entity (e.g., voter, system administrator, voting system component) created an election record and to verify that the record was not modified by unauthorized parties.

5.2.2 Software Integrity Properties

Property: Integrity of server software

Voting system components only load and execute authorized software.

Notes:

The voting system back-end components, such as servers, databases, and supporting network components, should only run authorized software. Front-end components under the control of election officials, such as kiosks, should also only run authorized software. For instance, the system should be free of malicious software. In addition, processes should be put in place to validate and authorize updates to voting system application software other third-party software used on the systems (e.g., operating systems, database software, anti-malware software).

Property: Authenticity of server software

Election auditors and/or system administrators are able to verify that only authorized software is present on voting system components.

Notes:

Auditors and system administrators should be able to verify that the voting system is free of malicious software and that only the authorized software is present on the voting system. In general, software validation is difficult to do rigorously and letting the voting system software verify itself is not sufficient.

Property: Proper software engineering practices

The voting system software is designed, implemented, tested and deployed with accepted software engineering best practices.

Notes:

Software engineering and testing best practices help to reduce errors in the design and implementation of voting systems.

5.3 Threats to Integrity

In general, any electronic system is prone to software bugs and malicious software attacks. Bugs and attacks related to software may result in partial loss of data integrity, and thus directly influence the election results. Moreover, Internet voting uses personally owned and operated devices which may be highly vulnerable to attacks that are capable of impacting election integrity. The election officials may have no practical way to assess the integrity of personal computers.

5.3.1 Software Bugs

One of the greatest threats to the integrity and accuracy of election records, including cast ballots, comes from non-malicious software defects, called software bugs. Software bugs accidently written into voting system application software, third-party libraries, and commercial software required to run the voting system all have the potential to impact election integrity.

Software bugs should be expected when dealing with software. In general, the larger a piece of software is, the more bugs are likely present. Estimates on the software industry's rate of bugs range from about 15 to 50 errors per 1000 lines of code [11]. Modern voting system application software can be quite large containing tens of thousands of lines of code. In most cases, voting systems run on top of commercial operating systems which can have

tens of millions of lines of code and use various other commercial libraries of software applications of varying complexity.

Extensive testing and analysis can identify many bugs but will never uncover all of them. Software bugs occur in medical devices, military equipment, and space exploration vehicles, despite extensive and sophisticated testing in these areas. In addition, software bugs affecting cast votes have been identified in certified voting systems [12], despite testing and code review during testing.

Even software whose source code is freely available to the public can contain major software bugs for years without discovery. The OpenSSL library included with the Debian-based linux distributions included a software bug in the cryptographic key generation function that resulted in a serious vulnerability in applications that relied on this library [13]. The bug went unnoticed for more than one year before being patched.

5.3.2 Malicious Software on System Servers

Specialized software could be maliciously placed on voting system equipment to modify or incorrectly store election records. The malicious code could be placed on the voting system equipment at any time in the system's life cycle. Developers of the voting system software, or any software used by the voting system, could include malicious code. Election insiders, such as system administrators, could install malicious software that changes election data. Or, remote attackers may be able to exploit a vulnerability in the voting system to install malicious code on the system. These attacks have the potential to change a large number of votes and can be difficult to detect.

5.3.3 Modification of Election Records and Data

Rather than installing malicious code on voting system servers and other back-end components, attackers may be able to modify election records directly to compromise election integrity. For example, a system administrator may be able to modify records stored on a database server. Or, vulnerabilities in the voting system may allow a remote attacker to perform an SQL injection attack to modify records in the database.

5.3.4 Malicious Software on Client Systems

The threats described in the previous sections are largely variations on similar threats faced by polling place electronic voting systems. However, Internet voting systems are also faced with threats to voters' personal

computers which are used as voting terminals. Attacks on these systems fall into a category generally referred to as client-side attacks. In most cases, these involve an attacker infecting a victim's computer with malicious software (e.g., a computer virus, trojan or worm) in order to gain access to information stored on that client machine or control it in various ways.

Client machines are quickly becoming a predominant attack vector in all types of information technology systems. Given the amount of sensitive information often stored on web, file, and database servers, these servers are often very tempting targets for attacks but they also tend to be the best protected, with professionally trained system administrators configuring and monitoring those systems. Client machines, used by regular employees or individuals, are often much less protected against attacks since they are operated by less technically sophisticated users. The client machine may be the intended target of an attacker, or it may be used as a stepping stone to attacking another computer system.

Attacks can use a variety of means to get malicious software on individuals' personal computers. Historically, file attachments sent over electronic mail were a common method for distributing malicious software. Alternatively, an attacker could post malicious software that appears to have a desirable purpose (e.g., a game, anti-virus software, screensaver, etc.) on a web site and encourage people to download it. In these cases, the victim became infected with the malicious software by executing the file attachment or downloaded file.

More recently, vulnerabilities in commonly used software became a common attack vector for malicious software. Some malicious software is self-replicating, where infected machines seek out other machines to infect, such as the 2003 Blaster worm that exploited a vulnerability in the Windows operating system. Individuals could become infected with the Blaster worm merely by connecting their Windows computer to the Internet. New vulnerabilities in commonly used application software have led to a new attack method, commonly referred to as drive-by-downloads. Using vulnerabilities in browsers, browser plugins, and other commonly used software, users can become infected with malicious software merely by visiting infected web sites.

An infected machine is largely under the control of an attacker. If a voter's personal computer becomes infected with a malicious software targeting the election, an attacker can potentially steal the victim's authentication credentials (e.g., a password or PIN), or even change the victim's vote without the victim noticing.

Malicious software is a serious problem on the Internet, with a large number of computers already infected with some type of virus or trojan. A growing problem on the Internet is botnets: groups of infected computers under the control of an attacker. The malicious software running on infected computers in a botnet is often used to steal passwords and other credentials for email and social networking sites in order to facilitate spreading the software to other computers. In many cases, the purpose of the attack is to steal financial data, such as passwords to online banking sites or credit card numbers. In some cases, malicious software on botnet-infected computers can even change the data inputted on a website for a financial transaction. For instance, it can change the bank account destination and amount for a money transfer on an online banking website.

Botnets are sometimes rented or sold by the individuals that originally conducted the attack to other parties. In addition, the malicious software behind the botnets is sold on black-market websites. For example, the malicious software behind the Zeus botnet is sold for as little as $700. Researchers at Cisco found that attackers could build a complete Zeus botnet for $2500, which includes the cost for the Zeus malware, exploit tools to infect users, and servers for conducting the attack [22]. While existing malicious software would have to be modified to attack an Internet voting system, this may not be difficult. In fact, many existing botnets include the ability to remotely update the malicious software running on already-infected computers. This means attackers would not necessarily have to re-infect computers already in botnets to attack an Internet voting system.

Because voters' personal computers are outside the control of election officials and voting system administrators, client-side attacks are very difficult to mitigate. While each successful attack on the client can only impact one vote or voter (or potentially a small number of voters if a computer is shared), attackers have demonstrated an ability to infect a large number of clients, and thus client-side attacks have the ability to have a large-scale impact.

5.4 Current and Emerging Technical Approaches

There are a number of techniques, some more mature than others, which can be used to address some of the threats to integrity of election results in the context of remote electronic voting. A summary of these techniques is presented below.

5.4.1 Cryptographic Integrity Protection

The data which travels through the Internet between the voting system and the voter's computer can be efficiently protected from en-route modifications via protocols like Secure Socket Layer (SSL) and Transport Layer Security (TLS). SSL and TLS are widely used to protect the integrity of communications between web servers and browsers and are frequently used in other applications as well such as email client and server communications. When used with mutual authentication, these protocols provide end-to-end security. In addition, cryptographic integrity protections, such as digital signatures and message authentication codes, can detect any changes in data as it is transmitted from one system to another. Cryptography can be very effective at protecting data in-transit and at-rest. However, cryptographic integrity protections do little to protect data as it is being processed on voting system components, such as when cast votes are constructed on client machines, or when they are tabulated on back-end equipment.

5.4.2 Advanced Cryptographic Voting Techniques

A specific research area in cryptography has been investigating more secure voting protocols to protect ballot secrecy, while at the same time offering unique integrity protections. These protocols, often called end-to-end cryptographic voting protocols, may be able to detect certain types of attacks where the election outcome is not the result of the aggregation of all cast votes. They can produce irrefutable proofs of tampering, even if a small number of cast ballots have been modified or deleted. Both voters and the general public can check that all cast ballots have been correctly tallied by the voting system. Additionally, end-to-end cryptographic voting protocols may allow each voter to verify that his/her vote appears in the final tally. There is a high degree of overlap between these protocols and the cryptographic protocols previously described in Section 4.4.2 to protect ballot secrecy.

The threat model for end-to-end cryptographic voting systems often assumes attackers have compromised the back-end voting system software. Thus, these systems can provide protection against attacks when cast ballots are modified in-transit or stored on voting system back-end equipment, and attacks that modify ballots or cause them to be incorrectly tabulated.

However, there are many types of attacks on voting systems that are not mitigated by end-to-end cryptographic voting protocols alone. In general, end-to-end cryptographic voting protocols may do little to mitigate client-side security threats, as cast ballots can be modified as they are constructed on the client machine. While end-to-end cryptographic voting protocols allow

the voter, or their proxy, to detect changes to cast ballots after they are constructed on a machine, they provide limited or difficult means to check the constructed cast ballot actually corresponds to the voter's choices. However, systems that provide clear text receipts of voters' choices are much easier to check, but these systems present potential problems with ballot secrecy and coercion. In addition, end-to-end cryptographic voting protocols do little to protect against attacks where voters' authentication credentials are stolen or sold.

At this time, there have been no formal usability or accessibility studies of current cryptographic voting schemes, but researchers anticipate that such studies would identify issues that would need to be addressed.

Remote electronic voting systems using end-to-end cryptographic voting protocols have been fielded in a limited number of pilots, including a university election at the Université Catholique de Louvain in March of 2009 [23]. End-to-end cryptographic voting protocols are an ongoing area of research, and researchers in academia and industry are coming up with different methods to address the shortcomings of these techniques.

5.4.3 Use of a Voter-Held Trusted Hardware Component

The threat posed by client-side vulnerabilities might be significantly reduced if the voter could use a third computing device that could communicate with the client machine and which could reasonably be assumed to be secure. Smart-cards and cell phones could, in principle, play this role. But it may be too expensive to add this capability to these devices for the sole purpose of voting, but this could be implemented to also help secure electronic commerce transactions.

5.4.4 Malware Detection/Prevention Software

Many commercial and free tools protect against malware, including antivirus and anti-spyware programs. These tools typically work by scanning files downloaded or opened on a computer. The tools look for patterns in files that match those of known malware. This is called signature-based detection. Many newer forms of anti-malware software can do more sophisticated heuristic-based checking in addition to signature detection to identify new malware. However, this is generally only effective at identifying new variants of an already-known piece of malware.

Anti-malware programs do not completely mitigate the threat of malware. Because anti-malware programs are dependent on an up-to-date list of malware signatures, users must update their anti-malware programs

frequently. In addition, anti-malware programs are not effective against new types of malware that have not yet been identified by vendors of anti-malware software and added to signature lists. Even known malware can be difficult to detect, as there are several techniques for writing malware to try to avoid signature-based detection. Once a computer is infected with malware, antivirus software may fail to detect or remove the virus. Some malware disables anti-malware software running on infected machines in ways that are not easy to detect.

5.4.5 Remote Software Verification

One area of research and development is remotely verifying that a piece of software on a given computer has not been tampered with. The most common application for this technology is to limit cheating in online gaming. In some online games, hackers have discovered ways of modifying software on their system to give them an unfair advantage. These anti-cheating mechanisms check the integrity of gaming software and data files looking for known cheating software in memory. It may be possible to extend these ideas to remotely inspect a voter's computer for malware.

Some current virtual private network software distributions include mechanisms to do end-point security scanning. When connecting to a server, the client machine downloads software from within the browser (often a Java application or ActiveX control) which performs some security scans on the client machine and relays the results to the server. Typically the purpose of scanning the system is to enforce an organization's security policy, such as running up-to-date antivirus software and a properly patched operating system.

An area of active research and development that may bring about more rigorous methods for remote software attestation is trusted computing platforms. In the future, it may be possible to use trusted computing modules (TPM) in voters' computers to demonstrate to an Internet voting system server the computers are in a desired state free of malware capable of tampering votes. The use of TPMs in voting systems is an active research area, with researchers proposing different methods for their use in voting systems [22][24]. While much of this research is focused on using TPMs in Direct Record Electronic (DRE) systems, the ideas could be extended for use in personal computers and Internet voting system servers. However, there are significant technical challenges to finding a workable solution. Furthermore, if and when solutions are found and implemented, deployment of the necessary hardware and software would likely be slow.

5.4.6 Formal Verification of Software

Formal verification of software involves providing mathematical proofs of the correctness of a given piece of software. In order to do formal verification, it must be possible to very precisely describe correct behavior in an algorithm. For this reason, formal verification is very hard to do for large software systems since it is difficult to precisely capture the behavior of a complex system. However formal verification is sometimes done for smaller pieces of a larger software system, such as the software implementing a cryptographic algorithm or protocol. Formal verification of software is very expensive, and is only done in extraordinary applications. For example, the INTEGRITY-178B real-time operating system, one of only two formally-verified operating systems, is used in military and commercial avionics.

Formal verification of system designs, while still uncommon, is required at Evaluation Assurance Levels 5, 6 and 7 of a Common Criteria security evaluation [25]. Again, these often involve verifying only a small piece of software within a larger system.

Because of its considerable cost, formal verification of software or designs is likely not well-suited to mitigating risks of software defects or vulnerabilities in remote electronic voting systems.

5.4.7 Preconfigured Bootable Environments

One method proposed for dealing with client-side security issues on voters' personal computers is to give voters a known-secure voting environment. This could be accomplished by distributed bootable media, such as CDs, DVDs, or USB drives that have been preconfigured with security hardening, and for connecting only to the Internet voting servers.

However, this approach has several significant disadvantages. One of the arguments for remote electronic voting has been the difficulty of distributing election materials to voters. Bootable media would likely have to be distributed by mail and would pose similar delivery challenges, such as obtaining up-to-date mailing address information for each voter. In addition, it would be very difficult to guarantee the bootable media would work on the vast majority of voters' personal computers. And, perhaps most significantly, it may be very hard for voters to identify legitimate bootable media from fraudulent media. Rather than serving to protect voters from malicious software, this could provide an avenue for attackers to distribute their own bootable media with malicious software preinstalled.

5.4.8 Virtualization Technologies

A possible way of bypassing some of the logistical problems of creating and distributing bootable media may be to use virtualization technology to run a clean voting environment in a virtual machine. That is, software running on a voter's computer could simulate a computer free of malware. This could alleviate some of the problems associated with bootable media including appropriate drivers and ensuring the default configuration would be compatible with a given user's network. Nonetheless, there are still significant logistical problems associated with attempting to securely distribute virtual machine images to voters. And, as was the case with bootable media, there remains the potential problem of voters using virtual machines pre-loaded with malicious software.

Generally, virtualization technology has been concerned with protecting the host operating system that is running the virtual machine software from any malicious or unreliable software running on the virtual machine's operating system. However, vendors of virtualization technology are beginning to implement systems that provide some protection against unauthorized modification of virtual machines by applications running on the host operating system. This is an important feature, as the reason for using these virtual machines is to protect voters from any malicious software running on their computers.

5.4.9 Secondary Communication Channels

While many of the technical approaches described above attempt to deal with the problem of malicious software on voters' computers by either detecting the malicious software or preventing its installation, another approach is to try to make voting from an infected computer reasonably safe. There are methods that attempt to do this using a secondary communication channel between the voter and the election authority that is independent from the voter's channel to the election authority such as the Internet through his or her personal computer. This second channel could be used when voters mark ballots to prevent malicious code from modifying votes in a directed way, or it could be used to confirm voters' selections.

In the first case, voters could be given individualized code sheets with unique random codes assigned to each candidate or choice on the ballot. In this case, the second channel might be the postal mail. To vote for a particular candidate, the voter would have to enter the random code assigned to that candidate on the Internet voting website. Malicious code running on the voter's computer would not know the association between the candidates and random codes, and thus would not be able to change votes to a particular candidate. However, malicious software could still

prevent voters from casting ballots, or try to deceive the voter into giving it the necessary information to change votes. In addition, there are significant usability concerns about this type of approach, in addition to logistical concerns involving the distribution of these code sheets to voters.

Alternatively, the second communication channel could be used to confirm a voter's selections. For example, a voter could be sent a message indicating how he or she voted. In this case, it is important that the second channel offer very fast delivery of messages, like a text message or telephone call, so the voter can confirm their selections in real-time. However, this approach creates some concerns related to vote selling by providing a channel which could be used by a vote buyer to verify how someone voted.

Electronic mail may be a tempting choice for a secondary communications channel, but there are significant drawbacks to using e-mail in this manner. E-mail is not an independent second channel, as the same computer and Internet connection used to construct and transmit the vote would likely be used to receive the e-mail. Malicious software running on the voter's computer may be able to change incoming e-mails along with cast votes.

5.4.10 Messages Computers Can't Understand

An alternative to using secondary communication channels is to communicate with the voter through the standard channel but coding information in ways that a computer cannot understand such as CAPTCHAs. CAPTCHAs are little puzzles that users are asked to solve, often involving reading distorted text, to prove that a human is accessing a Web application. CAPTCHAs are often used to try to block attacks where automated computer programs access a website and attempt to submit or collect information.

In principle, the whole ballot could be rendered using CAPTCHAS with the voter exercising choices by clicking on the rendered image. In this case, the client-side machine is unable to associate voter choices with locations of clicks. Even without the use of CAPTCHAS, using pointers to images instead of text should make it harder for malware to decode voter choices in order to alter them in favor of a given choice, because this is not a feature offered by currently available malware kits. Further research on these ideas is needed to identify usability and other issues that may arise. Note, these techniques do not stop the client machine from preventing the vote or randomizing it, and introduce usability and accessibility challenges that may not be adequately addressed.

5.5 Open Issues

Ensuring the security of personally-owned computers remains a very serious open issue. At this time, there is relatively little jurisdictions can do to ensure that voters' computers are free from malware capable of changing ballots cast from those machines. Attackers have demonstrated an ability to infect large numbers of machines with malicious software. Although in the case of UOCAVA voting, attackers would need to successfully target the relatively small percentage of individuals' in the world that are eligible to vote as overseas or military voters. While remote software verification, trusted computing modules, and computer virtualization are potentially promising technologies for mitigating the threat of malware on voters' computers, none of these technologies appear ready for immediate use with remote electronic voting systems.

There are also open issues related to the security of software on voting system servers. While extensive testing may be able to uncover many software bugs, there are no guarantees it can uncover all bugs in the software.

Advanced cryptographic voting technique, specifically end-to-end cryptographic voting protocols, can be highly effective at detecting certain types of attacks on election integrity, including modification or deletion of cast ballots. However at this time, they are most effective against mitigating attacks that take place on the voting system servers. Most of these techniques are not effective at detecting attacks taking place on the computers used to cast ballots. While extending end-to-end cryptographic voting protocols to detect client-side attacks is an active research area, methods that have been proposed are either difficult to use or impractical. In some cases, end-to-end cryptographic voting techniques only detect if an integrity violation has occurred. It may not be possible to recover from the detected error or to measure the extent to which the detected error affects the outcome of the election. Also, end-to-end cryptographic voting techniques may not be able to distinguish between a bug and an active attack. While this is an area of ongoing research and activities, end-to-end cryptographic voting techniques for Internet voting are largely still an academic effort.

6 Availability

Availability is used to describe the proportion of time a system is functioning and operating, including times when the system is performing at reduced capacity. Due to resource overload, malicious attack, and system malfunction, a system may become unable to function, and thus is considered unavailable.

6.1 Potential Benefits

Electronic transmission of election materials can provide several benefits to UOCAVA voters and election officials compared to alternative voting methods for overseas and military voters. The following section describes some of the potential benefits.

6.1.1 Timeliness of Delivery

Internet voting systems do not suffer from the same delays associated with voting through the postal mail. Postal mail delivery to remote locations can take significantly more time than delivery times within the United States. For example, delivery through the military postal system to Middle East postal offices typically takes 7-12 days [27]. Internet transmission, however, is nearly instantaneous, as long as voting system endpoints (the server and the client) and communication lines are operational.

6.1.2 Receipt Confirmation

The United States Postal Service (USPS) is a relatively reliable delivery mechanism, with first class mail on-time performance exceeding 90% [28]. However, mail to UOCAVA voters must go through other postal services in addition to the USPS, such as the military postal system, or those of foreign nations. Delivery confirmation is an option for USPS mail to military addresses, but is often not an option for mail to and from foreign addresses. Therefore, it is nearly impossible to detect which blank or completed ballots have been lost or delayed in the mail system.

Remote voting over the Internet can provide immediate feedback to senders if there is a transmission problem via real-time confirmation and error messages. This information could be used to detect problems and remediate them.

6.1.3 Flexibility of Physical Locations

Overseas voters, particularly military voters, are a highly mobile population, and are not always quick to inform their local election officials of their new addresses. Remote voting over the Internet allows voters to receive or cast ballots regardless of their physical location.

6.2 Properties

Property: Up-time

Voters, election officials, and other system operators are able to use the voting system normally for a substantial percentage of the total time allowed to configure the system, cast votes, and tally votes.

Notes:

Up-time is a measure of the extent a system is available for use by system operators and users. A number of factors affect up-time, including how often failures occur (see the "Reliability" property) and time it takes system administrators to restore functionality after a failure occurs. System availability can be maliciously targeted by an attacker to disrupt voters from casting their ballots.

Property: Reliability

The voting system, to a high degree of probability, will remain operational during the election under predefined normal operating conditions.

Notes:

Reliability is a measure of the likelihood a system will continue to perform as intended for a specified time under a particular set of predefined conditions. In this case, reliability is referred to as the likelihood the voting system can complete an election without a loss of functionality when it is not facing a malicious attacker.

Property: Recoverability

Voting system operators are able to restore the system to normal operation in a timely manner when failures occur.

Notes:

Voting systems should be designed to limit downtime in the event of failures. In practice this implies a very low probability of catastrophic failure such as loss of stored cast ballots.

Property: Fault-Tolerance

The voting system is able to continue operation, perhaps at a reduced level of functionality, when failures or attacks occur.

Notes:

A common method for achieving some level of fault-tolerance is to use redundant system components or resources.

Property: Fail-Safe

In the event of a failure or attack, the voting system experiences minimal data loss or further damage to voting system components not directly affected by the failure or attack.

Notes:

Fail-safe is a system property which states that voting system failures or attacks should have limited impact on the integrity and availability of system components and data. For example, hardware component failures in the voting system should not result in the loss of cast vote records or audit information. An attack on one component in a voting system should not damage a second component. For instance, an attack on the voter registration database should not harm the voting system web server, although it may inhibit voting activities until the issue with the voter registration database is resolved.

Property: Scalability

The capacity of the voting system can be increased with additional resources (e.g., servers, network bandwidth, etc.) without redesigning the system's architecture.

Notes:

A scalable voting system can grow to accept greater and greater number of voters by adding additional hardware, more powerful hardware, faster network connections, other computing resources, or any combination thereof.

6.3 Threats to Availability

Like any information technology system, Internet voting may be the target of denial of service attacks (see [29] for precinct voting denial of service attacks). The potential scale and impact of the attack may be much larger for Internet voting systems than for polling place voting or mail-in voting. The attacks can be targeted towards the server providing the voting service, the personal computers of the voters, or the infrastructure connecting the two. Denial of service attacks may be selective, such as disrupting service for voters deemed likely to cast a ballot in a particular way (e.g., a particular demographic group).

6.3.1 Large-Scale Denial of Service

Denial of service attacks are a type of attack where malicious individuals attempt to make a computer system unavailable to its users. Depending on

the nature of the attack, and on its target, a denial of service attack can be anything from a minor nuisance to a devastating attack.

Denial of service attacks could prevent voters from being able to cast votes either by making Internet voting system servers inaccessible or disrupting systems they rely on, such as the communications infrastructure or voter registration database. Aimed at the back-end of the voting system, these attacks could prevent large numbers of people from casting ballots over the duration (anywhere from hours to days) of the attack.

Denial of service attacks of varying severity occur frequently on the Internet. The type of target and motivation differs from attack to attack. A frequent motive of attackers is political in nature, with attacks carried out by individuals or groups disagreeing with the victim's views. Large corporations, nation states, and the communications infrastructure are frequent targets for attack. For example, in 2007 the nation of Estonia was targeted with a large-scale denial of service attack [30], with the nation of Georgia experiencing a similar attack in 2008 [31]. Critical portions of the Domain Name System (DNS) have also been targeted with attacks, including distributed denial of service attacks against root DNS servers in 2002 [32] and 2007 [33].

Denial of service attacks can be conducted in a variety of ways, but most major attacks are distributed denial of service attacks. Collections of malware infected computers, known as botnets, can be purchased or rented by attackers to be used to attack a target organization.

6.3.2 Selective Disruption and Suppression

While denial of service attacks can cause voter disenfranchisement on a significant scale, their ability to impact the outcome of an election is somewhat limited unless the attack is focused on a particular demographic or jurisdiction. However, targeted denial of service attacks have been documented. In 2009, denial of service attacks targeted a specific Georgian blogger on Twitter, Facebook, Livejournal and Google [34]. Denial of service attacks that selectively disrupt systems at a particular jurisdiction or certain voter demographic could not only result in voter disenfranchisement, but also sway the results of an election.

Remote electronic voting may make it harder to prevent a voter from attempting to vote when the voting system is architected to function and operate even under vote suppression attacks. On the other hand, some cyber attacks, such as denial of service attacks, may make it easier to thwart an attempt to vote due to the resources available to an attacker in the form of computers controlled by botnets.

6.3.3 Client-Side Disruption

While most large-scale attacks on availability target one of the voting system's servers or the communications infrastructure, attacks can also target the voters' machines. Malware on voters' computers could prevent them from accessing voting web sites.

6.4 Current and Emerging Technical Approaches

While there is no general solution to denial of service attacks, a series of techniques can be used to prevent, detect and speed up recovery from such attacks.

6.4.1 Redundancy and Over-provisioning

The most widely used approaches for achieving high-availability systems include the use of redundant systems and over-provisioning of system resources. At a basic level, these approaches involve fielding systems with excess capacity so they are able to better handle failures on certain system components or attacks.

Redundancy involves the duplication of critical system components. The duplicate components are used as backups in the event of failures or to augment capacity in the event of a spike in legitimate or illegitimate traffic. For instance, a system could be designed with redundant web servers such that the backup system can take over the expected load in the event the primary system fails.

A more general approach, called over-provisioning of system resources, involves fielding systems capable of handling a much greater load than would be expected under normal conditions. A useful strategy is to identify possible performance bottlenecks in the system and to augment the capacity at those bottlenecks. Possible bottlenecks include capacity and performance of the communications lines, support infrastructure (such as firewalls and routers), or database and web servers. Over-provisioning can involve any combination of duplicating resources (e.g., mirrored sites located at multiple physical locations) or making individual resources more powerful or abundant (e.g., faster network connections, more powerful servers, etc.) than would ordinarily be needed.

Fielding over-provisioned systems can be costly, particularly for relatively small systems such as Internet voting systems that are rarely used and have less traffic than major e-commerce web sites. Small increases in system capacity are not likely to deter or prevent attacks on availability, but large

increases in capacity may be wasteful and still potentially ineffective. Over-provisioning raises the bar for attacks but does not make attacks impossible.

6.4.2 Detecting Active Attacks on Availability

Compared to other types of attacks on voting system, availability attacks are usually relatively easy to detect by system administrators. In some cases, the system crashes or becomes unavailable to all users. At this point, voters have already been affected and will continue to be affected until the attack is successfully repelled. The key to maximizing availability in the face of denial of service attacks is early detection and quick reaction.

6.4.3 Defending Against Active Attacks

The most common approach for defending against denial of service attacks is over-provisioning, which provides protection against all kinds of incidental or malicious threats to availability. However, there are a number of other things system designers and administrators can do to defend against attacks.

One approach is to preemptively harden systems against denial of service attacks. Hardening voting systems include identifying and fixing bottlenecks as well as vulnerabilities in host systems that make denial of service attacks easier to carry out, and carefully designing the internal network infrastructure. In some cases, there may be multiple technical options for designing a secure and usable voting system that works equally well for their intended tasks but may be more resistant to denial of service attacks.

Another approach is to filter dangerous network traffic containing known attacks carefully constructed to crash or overwhelm a particular system resource. Once an active denial of service attack is detected, an organization may be able to filter out the network traffic making up the attack. While network traffic filtering can be done on the border of an organization's network, an attack may attempt to overwhelm the filtering mechanism or merely fill the in-bound network connection. In these cases, it is helpful to filter attack traffic closer to the source, which usually requires the help of third-party Internet service providers.

Some distributed denial of service attacks work on the premise an attacking client can force a server or other device to consume far more resources than those required by the client to conduct the attack. For example, establishing a Transmission Control Protocol (TCP) connection with the server requires that the server allocate resources before the client. There are approaches that attempt to address the client server resource imbalance, such as SYN

Cookies and proof-of-work techniques, by forcing clients to allocate some resources before establishing a connection with a server [35].

6.4.4 Cloud Computing

In protecting system availability, there is strength in numbers. Having redundant systems to migrate to after a failure, or having excess capacity to raise the bar for denial of service attacks, can help systems achieve higher levels of availability. However, purchasing, deploying and maintaining this excess capacity may be cost-prohibitive. An emerging area in the computer industry is a concept known as cloud computing. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [36].

In the cloud computing model, a large pool of resources can be distributed between many different applications and even customers. Excess capacity in the system can be applied to any of the applications running in the cloud on an as-needed basis, and the cost associated with maintaining the excess capacity can essentially be distributed across all of the customers. In the event of a hardware failure on a particular machine in the cloud, any applications running on that machine can be almost immediately transferred to a different physical machine in the cloud. In the event of a spike in traffic for a particular application, additional physical or logical machines, network bandwidth, or other resources could be allocated to that application.

However, in cloud environments, multiple applications are being hosted on the same systems. So, in the case of an Internet voting system, the voting system may be running on the same equipment used to perform completely unrelated tasks. When a service provider manages the cloud, each customer may have little control of what other applications coexist on the same physical equipment. Typically, virtualization technology is used to keep different application resources logically, rather than physically, separate. However, this introduces new security issues researchers have only begun to look at in the last few years.

Cloud computing appears to be a very promising technology for increasing system availability in a cost-effective manner, but it is not clear if it is ready or suitable for use with remote electronic voting systems.

6.5 Open Issues

Most defensive techniques against denial of service attacks can raise the bar for an attacker to successfully mount an attack but cannot guarantee protection. In fact, due to the nature of the Internet, it may not be possible to provide complete protection from certain types of availability attacks. Given the commercial availability of botnets for use in distributed denial of service attacks, attacks on availability are a very real threat to Internet voting systems.

However, Internet voting systems are no more vulnerable to denial of service attacks than many other types of online computer systems as, at a high-level, their architectures have many similarities. And, the threats to voting system availability should be considered relative to availability issues faced by mail-in absentee voting, including undeliverable mail due to a frequently moving overseas voting population and the time necessary to send or return election materials.

Cloud computing appears to be a promising technology. However, it is a young field where researchers and developers in industry and academia are making advances at a rapid pace. The security issues associated with cloud computing, along with new types of potential vulnerabilities, continue to be identified.

7 Identification and Authentication

Determining if a user is authorized to use a voting system includes the distinct steps of identification and authentication. Identification is the act or process in which an entity (e.g., user or system component) provides a unique identity so a system can distinguish the entity from all others. Authentication is the process of establishing confidence in user identities.

Proper voter authentication is required to ensure only eligible voters can cast ballots and a valid voter contributes a single ballot to the final tally. A remote voting system will typically verify credentials it is provided with, and assume the person providing those credentials is the legitimate owner. As credentials may come from the voter's computer rather than from the human voter him or herself, the voter's computer may gain direct, unrestricted access to the voting credentials. The binding between voters and identities, and between identities and credentials, is established through "voter identification."

It is also important, in a remote setting, that the voting system authenticates itself to the voter. This implies that the voter is able to check that she is actually interacting with the legitimate Internet voting service.

7.1 Potential Benefits

Polling place voting typically authenticates voters by having polling place officials interact directly with the human voters. In some cases, voters may be asked for identification or some other authenticator. In Internet voting, strong cryptographic credentials can be used to authenticate voters. In such cases, cryptographic authentication mechanisms make it essentially impossible to trick the system into accepting forged credentials.

7.1.1 Automated Authentication Mechanisms

Hand signature verification generally requires trained election workers to inspect every ballot package returned by voters, matching the signature included with the ballot to a signature specimen on file. While some absentee voting management systems can automate some of the signature comparisons, it is still a moderately resource intensive activity. However, electronic authentication methods can be entirely automated.

7.1.2 Strong Remote Authentication

Currently, remote electronic authentication methods exist which are capable of providing high levels of assurance of a user's claimed identity. Many of these methods are widely deployed in the public and private sectors.

Although the stronger authentication mechanisms are typically used in government, military or corporate environments, they have not been widely deployed to general public. For instance, the federal government's Personal Identity Verification program of the federal government involves distributing smart cards to government employees and contractors for authentication purposes. The Department of Defense's Common Access Card is similar program for military personnel and contractors. However, most citizens of the United States that are not associated with the federal government or military so do not have smart cards. The situation in the United State is different from other countries that have deployed Internet voting systems, such as Estonia, which have smart cards deployed to the vast majority of the general population.

7.2 Properties

Property: Voter Identification

Election authorities and voting systems are able to uniquely identify eligible/registered voters within a particular jurisdiction.

Notes:

Unique identification of voters is necessary to bind eligible voters to digital identities and digital identities with credentials. The credentials are used for voter authentication and enforcing access control rules and keeping records of who did what on the voting system.

Property: Voter Authentication

The voting system verifies the credentials of potential voters before allowing them to perform any authorized actions on the system.

Notes:

The voting system should ensure that voters connecting to the system are eligible to use the system to perform the requested functions (e.g., cast a ballot, update voter registration information). In remote authentication, it is important to understand there is no difference between authentication of voters and authentication of credentials. That is, anybody with access to the voter's credentials is able to impersonate the voter. There is a spectrum of techniques that offer different levels of assurance in remote authentication. For example, 4-digit pins offer lower remote authentication assurance than strong passwords. Higher assurance can be obtained using "two-factor authentication" methods typically involving cryptographic token and a PIN, a password and a biometric, or a time-dependent random number generated by a small hardware device issued to the user. Voting system authentication in the foreseeable future is unlikely to make use

of biometrics, but deployment of some form of two-factor authentication does seem feasible for special populations such as military personnel. For instance, the Department of Defense has distributed the smart card-based Common Access Card (CAC) [43] to nearly all of its military personnel, employees and contractors.

Voter authentication should not compromise the secrecy of the vote. The authentication protocols should not attach easily retrievable or inferable voter identification information to cast ballots. If jurisdictions allow a voting system to attach voter identification information to cast ballots, then this information should be encrypted in such a way that it can only be decrypted under exceptional circumstances.

Property: Administrators/Officials Identification

Election authorities, system administrators, or other individuals with administrative access to voting systems, are uniquely identified by the voting system.

Notes:

Individuals with privileged access to the voting system should be uniquely identified by the voting system. That is, system administrators, election officials, and other with access to voting system should not share accounts or login credentials. This allows for greater accountability of administrative actions performed on the voting system.

Property: Administrators/Officials Authentication

The voting system components verify the credentials of system administrators, election officials, and other election insiders before allowing them to perform any actions, as authorized, on the system components.

Notes:

Voting system administrators and election officials do not require the same privacy protections as voters. Thus, every voting system component should verify the unique identity of the official or administrator before granting them access to the system.

Property: System Component Identification

Each voting system component is identified by the system.

Notes:

Like users, each voting system component should be identified. While some level of unique identification would be necessarily for various

administrative functions for logistical reasons, groups of components that act as one might be identified as part of a collective group. For instance, individual machines in a group of web servers behind a load balancer may all share the same identity for identification and authentication purposes.

Property: System Component Authentication

Users and system components should verify the identities of voting system components before any other interactions with those components.

Notes:

It is important to note that this property applies both to users (e.g., voters, election officials, administrators) connecting to voting system components, as well as voting system components connecting to other components. In both cases, users and voting system components connecting to the voting system should verify they are communicating with the component they intended and not some other computer system impersonating the intended component. In particular, voters should authenticate the voting system they are interacting with, to ensure it is the legitimate voting system.

Property: Non-transferable Credentials

It should be difficult for voting system credential holder to pass his or her credentials to an unauthorized party without detection.

Notes:

Section 7.3 discusses several threats to identification and authentication systems where an attacker convinces a legitimate user to disclose credentials to an unauthorized party. In most cases, this would involve deceiving the legitimate credential holder but could be done with the cooperation of the credential holder (e.g., in the case of vote selling). Credential transfer attacks should be difficult to perform without detection. In this case, difficult may mean the attack does not scale well, or that the threat of punishment if caught is severe enough to deter attacks.

7.3 Threats to Identification and Authentication

7.3.1 Unauthorized Issuance of Credentials

One common threat to identification and authentication systems is that unauthorized parties may be issued credentials they are not eligible for. For instance, an individual may impersonate some other individual and register

in his or her name. Alternatively, an individual who is not eligible to vote in a jurisdiction may register to vote and be issued credentials to vote. These types of threats are very similar to current forms of voter registration fraud.

There continues to be disagreement over the extent and severity of voter registration fraud in the United States. A study of election crimes by the Election Assistance Commission found that while experts agree fraudulent voter registration forms are filled out, most do not believe these fraudulent registrations result in fraudulent votes actually being cast [37].

It is not known how a move to remote electronic voting over the Internet will change the threat environment for these forms of voter registration fraud.

7.3.2 Phishing/Pharming

Phishing and pharming are two related attacks on the Internet today. While the method for conducting the attack differs between the two, the goal of the attacker is the same: to trick users into revealing their credentials on an illegitimate web site that looks like the legitimate site. In the case of phishing, an attacker sets up a fake website and lures users to the site. Attackers use a variety of means to lure users to these websites, but they typically involve registering a website domain name similar to the legitimate web site and sending mass e-mails claiming to be the legitimate website owner but including links to the fake website. Phishing is largely an attack on the user, rather than on any particular piece of equipment. Pharming is a similar attack, except rather than tricking a user into visiting the fake web site, attackers use some sort of computer or network vulnerability to redirect a user from the legitimate website to an illegitimate one without the user's knowledge.

Phishing attacks are very widespread on the Internet, with credentials to financial and social networking sites often being the target of the attacks. According to a Gartner report, five million consumers in the United States lost money to phishing attacks in fiscal year 2008 [38]. Their survey estimated the average consumer loss per successful phishing attack was $351. However, accurate information on the losses associated with phishing is very difficult to collect, and other researchers have questioned the accuracy of this information, claiming that actual losses are much lower [39]. A recent report by the Anti-Phishing Working Group found phishing attacks continue to be a significant problem, with a record number of organizations targeted by phishing attacks in the fourth quarter of 2009 [40].

Phishing and pharming attacks on Internet voting systems could successfully steal voters' credentials, allowing malicious parties to cast votes in place of the legitimate voters. Attackers may also conduct more targeted phishing attacks, sometimes called spear phishing, on election system administrators or election officials, possibly resulting in gaining privileged access to back-end voting system equipment. Because these attacks are just as much attacks on human users as they are on the technical system, they are very difficult to prevent. Phishing attacks in particular require very little resources and technical expertise to conduct, yet can impact a very large number of people. While Section 7.4.5 will discuss a common method for preventing phishing and pharming attacks, its benefits are somewhat limited.

7.3.3 Credential Selling

Some types of credentials are very easy to transfer to another individual. For instance, PINs and passwords can be physically or electronically sent to another individual as part of a vote selling attack, as described in Section 4.3.3 or in attempts to coerce voters, as described in Section 4.3.2. As noted in those sections, it is difficult to estimate the likelihood of such attacks or how motivated potentials attackers would be to conduct these types of attacks. However, depending on the types of credentials used, these attacks could scale fairly well, potentially allowing individuals or organizations to collect large numbers of voters' credentials and cast votes on their behalf.

There are technical measures that could be taken to greatly limit the ability of these attacks to scale, such as using credentials that cannot be easily passed from a voter to another individual. For instance, use of hardware tokens, such as smart cards or one-time password devices, could require a voter and coercer/vote-buyer to exchange a physical device. However, these mechanisms typically come at a higher cost than simple authentications based on passwords or PINs. Biometric characteristics used in conjunction with challenge-response protocols may also be used to make it impossible to transfer a person's credentials to someone else.

7.3.4 Social Engineering

Social engineering is a class of attack where malicious (or curious) individuals manipulate legitimate users of a system into divulging sensitive information, such as login credentials for a system. Phishing and pharming can be considered a type of large-scale, automated social engineering attack, but social engineering attacks could be highly targeted and interactive. For instance, an attacker conducting a social engineering attack could call an election official or system administrator claiming to be from the service provider hosting the voting system and convince the victim to divulge his or her password.

Social engineering is a class of attacks, and the objective of the attacker may not be solely to steal login credentials. The objectives of social engineers can be to obtain any type of sensitive information that may help them conduct an attack.

7.3.5 Cracking/Guessing

Depending on the type of authentication mechanism used and the location of the attacker, a malicious individual may be able to steal authentication credentials with brute force. This is particularly true for authentication mechanisms like passwords or PINs, as well as knowledge-based authentication. For example, a randomly-generated four-digit PIN has ten thousand different possible values, so an attacker has about a 0.5% chance of guessing a PIN after 5 attempts. In the case of user-chosen passwords, people tend to choose dictionary words for passwords, making it easier for attackers to guess or crack a password.

There are a number of methods that system designers can use that can make it very difficult to guess or crack a particular individual's login credentials. However, if a system has a large number of users, it is much more difficult to ensure that none of the users' credentials are cracked or guessed. This may not be a serious concern for voters' credentials, as these attacks do not appear to scale well.

More seriously, individuals with some level of access to the system, such as physical access to voting system equipment or the ability to watch network traffic between voting system components, may be able to use more sophisticated cracking or guessing attacks. This could be the first stage of an attack if the person is some sort of election system insider (e.g., a computer technician at the service provider hosting the system), or it may be done by a remote attacker that has already gained limited access to the voting system equipment. The impact of these attacks can vary. An attacker that successfully guesses or cracks the credentials associated with a privileged account would be able to perform any actions on the system as if they were the legitimate user.

7.3.6 Malicious Software

Malicious software, or malware, on computers of users' connecting to the voting system could steal credentials used to authenticate to the system. For instance, a common example of malware used by attackers is a keylogger. Keyloggers can record everything that users type on their keyboards. Therefore, it is capable of capturing authentication credentials like

passwords and PINs very easily and can pass them to a remote attacker over an Internet connection. Keylogging functionality is common in malicious code associated with botnets, which were previously discussed in Section 5.3.4.

As was the case with credential guessing and cracking, the impact of these attacks can vary. Attackers that steal the credentials associated with a voter's or administrator's account would be able to perform any actions on the system as if they were the legitimate user. This means that attackers may be able to cast votes in place of a voter, or even perform administrative functions if they are able to get malicious software on a computer used for system or election administration.

7.3.7 Insiders/Credential Issuers

If voting credentials are issued by a particular entity, such as the election officials giving voters usernames and passwords, these insiders have access to all the credentials used for casting ballots. Such an individual may use these credentials to cast votes in the name of voters (for example for voters who did not cast ballots until a couple of minutes before the polls close).

To avoid such scenarios, it may be best to have the voter choosing their own credentials, with insiders never having access to these credentials in clear text, but at the same time being able to check that the voter have knowledge/access to them. For example, if electronic signatures are produced using smartcards, the private keys have to be generated inside the smartcards and it should be impossible to read the clear text private keys, but only to use it to sign messages.

7.4 Current and Emerging Technical Approaches

7.4.1 Passwords and PINs

Passwords and PINs remain two of the most common methods for electronic authentication, largely because they are relatively cheap and easy to deploy. Most people use passwords to log into their computers and web-based accounts, including e-mail, social networking sites, and financial sites. Passwords and PINs are typically user-generated, although in some cases organizations or systems will send users pre-generated passwords initially and ask the users to change them when they are first used.

However, passwords and PINs have significant security disadvantages compared to other types of authentication mechanisms. User-generated passwords can often be easily cracked if the attackers have sufficient

information, and they are easily stolen by malware or phishing sites. For these reasons, many organizations are moving away from just using passwords for authentication. For instance, the federal government requires some form of two-factor authentication for remote access to government systems [41], and some financial institutions have begun using two-factor authentication for online banking.

7.4.2 One-time Passwords

One-time passwords are a common method for deploying two-factor authentication. A one-time password is a password that is only valid for a single transaction and usually a short period of time. In most cases, systems using one-time passwords still use user-generated, memorized passwords, with the one-time password adding an additional layer of authentication.

The difficulty of one-time passwords is organizations need a method for securely distributing these one-time use passwords to their users. This is typically done one of two ways: distributing trusted hardware devices to users or sending them on-demand through a secondary channel such as a cell phone.

Many organizations in the public and private sectors use trusted hardware devices to generate one-time passwords. Organizations must keep track of which users are given what one-time password device. These devices typically continuously generate random codes at regular intervals, such as every 30 seconds. When a user attempts to log into a system, he or she typically must enter both a memorized password in addition to the random code on the one-time password device at that particular moment. The use of a hardware device increases the cost of the system, and the device must be securely distributed to users either in-person, or by some other physical means, and may be lost by users.

Alternatively, one-time passwords can be sent or generated on devices that users already have. For instance, a user may have a piece of software on his or her mobile phone that generates one-time passwords in a similar manner as the hardware device described above. Or an organization may have the mobile phone number for a user and send one-time passwords as text messages on-demand to users attempting to authenticate to the system.

The use of one-time password devices can provide some protection against the threats described in Section 7.3 with some important limitations. Because these passwords are constantly-changing strings, they are very difficult to guess or crack, so malware and phishing sites cannot easily collect large numbers of passwords for later use. However, more

sophisticated attacks can be conducted by malware and phishing sites. If an attacker can capture a one-time password and use it before the user sends it to the legitimate system, the attacker can successfully impersonate that user. This can be accomplished with phishing websites that immediately connect to the legitimate website when a victim enters his or her information, or with malware that passes credentials to an attack in real-time. Both of these types of attacks have been used to attack online banking sites and do not require particularly high-levels of technical expertise. Some malware packages commercially available, as were discussed in Section 5.3.4, include the ability the conduct these types of attacks [42].

7.4.3 Cryptographic Authentication

There are various forms of cryptographic authentication that can be done remotely using cryptographic tokens. These tokens are used in a cryptographic protocol whereby the user proves to the organization authenticating them that he or she has possession of the cryptographic token without having to directly present the token. Authenticating using cryptographic tokens can have very strong security properties and can be implemented such that they are very difficult to crack or steal via phishing.

Cryptographic tokens can be software or hardware based. The difference is whether the cryptographic token is stored on a trusted hardware device, such as a smart card, or whether it is merely a file or piece of software on a computer, mobile phone, tablet PC, or other general-purpose computing device. Software-based cryptographic tokens are vulnerable to theft or tampering but do not require any special hardware. Hardware-based tokens provide greater security.

Hardware based cryptographic tokens often take the form of a smart card. Smart cards are used by many organizations in the public and private sectors for authentication purposes. The Department of Defense has distributed the smart card-based Common Access Card (CAC) [43] to nearly all of its military personnel, employees and contractors. The United States federal government is in the process of implementing a similar program, the Personal Identity Verification card [44], for civilian employees and contractors. In lieu of issuing credentials specifically for voting, UOCAVA voting systems should consider leveraging strong credentials that are already deployed. For example, the country of Estonia, which has a smart card-based national identification card, performed voter authentication in its Internet voting system using the electronic credentials found on the national identification card [45].

Cryptographic authentication is also well-suited for allowing components of the voting system to authenticate to one another. There are a number of networking protocols that allow one component to authenticate to other components. Transport Layer Security (TLS), for example, is a commonly used protocol on the Internet to encrypt traffic between a website and a user's computer and to authenticate the website to the user's system. TLS can also be used to authenticate the client connecting to a server. While client authentication is relatively uncommon in typical e-commerce transactions, it is often used in higher security systems.

7.4.4 Biometrics

Biometrics are methods for identifying and authenticating individuals based on one or more behavioral or physical traits. Commonly cited biometrics used for authentication purposes include fingerprints, iris recognition, and hand/palm geometry. Biometric authentication can offer high degrees of security depending on the quality of the biometric readers used in the system. However, biometrics are typically used for local authenticating, meaning the user authenticating to a system is in the same physical location as the system. This is because biometrics must be measured by a trusted reader, such as a fingerprint scanner.

Some biometrics are better suited for remote authentication, such as speaker verification. Speaker verification authenticates a user based on their speech patterns. This should not be confused with speech recognition, which recognizes the spoken words, regardless of the identity of the person speaking. Currently, speaker verification methods provide significantly higher error rates than other biometrics [48], but it is an active research area with a number of commercially-available systems. Speaker verification may be suitable as a secondary authentication method or, with improvements to technology, a primary method.

7.4.5 Phishing Filters

Many modern web browsers and anti-malware software distributions include some type of protection against phishing attacks. These approaches typically involve some combination of whitelisting websites known to be safe, blacklisting websites known to be fraudulent, and, in some cases, using heuristics for all other websites in an attempt to estimate the risk of phishing (e.g., a URL using an IP address instead of a domain name). When a user visits a website that is deemed unsafe, the phishing filter displays either a passive or active warning. An example of a passive warning in a browser is a short warning message, such as "Suspicious Website," placed next to the address bar, but does not require any user input to ignore. An active

warning interrupts the user and requires some sort of input by the user to ignore the warning. For instance, before displaying the phishing website, a browser may display a warning page telling the user the website is a suspected phishing site and asking the user if he or she would like to proceed to the page anyway.

However, the effectiveness of phishing filters is limited by their ability to identify fraudulent websites and how well users heed the warnings. A 2006 study by the Mozilla Project found that between 66% and 82% of fraudulent web sites were detected by the phishing filters used in two popular web browsers [46]. A limited number of usability studies have been done on phishing filters. A 2008 study found that 90% of Internet Explorer 7 users ignored passive warnings from the browser's phishing filter, with that percentage improving to 45% when an active warning was displayed [47]. However, new designs for phishing warnings may be able to improve those rates.

7.4.6 Security Awareness and Training

Many of the threats described in this section are attacks on users, rather than on the voting system components. In some cases, users are not aware of the security threats faced by a system, or what actions might pose a security risk. Security awareness presentations and materials can educate users about these threats in the hopes that they will be less likely to fall to a phishing or social engineering attack and more likely to use safe computing behaviors. Security training can educate users about relevant security skills and competencies that are necessary for them to conduct their jobs effectively and safely.

Jurisdictions should develop security awareness and training programs for election staff. They may also distribute security awareness materials to voters highlighting recommended security practices and potential threats.

7.5 Open issues

Unlike some the other topics areas described in this document, many of the security challenges associated with identification and authentication of users and voters have commercially-available technical solutions. However, there remain logistical concerns, as well as concerns over the cost of implementing some of these solutions.

Deployment of strong authentication credentials for voters is an issue that would likely be difficult for jurisdictions to manage at this time and could be difficult for the foreseeable future. The authentication methods providing the

highest levels of assurance of users' identities involve specialized hardware devices that increase the cost of the system and complicate deployment. It may be advantageous for jurisdictions to rely on already deployed authentication credentials, such as the DoD's Common Access Card and the federal government's Personal Identity Verification card, which are already deployed to many overseas voters. However, it is not known if these credentials could be used for voter authentication, or what would be done with the hundreds of thousands, if not millions, of overseas voters that do not have one of these electronic credentials. This could change over time; as more people conduct electronic transactions in their daily lives, it may become increasingly important for all citizens to have strong electronic credentials.

The threat of phishing and social engineering attacks are logistically, and even technically, difficult to mitigate. Cryptographic tokens can provide some protection against phishing attacks, but many other authentication techniques can still fall to variations of phishing and social engineering attacks. Mitigating phishing attacks will likely require a combination of technical controls, possibly in the form of cryptographic tokens, and users better able to understand risks and identify risky behavior.

8 Conclusions

This paper identified desirable security properties of remote electronic voting systems, threats of voting over the Internet from personally-owned devices, and current and emerging technologies that may be able to mitigate some of those threats. Based on the capabilities of current computer security and voting technologies, the following three issues remain to be significant challenges faced by remote electronic voting systems.

First, remote electronic absentee voting from personally-owned devices face a variety of potential attacks on voters and voters' personal computers. Since the voter's personal computer is outside the control of election officials, it is extremely difficult to protect against software attacks that could violate ballot secrecy or integrity or steal a voter's authentication credentials. These are serious threats that are already commonplace on the Internet today.

Second, remote electronic voter authentication is a difficult problem. Current technology does offer solutions for highly-secure voter authentication methods, but these may be difficult or expensive to deploy. Personally-owned computers may not be able to interface with these methods, such as having the necessary smart card readers for cryptographic authentication using Common Access Cards or Personal Identity Verification cards.

Third, it is not clear that remote electronic absentee voting systems can offer a comparable level of auditability to polling place systems. Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution.

Many of the current and emerging technologies identified in this report are areas with active research and development. Pilot projects should be encouraged, including those involving the use of voting-specific cryptographic protocols, such as the Helios voting system [23]. Emerging trends and developments in these areas should continue to be studied and monitored.

References

[1] Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), (as modified by the National Defense Authorization Act for FY 2005). http://www.fvap.gov/resources/media/uocavalaw.pdf

[2] 107th U.S. Congress (October 29, 2002). "Help America Vote Act of 2002 (Pub.L. 107-252)." U.S. Government Printing Office.

[3] National Institute of Standards and Technology Interagency Report: 7551, *A Threat Analysis on UOCAVA Voting Systems*, December 2008.

[4] Draft National Institute of Standards and Technology Interagency Report 7682, *Information System Security Best Practices for UOCAVA Supporting Systems*, April 2010.

[5] Draft National Institute of Standards and Technology Interagency Report 7711, *Security Best Practices for the Electronic Transmission fo Election Materials*, June 2010.

[6] U.S. Election Assistance Commission (2010, August 10). UOCAVA Pilot Program Testing Requirements, August 10, 2010. Accessed February 16, 2011 at http://www.eac.gov/testing_and_certification/eacs_work_with_military_and_overseas_voting.aspx

[7] EAC (2010, April 26). Report to Congress on EAC's Efforts to Establish Guidelines for Remote Electronic Absentee Voting Systems. Accessed May 10, 2010 at http://www.eac.gov/program-areas/voting-systems/docs/04-26-10-move-act-report-to-congress-final-congress/

[8] M. Volkamer and R. Vogt. Basic set of security requirements for Online Voting Products. Common Criteria Protection Profile BSI-CC-PP-0037, Bundesamt für Sicherheit in der Informationstechnik, Bonn, April 2008.

[9] Council of Europe. Legal, Operational, and Technical Standards for E-Voting. Recommendation Rec(2004)11, September 2004.

[10] Federal Voting Assistance Program. *Secure Electronic Registration and Voting Experiment. Threat Risk Assessment- Phase 3*. March 23, 2004.

[11] McConnell, Steven (2004), Code Complete (Second Edition), Microsoft Press.

[12] Georgia Tech Information Security Center (2008). *Emerging Cyber Threats Report for 2009.* Accessed May 15, 2010 at http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf

[13] US-CERT (2008, May 16). *Technical Cyber Security Alert TA08-137A: Debian/Ubuntu OpenSSL Random Number Generator Vulnerability*. Accessed May 15, 2010 at http://www.us-cert.gov/cas/techalerts/TA08-137A.html

[14] Symantec (2010, April). *Symantec Global Internet Security Threat Report: Tends for 2009*. Accessed May 15, 2010 at http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

[15] Dierks, T. and Rescorla, E., *The TLS Protocol Version 1.2*, Internet Engineering Task Force, Request for Comment 5246, August 2008, http://tools.ietf.org/html/rfc5246

[16] Atsushi Fujioka, Tatsuaki Okamoto, and Kazui Ohta. A Practical Secret Voting Scheme for Large Scale Elections. In Jennifer Seberry and Yuliang Zheng, editors, *Advances in Cryptology - AUSCRYPT '92*, volume 718 of *Lecture Notes in Computer Science*, pages 244--251, Berlin, 1993. Springer-Verlag.

[17] Rene Peralta. Issues, non-issues and cryptographic tools for Internet-based voting. In *Secure Electronic Voting* (Boston, 2003), Dimitris A. Gritzalis, editor. Kluwer Academic Publishers, pp. 153-164.

[18] Lorrie Faith Cranor and Ron K. Cytron, Sensus: A Security-Conscious Electronic Polling System for the Internet. *Proceedings of the Hawai`i International Conference on System Sciences* , January 7-10, 1997, Wailea, Hawaii, USA.

[19] J. Benaloh and D. Tuinstra. Receipt-Free Secret-Ballot Elections. *Proceedings of the 26th ACM Symposium on Theory of Computing*. Montreal, PQ. May 1994. (New York, USA: ACM 1994), pp. 544—553.

[20] Ronald Cramer, Rosario Gennaro, and Berry Schoenmakers. *A secure and optimally efficient multi-authority election scheme*. European Transactions on Telecommunications, 8:481-489, 1997.

[21] Premiere Election Solutions (2008, August 19). *Product Advisory Notice*. Accessed May 15, 2010 at http://www.sos.state.oh.us/sos/upload/news/20081001c.pdf

[22] Fink, R.A.; Sherman, A.T.; Carback, R.; , "TPM Meets DRE: Reducing the Trust Base for Electronic Voting Using Trusted Platform Modules," *Information Forensics and Security, IEEE Transactions on* , vol.4, no.4, pp.628-637, Dec. 2009.

[23] Ben Adida, Olivier de Marneffe, Olivier Pereira, and Jean-Jacques Quisquater. Electing a University President Using Open-Audit Voting: Analysis of Real-World Use of Helios, In D. Jefferson, J.L. Hall, T. Moran, editor(s), *Electronic Voting Technology Workshop/Workshop on Trustworthy Elections*, Usenix, August 2009.

[24] Nathanael Paul, Andrew S. Tanenbaum, "The Design of a Trustworthy Voting System," Computer Security Applications Conference, Annual, pp. 507-517, 2009 Annual Computer Security Applications Conference, 2009.

[25] Common Criteria for Information Security Evaluation. Part 3: Security assurance components. Version 3.1, Rev. 3, July 2009.

[26] Patrick Peterson, Henry Stern. "Botnets Gone Wild! Captured, Observed, Unraveled, Exterminated." Presented at RSA 2010, San Francisco, CA, March 1-5, 2010.

[27] Testimony of Bob Carey, Director of FVAP. (2010) EAC Public Meeting, Dec. 3 2009. Accessed April 5, 2010 at http://www.eac.gov/public_meeting_12032010/

[28] United States Postal Service (2007). *2007 Comprehensive Statement*. Accessed March 17, 2010 at http://www.usps.com/strategicplanning/cs07/chpt5_001.htm

[29] Alvarez, R. Michael (2005, October 5). “Precinct Voting Denial of Service”, *NIST Threats to Voting Systems Workshop*. Accessed March 17, 2010 at http://vote.nist.gov/threats/papers/precinct_dos.pdf

[30] Davis, Joshua (2007, August 21). “Hackers Take Down the Most Wired Country in Europe” *Wired Magazine*. Accessed March 5, 2010 at http://www.wired.com/politics/security/magazine/15-09/ff_estonia

[31] Markoff, John (2008, August 13). "Before the Gunfire, Cyberattacks" *The New York Times*. Accessed March 5, 2010 at http://www.nytimes.com/2008/08/13/technology/13cyber.html

[32] Vixie, Paul, Sneeringer, Gerry, and Mark Schleifer (2002, November 24). Events of 21-Oct-2002." Accessed March 5, 2010 at http://d.root-servers.org/october21.txt

[33] Internet Corporation for Assigned Names and Numbers. "Factsheet-Root server attack on 6 February 2007." Accessed March 5, 2010 at http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf

[34] Worthham, Jenna, and Andrew E. Kramer (2009, August 7) "Professor Main Target of Assault on Twitter" *The New York Times*. Accessed March 5, 2010 at http://www.nytimes.com/2009/08/08/technology/internet/08twitter.html

[35] D. J. Bernstein and Eric Schenk (1996). *SYN Cookies*. 1996. Accessed May 15, 2010 at http://cr.yp.to/syncookies.html

[36] Mell, Peter and Tim Grance (2009, October 7), *The NIST Definition of Cloud Computing.* Accessed March 2, 2010 at http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[37] U.S. Election Assistance Commission (2006, December). *Election Crimes: An Initial Review and Recommendations for Future Study*. Accessed June 15, 2010 at http://www.eac.gov/assets/1/workflow_staging/Page/57.PDF

[38] Gartner (2009, April 14). *Gartner Says Number of Phishing Attacks on U.S. Consumers Increased 40 Percent in 2008*. Accessed March 5, 2010 at http://www.gartner.com/it/page.jsp?id=936913

[39] Cormac Herley and Dinei Florencio, A Profitless Endeavor: Phishing as Tragedy of the Commons, in *Proc. New Security Paradigms Workshop*, Association for Computing Machinery, Inc., September 2008.

[40] Anti-Phishing Working Group (2009). *Phishing Activity Trends Report, 4th Quarter 2009*. Accessed March 5, 2010 at http://www.antiphishing.org/reports/apwg_report_Q4_2009.pdf

[41] Office of Management and Budget (2006, June 23). *OMB Memo M06-16*. Accessed March 5, 2010 at http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf

[42] McAfee Labs (2009). *2010 Threat Predictions*. Accessed April 13, 2010 at http://www.mcafee.com/us/local_content/white_papers/7985rpt_labs_threat_predict_1209_v2.pdf

[43] Department of Defense. *Common Access Card.* Accessed March 5, 2010 at http://www.cac.mil/

[44] National Institute of Standards and Technology (2009). *About Personal Identity Verification (PIV) of Federal Employees and Contractors.* Accessed March 5, 2010 at http://csrc.nist.gov/groups/SNS/piv/

[45] Estonian National Electoral Committee. *Internet voting in Estonia*. Accessed March 5, 2010 at http://www.vvk.ee/public/dok/Internet_Voting_in_Estonia.pdf

[46] Mozilla Foundation (2006, November 14). *Firefox 2 Phishing Protection Effectiveness Testing.* Accessed April 5, 2010 at http://www.mozilla.org/security/phishing-test.html

[47] S. Egelman, L. Cranor, and J. Hong. You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings. CHI '08: Proceedings of the SIGCHI conference on Human Factors in Computing Systems. April 2008.

[48] National Institute of Standards and Technology (2008, August). *The 2008 NIST Speaker Recognition Evaluation Results.* Accessed May 5, 2010 at http://www.itl.nist.gov/iad/mig/tests/sre/2008/official_results/index.html

Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting

Scantegrity is a security enhancement for any optical scan voting system. It lets voters verify that their ballots were correctly recorded and counted, but doesn't change how voters mark their ballots.

David Chaum

Aleks Essex
University of Ottawa

Richard Carback and Alan Sherman
University of Maryland, Baltimore County

Jeremy Clark
University of Waterloo

Stefan Popoveniuc and Poorvi Vora
The George Washington University

Voter confidence in the US electoral process is eroding as a steady stream of reports continue to expose fundamental security flaws in certified electronic voting machines.[1,2] Similar voting technology is used outside of the US, and resistance to electronic voting has spread to other democracies. Although proposals such as stricter design standards, more open systems (preferably open source), and independent verification methods (such as paper audit trails) are improvements, they don't go far enough. In any voting system, with or without an electronic component, the core security problem is *chain of custody*. An attacker who breaks chain of custody could stuff the ballot box, delete or switch votes, or add votes to contests that the voter left empty. Whether the attacker accomplishes this by inserting malicious code or altering paper ballots, such attacks go undetected even with a manual vote recount.

Recently proposed end-to-end (E2E) verification voting systems have focused on minimizing voting systems' reliance on chain of custody.[3] These E2E systems typically provide cryptographic checks indicating that ballots have been recorded as cast and tallied as recorded. Voters can check that their votes are recorded accurately using a receipt, and any observer can verify that the tally is correctly constructed, all without compromising ballot secrecy. In these systems, any chain-of-custody break causes a detectable alteration of the public record. In particular, erroneous voting machine software or voting machine malfunction doesn't dilute the voting systems' integrity. However, using these systems in real elections has been a challenge. They typically require a special type of ballot format—for example, Punch-scan ballots[4] require two sheets of paper, and Prêt à Voter ballots[5] randomize candidate name order.

The Scantegrity voting system combines E2E systems' cryptographic ideas with the familiarity of a widely used vote-counting system. It thus provides the strong security guarantees of E2E systems but is unobtrusive to the voter, has a minimal cost for wide-scale deployment, and doesn't interfere with existing procedural requirements such as paper audit trails and manual recounts. Scantegrity is designed for use with optical scan voting systems, which are the most widely used election technology in the US and are being adopted in other countries as well.[6] Scantegrity can be readily deployed in precincts with existing optical scan systems because it adds minimal requirements to the underlying optical scan process and doesn't introduce any new polling place equipment. It only requires extra information to be printed on the ballots during production and system access to the raw scan results after the election. In summary, Scantegrity minimally impacts election procedures and is the first independent E2E verification mechanism that preserves optical scan as the underlying voting system and doesn't interfere with a manual recount.

Independent E2E verification voting systems

E2E systems, sometimes called receipt-based or universally verifiable voting systems, don't derive security from any specific type of voting equipment. Instead, they generally produce an encrypted representation of

 PUBLISHED BY THE IEEE COMPUTER SOCIETY ■ 1540-7993/08/$25.00 © 2008 IEEE ■ IEEE SECURITY & PRIVACY

ballot choices that functions as a receipt. This receipt doesn't reveal the voter's identity or choices, so the voter can take home a signed or stamped copy of his or her receipt. Election officials publicly post the receipts of all the ballots they received, and voters can check this record to see that their ballot was included and is unmodified. If a voter's receipt doesn't appear or was modified, the signature or stamp on the receipt gives the voter proof of a discrepancy that he or she can use to dispute the record.

Election officials can only decrypt the receipts to recover the final tally by using a method that hides which decrypted ballots correspond to which receipts. They then perform a mandatory audit to prove mathematically that the public record was decrypted properly and that the votes were unmodified—whether by a software error, the election officials, a hacker, or some other entity. Any independent party can author the software used to verify the election outcome using a public specification. Under this model, we expect that several independent entities will make their software tool version freely available to the public, mitigating the issue of software error.

Other E2E systems include VoteHere's Mark-Pledge,[7,8] Votegrity,[9] Punchscan,[4] Prêt à Voter,[5] and Voter Initiated Auditing.[10] Scantegrity is closely related to Punchscan, but unlike its predecessors, it can also serve as an add-on to existing voting technology without interfering with the underlying system's tabulation procedures or paper audit trails. It also uses a new, simpler mechanism to replace the basic vote tallying mechanism of other E2E schemes.

Voter experience

The voter experience in Scantegrity is identical to that of regular optical scan systems (that is, the voter marks the optical scan ballot and feeds it into an optical precinct scanner), except the voter can take home a privacy-preserving receipt. To create the receipt, a voter tears off a perforated corner of the ballot, called a *ballot chit*, that contains a serial number. In addition, as Figure 1 shows, the voter writes down the randomly assigned code letter listed next to the selected candidate. Note that in the ballot in Figure 1, the letter A is beside Bob's name, but it might be beside Alice's name on other ballots. Thus, knowing that someone voted for a particular code letter doesn't tell you which candidate that person voted for.

After the underlying optical scan system tallies the election results, election officials post a public record containing the Scantegrity serial numbers and chosen code letters of all the scanned ballots, but not the candidate associated with the letter on each ballot. Voters can retrieve this public record, look up their serial number, and verify that the code letters they wrote match those in the posted record. Voters can also make a copy of the receipt and give it to third parties, who can also check the public record. The more receipts checked, the higher the chance of detecting a problem with the public record.[11]

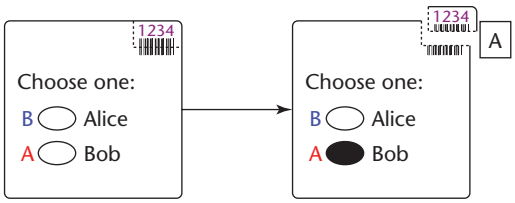


Figure 1. The Scantegrity ballot. Scantegrity uses an optical scan ballot with randomly assigned code letters next to each choice. The perforated chit in the corner contains a serial number written in human- and computer-readable forms.

Correct letters indicate to voters that the officials properly scanned and recorded their votes. However, if the public record contains a letter that's different from what a voter recorded, the voter can challenge the record through a dispute-resolution process.

Dial "0" for independent verification

Anyone can use the public record to verify the tally—that is, that the results were counted as recorded. Tally verification is challenging because the system must not directly reveal the links between code letter and candidate to preserve ballot secrecy.

Although Scantegrity isn't the first system to provide counted-as-recorded integrity verification,[4,5,7–9] its solution is the simplest. The importance of solution simplicity can't be overemphasized in voting—it lets the widest possible audience understand how the voting system works.

Some E2E solutions use a mix network[12] to create an anonymous but verifiable link between receipt and vote. The mix network applies a cryptographic operation at each node to obscure the path of messages through the network. This is especially important for identifiable (that is, unique) data such as email messages. Some E2E systems provide encrypted information on the ballot receipt (this information is sometimes called an "onion") to let the mix network perform the correct cryptographic operations to count the vote correctly. Punchscan, Scantegrity's direct ancestor, uses a simplified two-stage mix network with efficient cryptographic operations. It also doesn't use an onion on the ballot.

Election data doesn't necessarily need to be explicitly encrypted. Under the familiar plurality voting system (also known as "first-past-the-post"), voters express their intent by making a mark beside their chosen candidate. A cast ballot therefore can be ex-

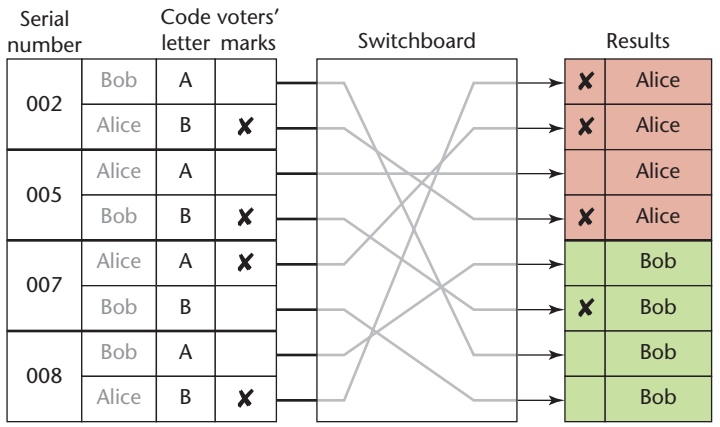


Figure 2. The switchboard. Marks beside code letters are routed to marks beside candidates using a random and obliviously generated circuit-switched network.

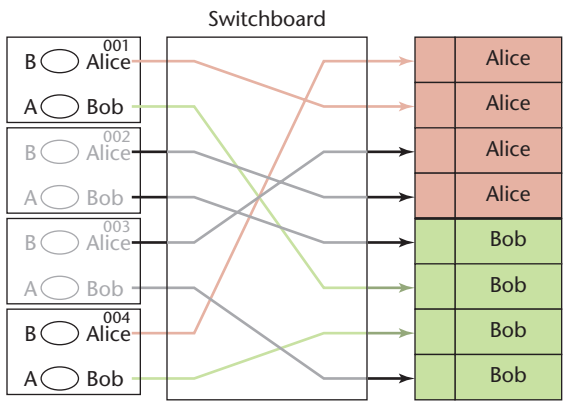


Figure 3. Ballot printing audit performed before an election. The figure shows revealed ballots 001 and 004, the association of code letters, and their connections through the switchboard. This information is made publicly available, and any independent party can see a mark for Alice or Bob would have been correctly registered as a vote for Alice or Bob, respectively. Once revealed, these ballots aren't used in the election.

pressed in terms of a specific collection of marked or unmarked regions. If treated individually, the states of these markable regions aren't unique, so they don't need to be encrypted as they pass through an anonymizing network. Instead of using a mix network architecture, we achieve the same anonymity properties through a simpler process—a secret permutation of the states of the markable regions (akin to shuffling a deck of cards). Thus, Scantegrity uses the permutation to recover the vote while hiding the link between serial number and vote.

The *switchboard* (see Figure 2) is a collection of circuits established between specific markable regions on ballots (marked or not marked) and a particular candidate (voted for or not voted for). The *trustee workstation* transmits the state of each markable region on each ballot in the election through the switchboard to votes for the corresponding candidates in the election results.

Finally, the public must be able to verify independently that marks are being transmitted to the correct candidate without exposing both of the circuit's end points (receipt and vote).

Auditing the switchboard

To ensure voter confidence in the switchboard's ability to produce a correct tally, Scantegrity must reveal some information for verification purposes. Initially, when election trustees create the ballots and switchboard, they commit to this secret information by using a cryptographically secure bit-commitment scheme.[4,13]

Before the election, election officials generate and publish these commitments, letting independent entities verify that no one could have simply "cooked up" the secret data revealed later on during the audit process. The verification requires publicly revealing some secret data and verifying its correctness against the committed data. We reveal secret information in two ways: reveal the full secret and then discard it from use in the election, or reveal partial information that's sufficient for checking, but that doesn't reveal anything about the secret.

Figure 3 illustrates the first technique, which auditors use to verify the correctness of the association between code letter and candidate in the switchboard. Before the election, auditors randomly choose half of the ballots to be revealed publicly, along with their serial numbers and connections through the switchboard. Those performing this printing audit can ensure that the path through the switchboard for each candidate on each of the revealed ballots leads to a vote for the correct candidate in the results. They then destroy these ballots. If they chose the ballots fairly and randomly, the public has a high level of assurance that the remaining sealed ballots are printed and routed correctly. Voters can also audit the printing themselves by keeping a ballot they receive once it's marked as "spoilt."

After the polls close, we use the second technique (illustrated in Figure 4) to audit the switchboard. If we segment the switchboard into two randomly generated circuit-switched networks, revealing a link in one of the networks doesn't reveal the full connection. Voters' marks travel through the first network and are recorded in an intermediary location. The marks in the intermediary position continue through the second network to their final place in the results table. For each intermediary position, auditors challenge the election trustees to reveal either the link to it through the first network or the

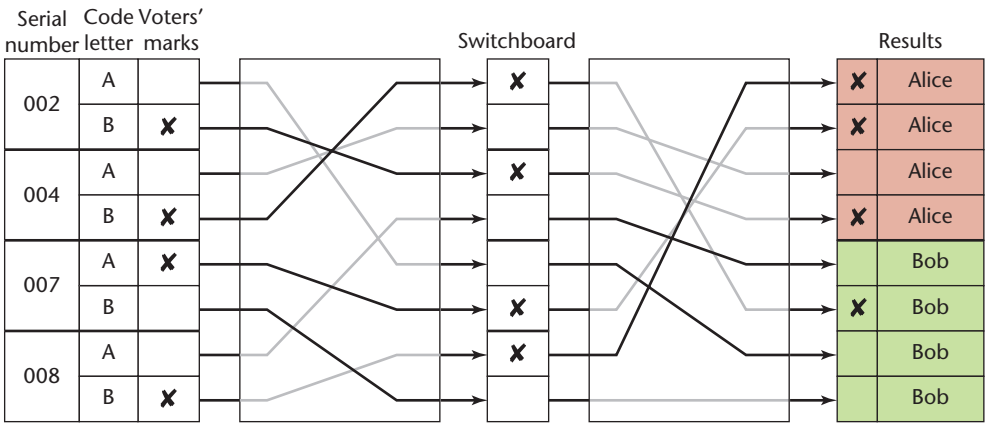


Figure 4. Mark audit performed after the election. Ballot 002 shows a mark for the candidate with code letter B and that this mark was correctly recorded in the intermediate position. Likewise, the first vote for Alice in the results table was correctly copied from the intermediary position. Knowing only one link doesn't reveal the connection between code letter and candidate, preserving the receipt's privacy.

link from it through the second network, but never both. Thus, the connection between a recorded receipt and its position in the final results table is never revealed. For each of these links, anyone can publicly verify that a mark (or absence of mark) traveled through the link unchanged. In this way, observers can be assured that the remaining secret links also routed marks correctly. To increase the audit's statistical certainty, trustees may be mandated to use multiple instances of the switchboard with different random links.

These print and mark audits, in conjunction with the receipt check, provide the verification process's end-to-end nature: integrity is ensured from ballot printing through to the final tally.

Although these audits are conceptually simple to perform, any nontrivial-sized election would warrant the use of a software audit tool to perform these repetitive checks quickly. The software tool is intended to be open source, exceptionally easy to use, and universally available to anyone for free. Concerned parties can code their own independent version following a published specification.

System architecture

Figure 5 shows how Scantegrity interfaces with the optical scan election process. The election authority—a collection of election trustees—uses a workstation on three separate occasions to compute all the information Scantegrity needs. This set of meetings represents Scantegrity's three core processes:

- Before the ballots are printed, election trustees use the workstation to compute the serial number and code letters to add to the optical scan ballots as well as generate the switchboard connections. They cryptographically commit to this (secret) data and post the commitments publicly.
- After the marked ballots are scanned on election day, election trustees give the *electronic ballot images* (EBIs) to the Scantegrity system. They post the code letters and corresponding voter-created marks made on each ballot to the public record, which voters can compare to their receipts.
- After the election results are tabulated and published, auditors challenge the election trustees to open one half of the switchboard for each marking region to prove that they counted the ballots faithfully.

Using a workstation, the officials can regenerate all the data needed for each meeting from their passphrases, preventing the need to physically store any sensitive election data. Trustees secure the workstation by removing any persistent data storage and boot the open source operating system and software from a self-contained medium that can undergo attestation by anyone present both before and after its use.[4] Fortifying the workstation protects voter privacy; the election's integrity is unconditional, and thus independent of the workstation's trustworthiness.

Resolving disputes

Because there's no control over what voters write on their receipt chits, they could write the wrong code letter. Then, when checking the official record, the voter will find a discrepancy. Officials need a voter-verifiable method to determine whether the discrepancy is the result of an incorrectly written letter or a scanner error, or malfeasance.

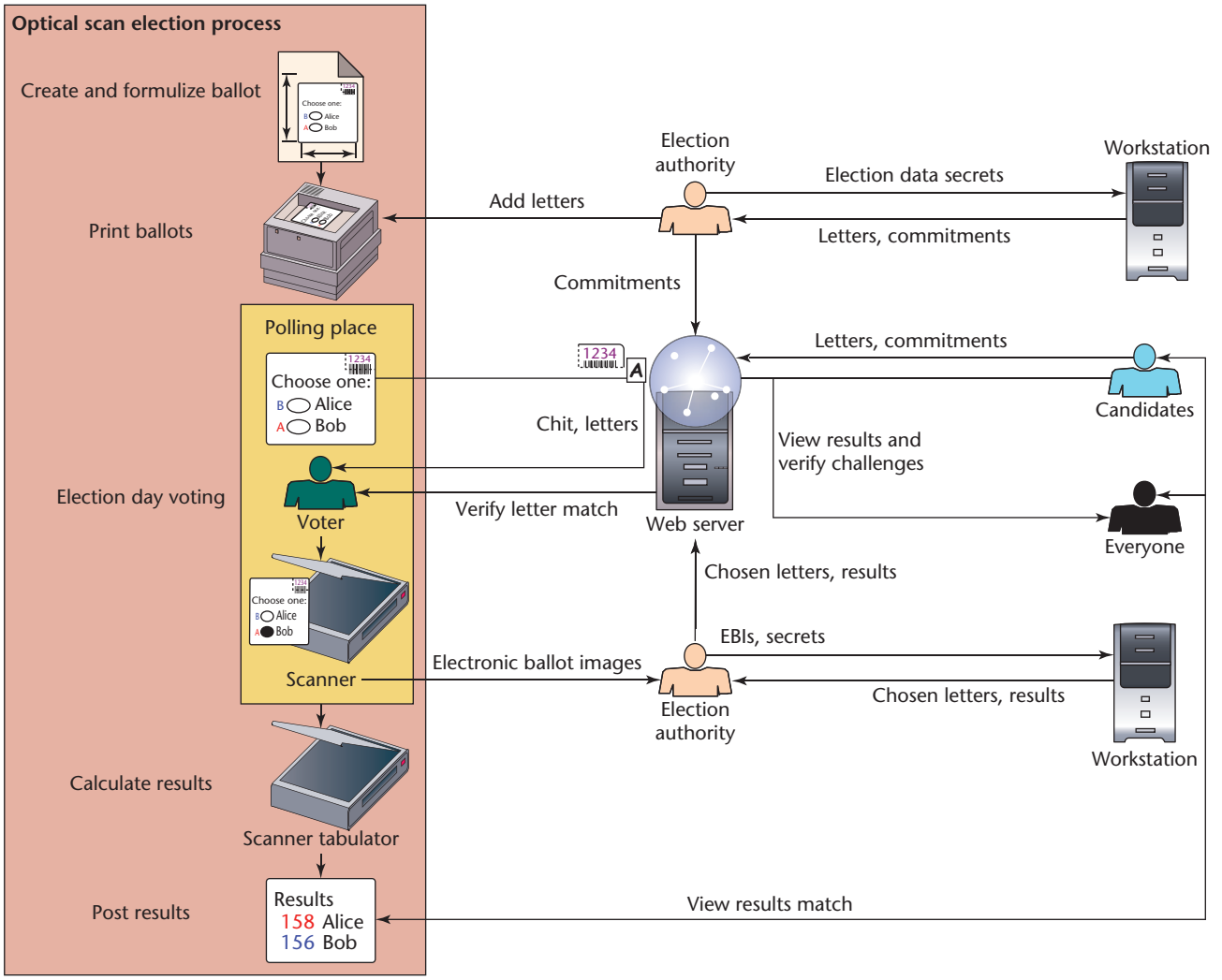


Figure 5. Overall election process with Scantegrity. Scantegrity inserts itself into the traditional optical scan election process, creating a separate mechanism for independent universal verification of election results. Election trustees use a workstation to create letters and add them to the ballots. After voting, they use the workstation again, reading the electronic ballot images (EBIs) to interpret marks on each ballot and post the chosen letters. They use the workstation a third time to respond to audit challenges, and everyone can check the responses to be sure the results tallied properly.

Figure 6 illustrates the receipt-dispute-resolution protocol. This is a two-step process that preserves ballot secrecy. First, an election official retrieves the original ballot and puts it in a privacy sleeve that reveals only the ballot's serial number, not its contents. If necessary, forensic analysis could be performed to match the chit fibers to the ballot.

Second, officials must show the code letter marked on the ballot without revealing the corresponding candidate. The official observably moves the ballot to a second privacy sleeve that will show the marks for the disputed race but not the serial number. The official notes the marked letter's position and drops the sleeve into an empty lottery-style hopper. The official then collects a set of dummy ballots with the same code letter marked for each of the other candidates, puts them in similar privacy sleeves, and drops them into the hopper.

After tumbling the hopper, the election official retrieves each privacy sleeve envelope and places it in plain view. Because the ballot was already matched to the chit, it will be in this collection. Thus, the election officials have successfully demonstrated the code letter voted for without revealing the candidate voted for. Anyone can then compare the single code letter (marked on all the shown ballots) to the public record. After all disputes are settled, everyone can assume that the public record of chosen letters is correct, and that

no ballots were lost. If necessary, officials recompute the results from the corrected public record.

We've developed a more efficient dispute-resolution procedure that doesn't require physical interaction or forensic analysis.[14]

Implementation

We created a Java-based software implementation and merged it with the open source Punchscan codebase. Our software is general enough to author ballots of both styles, even allowing an election to mix Punchscan ballots with Scantegrity ballots. The software takes a ballot layout in PDF format as input and produces a multiple-page PDF document of the ballot collection with letters and serial numbers inserted.

We tested our implementation on an Intel P4 1.73 GHz laptop, simulating the 2000 Polk County Florida general election of 32 contests with an average of 3.2 candidates per contests and 200,000 ballots cast. Under this scenario the election trustees could produce the necessary Switchboard audit data in under 4 minutes, with which the voters could independently verify the election tally in under 2 minutes.

Security considerations

Scantegrity offers a level of integrity not found in conventional voting systems. As with any security system, Scantegrity's security properties depend both on its technology and its procedural protections. However, a few security threats could arise during a Scantegrity election.

First, a coercer might attempt to collect ballot chits and match them to marked ballots. A corrupt election official, for example, might have sufficient ballot access to attempt this attack. This situation isn't significantly different from an attack on the underlying optical scan system. A coercer with access to ballots can scan the ballots for fingerprints. Alternatively, an attacker might be able to coerce a voter to choose a unique write-in candidate or mark the ballot in a unique way.

Second, without such access, a coercer can still force a voter to choose a particular letter on the ballot, creating a random vote. In this case, a voter can fight back by spoiling a ballot until he or she receives a ballot with the letter next to the desired candidate. Alternatively, voters could exchange receipts at random, as in the Farnel voting system,[15] or each voter could give the receipt to a trusted third party to check. However, forcing a random vote is similar to forcing the voter not to vote at all.[16]

Third, an attacker might attempt to inject optical scan ballots where the candidates or letters have been printed out of their intended order. Scantegrity avoids this attack by letting voters optionally spoil the ballot they receive before they see the information on it and take it home for later checking. By spoiling a ballot, all of its corresponding commitments will be revealed, and the voter can check that the ballot was printed properly. Misprinting can hurt attackers' chances of success, because they don't know which voter will get the altered ballot or for whom that voter will vote.

Because Scantegrity provides both E2E integrity and a traditional voter verifiable paper trail, it's more likely than a purely cryptographic system to meet requirements of a human-readable paper record of votes cast.

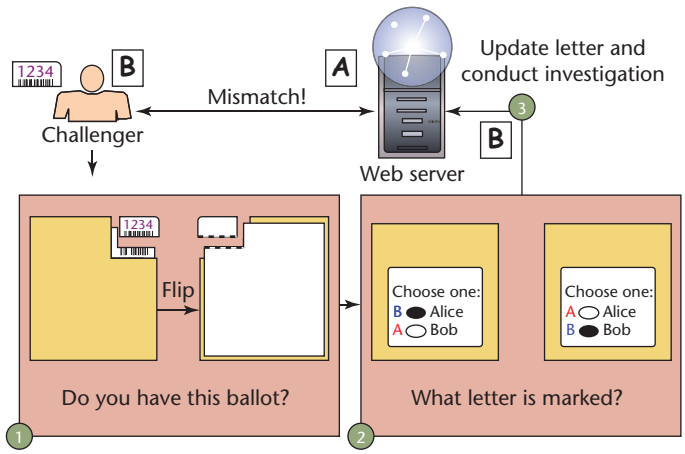


Figure 6. Dispute resolution. The election authority proves to the challenger that the ballot belonging to the chit is present and shows the letter marked on that ballot for each race. If the letter doesn't match the public record, election officials change the public record and conduct an investigation.

For democracy to stay strong, it must vigorously keep apace with the emerging vulnerabilities and possibilities of information technology—especially for its core mechanism. Scantegrity, with its simplicity, low cost, and low risk, is ready to take on the challenge and restore voter confidence. □

References

1. S. Garera and A.D. Rubin, "An Independent Audit Framework for Software Dependent Voting Systems," *Proc. 14th ACM Conf. Computer and Comm. Security* (CCS 07), ACM Press, 2007, pp. 256–265.
2. A.J. Feldman, J.A. Halderman, and E.W. Felten, "Security Analysis of the Diebold Accuvote-ts Voting Machine," *Proc. Usenix Accurate Electronic Voting Technology on Usenix/Accurate Electronic Voting Technology Workshop* (EVT 07), Usenix Assoc., 2007, p. 2.
3. US Election Assistance Commission, "2005 Voluntary Voting System Guidelines (VVSG)," Dec. 2005; www.eac.gov/voting%20systems/voting-system-certification/2005-vvsg.

4. A. Essex et al., "The Punchscan Voting System: VoComp Competition Submission," *Proc. 1st Univ. Voting Systems Competition* (VoComp), 2007; http://punchscan.org/vocomp/PunchscanVocompSubmission.pdf.
5. D. Chaum, P.Y. Ryan, and S.A. Schneider, "A Practical, Voterverifiable, Election Scheme," tech. report series CS-TR-880, School of Computer Science, Univ. of Newcastle upon Tyne, 2004.
6. Election Data Services, "2006 Voting Equipment Study," Oct. 2006; www.edssurvey.com/index.php?content=ves06n.
7. C.A. Neff, "Practical High Certainty Intent Verification for Encrypted Votes," 14 Oct. 2004; www.votehere.com/documents.php.
8. C.A. Neff, "Verifiable Mixing (Shuffling) of ElGamal Pairs," 21 Apr. 2004; www.votehere.com/vhti/documentation/egshuf-2.0.3638.pdf.
9. D. Chaum. "Secret-Ballot Receipts: True Voter-Verifiable Elections," *IEEE Security & Privacy*, vol. 2, no. 1, 2004, pp. 38–47.
10. J. Benaloh, "Ballot Casting Assurance via Voter-Initiated Poll Station Auditing," *Proc. 2007 Usenix/ACCURATE Electronic Voting Technology Workshop* (EVT 07), Usenix Assoc., 2007, p. 14.
11. J.A. Aslam, R.A. Popa, and R.L. Rivest, "On Estimating the Size and Confidence of a Statistical Audit," *Proc. Usenix/Accurate Electronic Voting Technology on Usenix/Accurate Electronic Voting Technology Workshop* (EVT 07), Usenix Assoc., 2007, p. 8.
12. D. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Comm. ACM*, vol. 4, no. 2, Feb. 1981, pp. 84–90.
13. A. Kent, "Unconditionally Secure Bit Commitment," *Physical Rev. Letters*, vol. 83, no. 7, Aug. 1999, pp. 1447–1450.
14. D. Chaum, R. Carback, J. Clark, A. Essex, S. Popoveniuc, R. Rivest, P. Ryan, E. Shen, A. Sherman, "Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems Using Invisible Ink Confirmation Codes," submitted.
15. A.J. Devegili, "Farnel: Uma Proposta de Protocolo Criptográco para Votação Digital," Curso de Pós-Graduação em Ciência da Computação da Universidade Federal de Santa Catarina, Florianópolis, Santa Catarina, Brazil, 2001.
16. S. Popoveniuc and J. Stanton, "Buying Random Votes Is as Hard as Buying No-votes," Cryptology ePrint Archive, report 2008/059, 2008; http://eprint.iacr.org/2008/059.pdf.

***David Chaum**, widely recognized as the inventor of electronic cash and techniques that more generally let individuals protect their privacy in interactions with organizations, has also made fundamental contributions related to the theory of cryptography. He has taught, led a crypto research group, launched several conferences as well as international projects, and founded DigiCash and the International Association for Cryptologic Research (IACR). Chaum has a PhD in computer science from the University of California, Berkeley.*

***Aleks Essex** is a PhD student at the University of Ottawa's School of Information Technology and Engineering. He is a member of the Punchscan team, which won first place at the 2007 intercollegiate voting systems competition, VoComp. His research interests include electronic voting, information security, cryptography, and engineering design. Essex has a master's degree in electrical engineering from the University of Ottawa. Contact him at aesse083@site.uottawa.ca.*

***Richard Carback** is a PhD student at the University of Maryland, Baltimore County in the Department of Computer Science and Electrical Engineering. He is a member of the Punchscan team, which won first place at the 2007 intercollegiate voting systems competition, VoComp. Carback has an MS in computer science from UMBC. Contact him at carback1@umbc.edu.*

***Jeremy Clark** is a PhD student at the University of Waterloo's Center for Applied Cryptographic Research. He is a member of the Punchscan team, which won first place at the 2007 intercollegiate voting systems competition, VoComp. His research interests include electronic voting, online anonymity networks, usability, economics of information security, and cryptography. Clark has an MS in electrical engineering from the University of Ottawa. Contact him at j5clark@cs.uwaterloo.ca.*

***Stefan Popoveniuc** is a PhD student at George Washington University, working on computer security and privacy in general and on electronic voting in particular. He is a member of the Punchscan team, which won first place at the 2007 intercollegiate voting systems competition, VoComp. His current research interests include the relations between the various properties that voting systems have, trying to establish a framework that would allow election officials to take informed decisions when purchasing voting system to use for their special needs. Popoveniuc has a BS in computer science from Politechnical University, Bucharest, Romania. Contact him at poste@gwu.edu.*

***Alan Sherman** is an associate professor of computer science at the Department of Computer Science and Electrical Engineering at the University of Maryland, Baltimore County. He is a member of the National Center for the Study of Elections at UMBC. His research interests include high-integrity voting systems, information assurance, cryptology, discrete algorithms. Sherman has a PhD in computer science from MIT. Contact him at dralansherman@starpower.net.*

***Poorvi Vora** is an assistant professor at the Department of Computer Science at George Washington University. Her research interests include privacy, cryptology, electronic voting, and game theory. Vora has a PhD in electrical engineering from North Carolina State University. Contact her at poorvi@gwu.edu.*