Internet Voting:
Risks, Benefits, and Recommendations

Charlin Lu

Yale University

Adviser: Robert Dunne
# Table of Contents

1. **Introduction**  

2. **Potential Advantages of Internet Voting**  
   2.1 Accuracy  
   2.2 Access  
   2.3 Convenience  
   2.4 Voter Turnout  

3. **Structural Requirements for Any Voting System**  
   3.1 Voter Authentication  
   3.2 Ballot Secrecy  
   3.3 Audit Trail  

4. **Security Concerns**  
   4.1 Attack on Client  
     4.1.1 Malicious Code  
     4.1.2 Delivery Mechanisms  
     4.1.3 Specialized Devices  
   4.2 Attack on Server  
     4.2.1 Software Vulnerabilities  
     4.2.2 Insider Attacks  
     4.2.3 Open Source Code, Testing, and Standards  
   4.3 Attack on Communications Path  
     4.3.1 Denial of Service Attack  
     4.3.2 Spoofing and Man-in-the-Middle Attacks  
     4.3.3 Domain Name Service Attack  

5. **Social and Political Ramifications**  
   5.1 Equal Access  
   5.2 Public Acceptance  
   5.3 Direct Involvement  
   5.4 Character of Elections  

6. **Past, Present, and Future**  
   6.1 Pilot Projects  
   6.2 Feasibility of Internet Voting  
   6.3 Recommendations  
     6.3.1 Internet Voter Registration  
     6.3.2 Print and Mail Option  

7. **Conclusion**  
   Additional Sources  
   Appendix I  
   Appendix II  
   Appendix III
1. Introduction

After the November 2000 presidential election fiasco, it became clear that there was something terribly wrong with our current voting system. Fewer than 537 votes determined the results of the election. With a 0.009% margin of victory, there was absolutely no room for error; yet there were errors—egregious, systemic errors that resulted in the loss of four to six million votes.¹ The margin of error was orders of magnitude larger than the margin of victory. Though Florida soon became notorious for its butterfly ballots, hanging chads, and nearly 180,000 invalid ballots, it was not the worst offender in terms of lost votes: Illinois, South Carolina, and Georgia had even higher rates of spoiled or uncounted ballots. Nor was Palm Beach the county with the worst record: nearly 10% of all ballots in Chicago were not counted, and large numbers of votes in New York City were lost due to improperly printed ballots and broken lever machines.² Not only did these findings shake America’s faith in the apparatus of its voting system, they raised serious doubts about the legitimacy of Bush’s presidency. One clear lesson from the events of November 2000 was the importance of voting mechanisms in ensuring public faith in the workings of democracy.

Once the public became aware of the myriad of problems associated with punch cards and antiquated lever machines, public officials began searching for a replacement.³ They had several possible alternatives using existing technology, including hand-counted paper ballots, optical scan devices, and Direct Recording Electronic (DRE) or touchscreen machines. Each of these systems has its own set of costs and benefits. Some experts recommend immediately replacing punch card and lever systems with optical scanning systems while exploring better

long term solutions. One such possible solution is Internet voting. In the last decade, the Internet has revolutionized the way people live, from their shopping habits to their mode of communication. Having grown accustomed to the speed of immediate electronic mail delivery and the convenience of being able to browse, price-compare, and purchase in their pajamas, they have come to expect the same degree of ease and efficiency for government transactions. A natural consequence is the desire to be able to vote online with a few clicks of the mouse.

2. Potential Advantages of Internet Voting

There are three different types of Internet voting, which are generally referred to as poll site Internet voting, kiosk Internet voting, and remote Internet voting. Each system offers a different degree of convenience and other potential benefits. Poll site Internet voting involves voting at traditional polling sites using computers that are connected to the Internet, so that votes can be transmitted through the Internet for central storage and tabulation. Kiosk Internet voting is similar, only the machines, or kiosks, can be located in nontraditional public places, such as libraries, post offices, or shopping malls, for the convenience of voters. Remote Internet voting is what most people think of when they hear the term Internet voting; it means that voting can occur from any location where there is a computer with Internet access. Remote Internet voting offers the greatest convenience but is the most difficult to deploy in a secure and reliable manner.

2.1 Accuracy

All three forms of Internet voting—by virtue of being electronic systems—can provide greatly increased accuracy, both by reducing errors made by voters and by eliminating errors in vote tabulation. One of the major problems that election officials face is voters’ inability to

---

4 Caltech-MIT Voting Technology Project.
follow simple directions. For example, when told to circle a candidate’s name, voters will often underline it instead. As a result, 2% of the 100 million ballots cast for president in 2000 were not counted because they were unmarked, spoiled, or ambiguous. While it is impossible to ensure that all polling place volunteers will give correct instructions for how to vote, electronic systems can ensure an identical experience for all voters. By forcing the user to take a specific action and disallowing all others, an electronic voting system provides a more controlled environment. Moreover, an electronic voting system, whether it consists of touchscreen devices at a polling place or personal computers at home, can easily prevent over-voting, warn voters when they skip a contest, and allow voters to verify that their selection is correctly indicated before casting the ballot. Reducing voter mistakes with a user-friendly interface is particularly important because voting is not a frequent occurrence, meaning voters have limited experience with the process and thus do not have the chance to become familiar with voting procedures. Additionally, miscounting is virtually impossible with a computer, while systems involving paper may result in some errors in tabulation, particularly with ambiguously marked ballots. In the 2000 presidential election, for example, some precincts found that each time the punch cards were run through the counters for a recount, the tally was different.

2.2 Access

Another advantage inherent in any of the three types of Internet voting (and in electronic systems in general) is increased access for those who experience difficulty voting with conventional methods. The National Organization on Disability has praised current electronic

---

7 Caltech-MIT Voting Technology Project.
10 Caltech-MIT Voting Technology Project.
systems as the most accessible existing voting technology because large fonts and sound systems allow the visually impaired to vote without assistance for the first time.\textsuperscript{11} Moreover, with an electronic system, it is easy to provide multiple versions of the ballot in different languages and a photo of each candidate so that those who do not read English are able to vote. In order for these benefits to be realized with Internet voting, however, the current situation of unequal Internet access must first be remedied, so that those with disabilities and those who do not read English have easy access to a computer connected to the Internet.

In addition to the above benefits which can be provided through any electronic voting system, with or without a connection to the Internet, an Internet voting system has the unique capability to increase access for military personnel, their families, and other overseas Americans. Even now, it remains unknown how many votes were lost in the 2000 presidential election due to mishandled or otherwise controversial absentee ballots. Moreover, the Federal Voting Assistance Program (FVAP) has found mail transit time to be a significant barrier to the ability of military and overseas citizens to vote.\textsuperscript{12} Registering to vote, receiving the absentee ballot, and then returning the completed ballot in time for it to be counted is particularly difficult for soldiers who are located in desolate areas lacking reliable mail transport and those who are constantly on the move. Surveys suggest that the obstacles and frustration they encounter in attempting to exercise their right to vote has led large numbers to forego even making the attempt. Those who try to vote through the current mail-in process are often disenfranchised anyway: nearly one in three overseas soldiers registered to vote in the 2000 presidential election did not receive their


ballots in time.\textsuperscript{13} Clearly such disenfranchisement of those who risk their lives to protect their country is unacceptable and demands an effective remedy.

2.3 Convenience

Though all three types of Internet voting systems offer greater convenience than the current system, only remote Internet voting provides a truly substantial and noteworthy increase in convenience. Polling place Internet voting would allow voters to cast a ballot from any polling place rather than requiring them to vote in their home precinct, and kiosk Internet voting would provide more numerous and possibly more convenient locations for voting. With remote Internet voting, voters would have the ability to vote at any time of day, from any location with Internet access, whether it is at the office, at home, or at the local public library.

Improving the ease with which voters are able to cast their ballots may seem to be a matter of “mere convenience” but its effect on elections is real and can be significant, particularly in close elections. According to the U.S. Census Current Population Survey, 2.8 percent of the forty million registered voters who did not vote in 2000 were prevented from casting their ballots due to problems with polling place operations, such as lines, hours, or locations.\textsuperscript{14} These numbers include both those who did not travel to their polling place due to the perceived inconvenience and those who attempted to vote but were turned away. While this is not an overwhelming portion of the population, it certainly could have played a deciding role in the extremely close presidential election in 2000. In a more general sense, it suggests that inconvenient hours, locations, and long lines can result in voter disenfranchisement.

The growing number of ballots that are cast either absentee or early (fourteen percent of all ballots in 2000) is evidence that more and more Americans find the time and place restrictions


\textsuperscript{14} Caltech-MIT Voting Technology Project.
of conventional voting on Election Day to be too inconvenient. When remote Internet voting was offered as an option in the 2000 Arizona Democratic primary, the number of ballots cast remotely through the Internet dwarfed the number of ballots cast by conventional means, further confirming the importance of convenience to today’s voters.\textsuperscript{15}

\textbf{2.4 Voter Turnout}

Perhaps the most oft-cited benefit of Internet voting is the possibility of substantially increasing voter turnout. Increasing voter turnout is a goal of utmost importance because low voter participation not only reflects growing indifference about civic affairs but also undermines the legitimacy of a democratically-elected government. While it remains debatable whether voter participation has been declining dramatically in the past few decades, it is undisputed that the current rate of voter turnout is less than optimal. In the last fifty years, voter turnout has not exceeded sixty-five percent for presidential elections, and the figures are considerably lower for elections for other public offices.\textsuperscript{16} At the very least, this lack of broad participation in the most fundamental of all civic activities reflects growing apathy among citizens; at its worst, officials who have been elected by far less than a majority of the population lack the authority and legitimacy of a popular mandate.

There is some controversy over whether the introduction of Internet voting would actually result in a significant increase in the number of people who vote. Some evidence seems to imply that it would not. Measures that have sought to make voter registration more convenient, such as the National Voter Registration Act of 1993, have succeeded in increasing the number of registrations but have not resulted in a similar increase in the number of voters. In


fact, since the implementation of this Act, voter turnout has generally declined. Nonetheless, proponents of Internet voting contend that Internet voting is different because it actually makes the act of voting itself more convenient. Just as making registration procedures simpler has prompted more people to register to vote, making voting itself more convenient should encourage more people to vote.

Yet many social scientists who study the pattern of decline in voter participation do not believe Internet voting would substantially increase voter turnout. They point to research indicating that increased information, motivation, and mobilization are far more powerful forces in shaping voter turnout than greater convenience is. Additionally, there has been no evidence that liberalizing absentee voting laws or implementing early or by-mail voting schemes have had a significant positive effect on voter participation. For example, Oregon, the first and only state to have an entirely vote-by-mail system, experienced only a slightly higher increase in voter turnout in the 2000 presidential election compared to the nationwide average. In Texas, the picture is even more dismal: ever since the introduction of early voting as an option in 1998, increases in voter participation have been less than the nationwide average in every presidential election.

If convenience is not enough to induce non-voters to participate in elections, then Internet voting may simply increase convenience for established voters with no effect on voter turnout. However, there is also a body of evidence that suggests Internet voting has the potential to dramatically revitalize our democracy by encouraging many to vote. In a study at the University of Arizona, 42% of survey respondents who did not vote in the 2000 presidential election

---

18 Internet Policy Institute.
19 Caltech-MIT Voting Technology Project.
indicated that they would have voted if Internet voting had been available. Moreover, many of the private and party-run elections that have offered Internet voting as an option have experienced substantial increases in voter turnout. When Internet voting was provided in the 2000 Arizona Democratic primary, for example, there was a significant increase in voter participation over 1996. If Internet voting had been available and resulted in the same level of increased participation for the 2000 presidential election, then 71% of the voting age population would have cast a ballot. Thus, advocates dismiss the view that Internet voting would have little effect on voter turnout as mere speculation that is at odds with the demonstrated facts.

The truth is probably less clear-cut than either side claims. The novelty of Internet voting as an option, along with news coverage of the legal wrangling over whether Internet voting would dilute minority votes, most likely had some effect on the number of voters who participated in the 2000 Arizona Democratic primary. Consequently, maintaining such a dramatic increase in voter turnout should not be expected, as interest in Internet voting as a novelty is sure to fade over time. Lasting change in voter participation may require more than increased convenience, but allowing people to vote online is likely to boost the number of young college students and professionals who vote. One of the reasons many believe that Internet voting holds great promise for increasing voter turnout is the fact that those who are currently the least likely to vote—18- to 25-year-old students and professionals—are also the most likely to use the Internet on a regular basis. Even those who are initially attracted by the novelty of the new voting system may become regular voters once they have taken the first step of becoming involved in the democratic process, particularly if it requires little extra time and effort.

---


21 California Internet Voting Task Force.
The question then becomes whether it is even desirable to encourage those who are not willing to devote their time and energy to physically go to the polls to vote through an Internet system. Those who are motivated enough to go to a polling place to cast a ballot are more likely to have taken the time to understand the candidates’ positions than those who could not be bothered to go to the polls. Hence, some have concluded that “the solution to a lack of commitment of voters is not to reduce the necessary commitment needed to vote.” On the other hand, one could view this stance as reminiscent of the now-abolished literacy test which was once administered, supposedly for the purpose of ensuring that voters were educated enough to be informed of the issues. After all, even those who are motivated and well-informed may find a trip to the polls overly burdensome due to unforeseen conflicts or other personal circumstances. Who is to judge that an overseas serviceman, a mother with a sick child, or a professional who is called away on a last-minute business trip should not be afforded the ability to cast a ballot? In any case, most people would support measures seeking to increase voter turnout through a combination of political awareness campaigns and a more convenient voting system.

3. Structural Requirements for Any Voting System

Given the potential benefits of Internet voting, many experts, both in electoral matters and in computer science, have sought to design such a system. There are several basic requirements, such as voter authentication and ballot secrecy, that any voting system must satisfy in order to be acceptable. Meeting all of these requirements poses some challenges for Internet voting, especially remote Internet voting. In particular, it is difficult to preserve the anonymity

---

of each vote while ensuring strong identity verification for each voter and maintaining an audit trail.

3.1 Voter Authentication

Voter authentication serves two essential purposes. Verifying the identity of the voter allows a voting system to determine whether a person is eligible to vote, and by maintaining a record of those who have already cast a ballot, it ensures that each eligible voter is only allowed to vote once. Voter authentication has traditionally been accomplished by requiring voters to vote in their home precinct and using government-issued photo identification to prove the identity of each voter at the polling place. With absentee or other mail-in ballots, however, the voter’s signature on an affidavit accompanying the ballot or on the envelope containing the ballot is used for identity verification. This signature is compared to the signature on the original voter registration card. In these instances, the prevention of fraud relies largely upon the local election officials’ signature verification skills. Some critics believe that absentee voting and vote-by-mail provide insufficiently strong voter authentication and thus should be abolished or greatly reduced. Nonetheless, both methods have become increasingly popular with the American public in recent years, and Oregon has become the first state to implement a completely vote-by-mail system.

At a minimum, Internet voting must guarantee the same protection from fraud that existing mail-in voting procedures provide, and ideally, its method of voter authentication should be as strong as the traditional means using photo identification. While poll site Internet voting can rely on conventional polling place methods for verifying voter identities, both kiosk and remote Internet voting require a new means for voter authentication. Existing remote Internet voting schemes provide the voter with a unique identifier, whether it is a password, personal

23 Caltech-MIT Voting Technology Project.
identification number (PIN), smart card, or a digital signature. In the 2000 Arizona primary, for example, all registered Democrats were mailed a random seven-digit alphanumeric PIN, and those who chose to vote online were required to identify themselves by entering their assigned PIN and answering additional challenge questions, based on their registration information. Unfortunately, there are several problems with assigning voters such one-time-use identifiers. First is the issue of communicating this identifier to the voter. There needs to be a secure and reliable means of transport to ensure that identifiers do not fall into the wrong hands and that each voter receives the identifier in time to cast a ballot. Additionally, unlike commonly used government-issued photo identification, like a driver’s license, many voters may lose or forget their password or PIN number. Already, several remote Internet voting pilot projects have experienced difficulties due to untimely delivery of identifiers or forgotten passwords, demonstrating the likelihood that these problems would occur on a large scale. Furthermore, such a means of identity verification would facilitate vote-buying schemes: one could simply sell the one-time identifier and the commonly used information for challenge questions (address, date of birth, mother’s maiden name).

One way to avoid these problems is to use biometric means of identification. However, biometric identification would give rise to a whole host of other obstacles. Currently there is not a broad base of biometric technology users, and it is unlikely that such technology will soon become widespread. A far greater impediment to its implementation is the fact that before a biometric signature can be used for online identification, the government must compile a comprehensive voter registration database containing each registered voter’s biometric information. This raises serious privacy issues and is almost certain to meet stiff public resistance that may result in a drop in voter participation.

---

24 Done.
A possible alternative to biometric signatures and one-time identifiers is a multi-purpose digital certificate. Digital certificates provide strong identification through a trusted certification authority (CA) and public and private cryptographic keys that allow the production and verification of digital signatures. If digital certificates one day become as commonly used as driver’s licenses are today, they may offer a viable means of voter authentication. Individuals are less likely to be willing to compromise a digital certificate that they need and use for multiple everyday applications in order to sell a vote than if they were provided with a one-use identifier. Also, because the same digital certificate could be used in every election, election officials would only need to transmit it to the voter once—possibly at the time of voter registration.

Unfortunately, though digital certificates can already be purchased relatively inexpensively, the American public remains generally unfamiliar with this technology, lacking both experience in the use of digital certificates and an understanding of how they work.\(^\text{25}\)

Experts have suggested several methods for preventing eligible voters from voting multiple times with a kiosk or remote Internet voting system. If all votes must be cast through Internet voting, the voting server can simply track which voters have already cast a ballot and thus prevent multiple votes. If alternative options, such as optical scan ballots, are provided in addition to Internet voting, there are other simple mechanisms that can prevent multiple voting. One method, which was employed during the 2000 Arizona Democratic primary, is to allow remote Internet voting prior to Election Day but not on Election Day itself.\(^\text{26}\) As long as each polling place is provided with a list of those who have already voted online, local polling place staff can prevent voters from casting multiple ballots. Moreover, if each polling place has Internet access, then there is no need to even prevent remote or kiosk Internet voting on Election

\(^{25}\) Department of Defense Washington Headquarters Services FVAP.

\(^{26}\) Done.
Day, as long as poll site workers remove each voter from the online database of eligible voters as they check them in.

3.2 Ballot Secrecy

Another essential requirement for any voting system is the ability to keep the contents of the ballot secret. Without ballot secrecy, both coercion and vote-buying can easily take place. One of the problems with a remote Internet voting system and, to some extent, with kiosk Internet voting is they lack the guaranteed privacy of a physical voting booth. This drawback occurs with current absentee and mail-in ballots as well, but in those cases, vote-buying is facilitated on a much smaller scale, and the possibility of intimidation is mostly a concern for those who rely on caregivers, such as elderly people in nursing homes. With remote Internet voting, the secrecy of the ballot may easily be compromised for anyone using a computer that is not their own.27 This includes the large number of people whose primary source of Internet access is computers at their workplace as well as those who rely on public computers in Internet cafes or libraries for Internet access. The owner of the computer and possibly any previous user may have installed software on the machine that would allow remote monitoring or even remote control. Even those who use their own personal computers to vote may have their privacy compromised if they access the Internet through a local area network (LAN), since the network administrator could access the ballot information on the computer before it is encrypted.

Additionally, those who wish to sell their votes can intentionally compromise the secrecy of their ballot in a multitude of ways. For example, the vote-seller can simply connect to the vote-buyer’s proxy server so that all traffic passes through this server, allowing the buyer to

verify how the seller voted.\textsuperscript{28} This allows an easy and automated form of vote-buying, thus facilitating its occurrence on a large scale. One way to mitigate this problem is to allow voters to vote multiple times, having only the last vote count.\textsuperscript{29} However, this solution has several drawbacks: it would complicate audit trails or recounts and encourage last-minute voting.

Guaranteeing ballot secrecy from the prying eyes of election officials is less of a challenge. Ballot secrecy can be maintained by stripping the ballot of all identifying information before allowing the appropriate election official to decrypt its contents for vote tabulation.\textsuperscript{30} In this way, election officials can maintain a record of who has voted in a database that is separate and cannot be merged with a database of ballot contents. This technique for ensuring ballot secrecy is similar to current procedures for absentee ballots. With absentee or mail-in ballots, voters generally use two envelopes: they insert the ballot in an inner envelope that contains no identifying information and then place the inner envelope in an outer envelope containing information identifying the voter (such as a name and signature).\textsuperscript{31} Thus, the outer envelope allows voter authentication, but the contents of the ballot is hidden from view by the inner envelope and is opened separately. With kiosk or remote Internet voting, several levels of encryption act as envelopes, separating and hiding the contents of the ballot.

\subsection*{3.3 Audit Trail}

While not all voting systems currently in use provide an independent audit trail, some would argue that a voting system that does not provide such an audit trail should not be used for this reason alone. The purpose of an audit trail is to ensure that the results of an election accurately reflect voters’ desires. Accomplishing this goal requires both proof of vote tabulation

\begin{footnotesize}
\begin{enumerate}
\item\textsuperscript{28} Jefferson, Rubin, Simons, and Wagner.
\item\textsuperscript{29} Internet Policy Institute.
\item\textsuperscript{30} California Internet Voting Task Force.
\item\textsuperscript{31} Jefferson, Rubin, Simons, and Wagner.
\end{enumerate}
\end{footnotesize}
correctness and proof of ballot integrity. Ballot integrity is concerned with the correct mapping of a voter’s intent to a ballot’s stored content, while vote tabulation correctness is concerned with the accurate tallying of ballots according to their stored content. Thus the main difference between the two is merely the phase in which the distortion of voter intent may take place. An audit trail makes an independent recount of ballots possible, but this is only meaningful if there is certainty that the voter’s intent was accurately captured and stored on each ballot.

With paper ballots, such as optical scan devices or punch cards, voter intent is generally assumed to have been captured, though experiences with butterfly ballots have shown that this assumption may not always be warranted. Similarly, with lever machines, though the inner workings are not revealed to or understood by the common voter, the mechanical parts are simple enough to provide a reasonable guarantee that they function correctly in the capturing and tallying of votes. One major problem with DRE devices is that the so-called audit trail is simply a record of what the machine recorded. Naturally, this means that any systemic error would be replicated in the audit trail, making it impossible to identify any errors, much less rectify them. Even machines that produce an internal paper tape and an electronic recording of every voting session do not solve the problem of a failure, whether intentional or accidental, between the touchscreen and the tape.32 Because DRE machines often contain complex code, many computer scientists contend that there can be no certainty that they are functioning correctly. Hence critics have called for voter verification to ensure ballot integrity, and several possible techniques for facilitating voter verification have been devised.

One such scheme is the Mercuri Method, also commonly referred to as verified voting. Designed by Rebecca Mercuri, this system allows voters to personally verify their ballot choices,
thus preventing and detecting any misbehavior on the part of the voting machine.³³ Each electronic voting machine would simply print out a paper receipt listing the voter’s choices in human-readable form so that each voter can confirm that the ballot correctly reflects his or her intentions. To prevent the receipt from being removed from the polling place premises, the printout would be displayed under a transparent barrier and, upon approval, deposited directly into a locked box for safe-keeping. These paper receipts would allow both a complete recount and random auditing to ensure that electronic voting machines are functioning correctly. The beauty of the Mercuri Method lies in its sheer simplicity; this is a scheme that is easy for the common voter to understand and to trust.

An alternative technique for creating an independent audit trail is David Chaum’s revolutionary receipt system. While take-home receipts have generally been banned from voting systems to prevent vote-buying and coercion, Chaum’s method provides voters with receipts proving that their ballots have been stored and counted, yet maintains the confidentiality of each ballot’s contents.³⁴ As with the Mercuri Method, each voter would verify his or her choices on a human-readable printout, but this printout would be a two-layer receipt with a serial number. Each of the two layers would independently have the ballot choices encoded on it using a graphical form of public key cryptography. Once separated, however, only a group of trustees with access to the necessary private keys would be able to derive the ballot contents using only a single layer. After the voter chooses one layer to take home as a receipt, the image on this layer would be stored electronically for tabulation, and the polling place staff would then physically destroy the other layer in the presence of the voter. Each voter can later visit the official election website to verify that his or her ballot has been stored and counted by comparing the image on

³⁴ David Chaum, Secret-Ballot Receipts and Transparent Integrity, online, Internet, 12 Apr. 2004.
his receipt with the image listed under his serial number. The main drawback of this system is its reliance on graphical encryption, which is beyond the understanding of the average voter. Thus, while voters can easily verify that their ballots have been stored for tabulation, they are unable to decrypt receipts to personally verify ballot integrity. Though Chaum can demonstrate ballot integrity through mathematical proofs, public faith remains dependent on somewhat blind trust in expert cryptographers.\(^{35}\)

Furthermore, neither the Mercuri Method nor Chaum’s system can be implemented in a remote voting system since both depend on printing paper receipts that must be either partially destroyed or physically retained. While poll site and possibly kiosk Internet voting can incorporate these solutions, providing a voter-verified audit trail in a remote Internet voting system poses a difficult challenge which has yet to be solved. A complete recording of all activity cannot be kept because such an electronic audit trail would compromise the principle of ballot secrecy by making it possible to trace each voter’s steps.\(^{36}\) Moreover, any remote system that allows voters to personally verify that their votes have been accurately captured, stored, and counted would necessarily facilitate coercion or vote-buying by providing a method for proving how one voted.

4. Security Concerns

Without an independent audit trail to guarantee ballot integrity and vote-tabulation accuracy, ensuring security is crucial for remote Internet voting. Unfortunately, computer scientists have identified an alarming number of security vulnerabilities inherent to any Internet voting system. While vote fraud is certainly possible with current systems that rely on physical precincts and mechanical devices, the decentralized nature of the existing voting system makes it

---

extremely difficult to perpetrate vote manipulation on a large scale. However, with computer systems, particularly with a central server, failure typically occurs on a large scale; a single exploited vulnerability could affect millions of votes. Moreover, attacks on computer systems are easily automated. Hackers routinely scan thousands of computers to find the ones that are the easiest to compromise, and worms spread themselves without human supervision. The international nature of the Internet further compounds these problems. In addition to posing difficult jurisdictional issues, it means that an election held over the Internet could be attacked remotely from anywhere in the world, whether by a lone hacker or a foreign government.

It is also more difficult to shield an Internet voting system from attack than it is to secure an e-commerce application. Mechanisms commonly used to protect e-commerce from fraud, such as bills, statements, receipts, and comprehensive logging of each electronic session, cannot be incorporated in a voting system because they would compromise ballot secrecy. The fact that a successful attack on an American election would be extremely high profile also provides an exceptionally strong incentive for hackers to attempt such an attack. Furthermore, unlike with e-commerce, in which refunds and insurance can help to rectify any damage caused by fraud, there is no way to recover from a failure in an Internet voting system. Not only is voter disenfranchisement difficult to reverse, the legitimacy of the democratic government is at stake. Even if an attack were discovered, anonymity requirements necessarily make it impossible to recover from a security failure, and public confidence may be irrevocably damaged.

With such high stakes, it is essential that any voting system provide adequate security. Nonetheless, requiring adequate security does not mean demanding that Internet voting be one

---

38 Internet Policy Institute.
40 Rubin.
hundred percent secure. After all, current voting systems have their security flaws as well; most are potentially susceptible to vote manipulation on a small scale but are well-protected against large scale fraud.\textsuperscript{41} Consequently, a more reasonable approach would be to require any Internet voting system to be at least as secure as existing systems. There are three ways for an attacker to compromise the security of an Internet voting system: penetrating the client,\textsuperscript{42} penetrating the election server, and disrupting or corrupting the communication path between the two. Before any Internet voting system can be responsibly deployed, it must contain adequate safeguards against all three forms of attack.

\textbf{4.1 Attack on Client}

Remote Internet voting is unlike any current or previous voting system because the machines used to cast ballots would not be owned, controlled, or even monitored by election officials. This lack of control over voting equipment is perhaps the greatest obstacle to providing secure remote Internet voting.\textsuperscript{43} Hence, poll site voting and even kiosk voting, in which voting equipment is owned, inspected, and maintained by election officials, is far less susceptible to client attacks. While use of personal computers has become prevalent, knowledge about how to secure one’s computer against outside attackers is far less widespread. Moreover, those who depend on shared computers at their workplace, a public library, or a cyber café have no control over the equipment. Not only does the owner or system administrator have the ability to control and monitor all actions on the computer, unless strict network configuration management

\begin{itemize}
\item \textsuperscript{42} The client is the machine from which individual users vote. In poll site or kiosk voting, the client would be the electronic voting machine from which voters cast their ballots. In a remote Internet voting scheme, the client could be any computer connected to the Internet.
\item \textsuperscript{43} Jefferson, Rubin, Simons, and Wagner.
\end{itemize}
protocols are enforced, any previous user could have installed remote spying or subversion software.

One reason personal computers (PCs) are so vulnerable to attack is PC hardware was not designed with security as a priority, or even as a serious concern. As a result, none of the primary human interface devices for PCs, such as the keyboard, printer, screen, or speakers, were designed with the capability to perform cryptographic operations. Consequently, all data must be manipulated while unencrypted on the main part of the PC, where is it vulnerable to malicious software. Further exacerbating these shortcomings is Microsoft’s Windows operating system. Microsoft designed Windows to provide maximal functionality and ease of use—not to provide good security. Unsurprisingly, Windows has countless security vulnerabilities, and a PC running Windows can easily be compromised.

4.1.1 Malicious Code

There are several types of malicious code that are likely to be a threat to Internet voting, particularly in a remote Internet voting scheme. These include computer viruses, worms, Trojan horses, spyware, and remote control programs. While a computer virus is a parasitic computer program that can only reproduce by altering other programs to include a copy of itself, a worm has the ability to independently replicate itself from machine to machine through computer networks, usually by taking advantage of security vulnerabilities. Unlike viruses and worms, a Trojan horse cannot replicate itself automatically; it is simply a destructive computer program that masquerades as a harmless application. Spyware (spy software) allows an attacker to invisibly monitor the user’s activities, recording keystrokes typed, websites visited, and other actions taken by the user. In addition to monitoring the user’s actions, remote control programs allow the attacker control them, often without the user’s knowledge. Once installed onto a

---

computer, viruses, worms, and Trojan horses containing spyware, remote control programs, and other malicious code can allow the attacker to disrupt, monitor, or subvert the voting process by damaging the computer, spying on the user’s actions, or modifying ballots.

One example of a remote control program is Backorifice 2000 (BO2K). Installing this program on a computer allows a network administrator to monitor and control any aspect of the machine remotely. Not only is it freely available, it is open source and extensible, meaning that anyone with the technical expertise can alter the code and recompile it so that the program will not be detected by virus or intrusion detection software, which looks for known digital signatures of programs. Additionally, it provides the option of running in stealth mode, which keeps the program from appearing in the Task Menu of running processes so that even an experienced administrator would have difficulty detecting its presence on a computer, even while it is running. There is no way an average computer user can reasonably be expected to detect and remove BO2K from his or her computer. An attacker can use BO2K to compromise ballot secrecy, to modify users’ ballot choices without their knowledge, and even to disenfranchise users by remotely locking the keyboard and mouse. Consequently, BO2K and all similar programs are a cause for serious concern in any remote Internet voting scheme.

Another example of malicious code that has the potential to threaten an online election is the Chernobyl (CIH) virus. This virus was designed so to be triggered on a specific day. On that chosen date, the code changes the BIOS of the computer so that it is unable to boot. On April 26, 1999, the CIH virus wreaked havoc in Asia, damaging thousands of computers so severely that many of them needed to be physically taken to a store for repair. A virus like CIH is particularly worrisome for an Internet voting system because election days are known well in

---

45 Rubin.
advance.\textsuperscript{46} Even if the voting window is extended to be longer than a day or a few days, past experience has shown that many voters will wait until the last day to vote. Thus, activating a virus on the last day of elections could easily disenfranchise a large portion of voters.

While viruses are troublesome enough, malicious worms can be even more detrimental. The ability of worms to replicate themselves without depending on a host application has allowed them to spread extremely quickly. In 2001, the Code Red worm infected 360,000 computers in just fourteen hours, and in 2003, the Slammer worm infected numerous Internet hosts and shut down many ATM machines. Worms have become more and more virulent in recent years; they are now often spread by multiple methods and have the ability to bypass firewalls and other security defenses. Even once their presence has been detected, they can be quite difficult to analyze. For example, it took computer scientists quite some time before they realized that SoBig.F was a Trojan horse that planted spam engines. Some experts have estimated that in a matter of months, a small team of experienced programmers could develop a worm that would penetrate the majority of all Internet-connected computers in just a few hours.\textsuperscript{47} With the potential for such a large scale attack, a worm could threaten the validity of any election held over the Internet.

\textit{4.1.2 Delivery Mechanisms}

Malicious code poses such a threat to remote Internet elections due to the ease with which such code can be delivered to a personal computer without the user’s knowledge. Physical installation is an obvious means for installing remote monitoring or subversive software on a computer. While this is unlikely to occur on a large scale, particularly for home computers, it is certainly a possibility for public or shared computers. Remote automated delivery is a more

\textsuperscript{46} Rubin.
\textsuperscript{47} Jefferson, Rubin, Simons, and Wagner.
worrisome scenario. E-mail makes it easy to spread worms, viruses, and Trojan horses which can be activated simply by previewing the message using Microsoft Outlook. Malicious scripts, such as ActiveX controls, JavaScript programs, or Java applets, can also be automatically downloaded as an invisible side effect of visiting a web site. Though only ActiveX controls that are marked as trusted will run automatically, any programmer who is a valid publisher can write code that is implicitly trusted by the Windows operating system. A hacker could cause selective disenfranchisement by installing malicious code on all computers that visit a candidate’s web site, for example. Alternatively, a hacker may simply scan a large number of computers that are connected to the Internet and directly attack those that are most easily compromised, either through a known vulnerability (because the user has not diligently installed all the security patches that have been issued) or through a newly discovered weakness, such as a buffer overflow in the operating system or web browser.

Additionally, computer users often download and install free software, such as browser plug-ins, games, and screen savers, from the Internet. This common habit is detrimental to the security of one’s personal computer. Anytime software is downloaded off the Internet, there is the possibility that it contains malicious code that may allow a remote attacker to damage, monitor, or control the computer. Even if the application itself is free of malicious code, it may automatically install a dynamically linked library (DLL) that has been compromised. Moreover, even those who are cautious enough to scan any application with a virus-checking program before downloading it are not protected because these programs simply scan for the

---

49 Internet Policy Institute.
50 Rubin.
digital signature of previously known viruses; they would not detect the existence of a new or modified worm or virus.

To make matters worse, even the most security-conscious users who refrain from downloading free software from unfamiliar sites may have their computers compromised through commercial software. Programmers can hide backdoors in commercial software packages that will be activated when the user tries to vote, allowing an attacker to spy on or subvert the voting process without the user’s knowledge. Though this scenario may sound far-fetched to some, the ease with which it can be executed has already been demonstrated. Easter Eggs—cute extras that programmers add to applications without permission—are known to exist in many software programs today.⁵¹ One well-known example of an Easter Egg is the flight simulator program that can be launched from Microsoft Excel 97 using a specific sequence of keystrokes. With millions of personal computers running Microsoft Office, AOL Instant Messenger, Adobe Acrobat, WinZip, and other proprietary commercial software, this small handful of software vendors would have the ability to control a large portion of votes simply by inserting malicious code in their popular software packages and providing free updates to users. As long as the program functions as expected, users would never suspect that their computers had been compromised. Even if the software firms would not engage in any such practices, a single rogue programmer working for any one of these companies could easily add malicious code into an application without detection. The combination of the ease with which a single programmer could launch such an attack and the devastating effect it would have on voter confidence if discovered and on election results if undetected make it imperative that the security vulnerabilities inherent in personal computers as voting clients are solved before any remote Internet voting system can be implemented.

⁵¹ Garfinkel.
4.1.3 Specialized Devices

Some computer scientists have suggested using specialized devices such as wireless handheld appliances with “software-closed” architecture as voting machines rather than personal computers.\textsuperscript{52} This would solve many of the security problems inherent in using general-purpose processors. Unfortunately, there are considerable obstacles that stand in the way of implementing such a voting scheme. Most handheld devices are limited in terms of user interface, and use of such specialized electronic devices is not nearly as widespread as computer-based Internet use. Another solution that has been suggested involves using tamper-resistant devices, such as smart cards, which can store cryptographic keys and perform complex computations, allowing the exchange of credentials between a client and a voting server.\textsuperscript{53} As with handheld devices, the lack of smart card readers on the average Internet user’s personal computer prevents this scheme from being implemented in the near future. Moreover, because the smart card cannot interact directly with the election server, malicious code on the computer may still be able to deceive and misuse the smart card.

4.2 Attack on Server

The voting server faces some of the same security issues as the voting client, but many security vulnerabilities are mitigated because election officials own and control this portion of the voting equipment. Thus, physical measures that prevent unauthorized access, along with strictly enforced system configuration protocols, greatly reduce the possibility that suspect code will be downloaded and installed onto the server. Certainly the level of sophistication and dedication required for a hacker to gain access to the server is higher. Nonetheless, despite all the firewalls, antivirus programs, and intrusion detection systems that are available, any

\textsuperscript{52} Internet Policy Institute.
\textsuperscript{53} Rubin.
computer that is connected to the Internet faces some security risk, as minute as it may be, that a hacker will successfully penetrate its defenses and gain unauthorized access.

4.2.1 Software Vulnerabilities

A fundamental difference between the software for Internet voting systems and the mechanical parts of a conventional voting machine is that computer code is orders of magnitude more complex. While the laws of physics dictate the movements of each mechanical part, the complexity of software programs means that the code may contain various bugs and security vulnerabilities, and the program may behave in an unexpected manner. The possible security vulnerabilities are numerous, including buffer overflows, format string vulnerabilities, directory traversal bugs, race conditions, cross-site scripting bugs, SQL injection bugs, cryptographic failures, and session authentication weaknesses. It is impossible to determine with certainty whether a specific one of these bugs exists in a program, much less confirm that none of them do. In fact, computer scientists have proven that there is no way to determine by any finite means whether a program satisfies the properties of correctness and reliability, much less whether it is secure or contains malicious logic.

Some have attacked this as a purely academic concern, pointing out that no security system can guarantee that it has absolutely no vulnerabilities and is perfectly secure. Despite the inability to prove absolute security, computer programs are used for financial transactions, medical records, aviation control, and in other applications that require high levels of security and reliability. Nonetheless, the concerns voiced by computer scientists are far from pure academic speculation: the fact that Microsoft and other software vendors must continuously

---

release software patches to fix security holes is proof that the danger in using complex computer programs for a voting system is very real, particularly if the application depends upon commercial off the shelf (COTS) software. When software is designed specifically for a high stakes, safety-critical application, such as nuclear reactor control systems or air traffic control systems, programmers refrain from using any COTS software. In addition to keeping the program as simple as possible, they undertake careful mathematical and algorithmic analysis of the code and scrutinize the program, putting it under both systematic and random testing procedures, to keep the likelihood of security vulnerabilities acceptably low.\textsuperscript{57} This is an extremely time-consuming and costly procedure, which commercial software vendors do not even attempt to undertake—a problem for any Internet voting system relying on any COTS software. While it is theoretically possible to create software programs for poll site and kiosk voting that do not rely on COTS, some would argue that it is prohibitively expensive. Moreover, for remote Internet voting, users depend on currently available commercial operating systems and web browsers.

One might wonder why the code would need to be so complex if all the program has to do is count votes. In addition to capturing and transmitting a completed ballot to the server for secure and anonymous storage and tabulation, an Internet voting system must also accomplish strong identity authentication, server verification, and encryption of the vote. Each of these components complicates the task at hand. For a remote Internet voting system, ensuring system compatibility is an additional challenge. The software would need to support a wide variety of platforms, so that it can be used with different types of computers with different operating

\footnote{57 Fischer.}
systems running different versions of web browsers. Satisfying all of these demands inevitably increases the complexity of the system.\footnote{California Internet Voting Task Force.}

4.2.2 Insider Attacks

Even if it were possible to determine that a program had no security vulnerabilities to outside attack, insider attacks remain a threat. A lone programmer could add malicious logic to the voting system program such that either votes are lost or a vote for one candidate is counted as a vote for another. Due to the inherent complexity of computer code, some computer scientists assert that even programmers on the development team cannot determine with any degree of certainty that the program does not contain some hidden functionality, regardless of the amount of time and effort spent testing and scrutinizing the program. For this reason, the computer security community is nearly unanimous in their agreement that no electronic voting system should be implemented without some form of voter verification to guard against insider attacks.\footnote{Jefferson, Rubin, Simons, and Wagner.}

4.2.3 Open Source Code, Testing, and Standards

Besides voter verification, there are several ways to mitigate both the risk of security vulnerabilities and the possibility of insider attacks. One is to make all source code (or at least the source code for key operations such as ballot tabulation) open to public scrutiny. Many computer scientists believe that allowing all interested parties to examine, analyze, and test source code makes it more secure by increasing the likelihood that vulnerabilities will be found and corrected.\footnote{Internet Policy Institute.} Vendors who want to keep their source code proprietary argue that making source code public aids hackers by providing them with a detailed understanding of how the system works.\footnote{Fischer.} Their argument is unpersuasive for several reasons. Not only does it ignore the
possibility of insider attacks, such a principle of relying on secrecy means that once someone outside of the trusted development team gains access to information about how the system works, the system is much more vulnerable to attack.\textsuperscript{62} Experience with security systems validates the wisdom of allowing public scrutiny to take place. For example, cryptographic systems developed and tested in public tend to endure, while those created in secret are often soon broken.\textsuperscript{63}

Setting standards and using comprehensive testing to enforce those standards is another way to mitigate the security risks of any voting system. For an Internet voting system, testing is meant to verify that the software is accurate, reliable, robust, and secure. The problem with complex code, as noted earlier, is that performing testing that is comprehensive enough to be fairly confident of any of these properties may prove to be prohibitively expensive. Moreover, while testing may confirm that bugs and security vulnerabilities exist, no finite amount of testing can ever prove that a piece of code is flawless. Nonetheless, though testing cannot provide an absolute guarantee that code is free from bugs, malicious logic, or vulnerabilities, it is essential for providing some degree of confidence in the correctness, reliability, and security of the voting system.

Currently, a voting system must be tested by Independent Testing Authorities (ITAs) before it is certified for use. Additionally, to promote national uniformity among voting systems, the Federal Election Commission (FEC) and the National Association of State Election Directors (NASED) created a set of voluntary standards for minimal functional requirements.\textsuperscript{64} Critics have suggested various ways to improve upon the current testing protocol to provide a better

\textsuperscript{62} Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, Analysis of an Electronic Voting System (23 July 2003), online, Internet, 10 Feb. 2004.
\textsuperscript{64} Fischer.
guarantee of security. All software should be modeless so that there is not a separate “test” mode which would facilitate the hiding of malicious logic.\textsuperscript{65} Besides making all source code for vote recording and vote counting processes open source, having independent third party “white hat” hacking efforts could discover system vulnerabilities so that they can be patched before the system is used. Additionally, adopting software engineering protocols for safety-critical systems and implementing industry best practices, including a rigorous implementation of due diligence, can greatly reduce security risks.\textsuperscript{66}

One of the glaring loopholes in the FEC requirements is that COTS software does not have to be tested by the ITAs at all.\textsuperscript{67} COTS software is simply assumed to be free of bugs or malicious logic and impenetrable to outside attack. Those who defend this rule believe that because COTS software is so widely used, it has been thoroughly tested and must be reliable. However, the facts prove otherwise. New security vulnerabilities in COTS software are discovered every day, with over four thousand new COTS vulnerabilities reported in 2002 alone.\textsuperscript{68} In order to reduce security risks, experts urge election officials to refrain from using any voting system that relies on COTS software and to adopt a continuous certification program, which would allow Internet voting systems to be decertified when new vulnerabilities have been identified and then re-certified once effective measures have been taken to address the new threats.\textsuperscript{69} Together, a combination of these methods would minimize the risk of security vulnerabilities inherent in a software system.

\textsuperscript{65} Caltech-MIT Voting Technology Project.
\textsuperscript{66} Department of Defense Washington Headquarters Services FVAP.
\textsuperscript{67} Mercuri, “The FEC Proposed Voting Systems Standard Update.”
\textsuperscript{68} Jefferson, Rubin, Simons, and Wagner.
\textsuperscript{69} Internet Policy Institute.
4.3 Attack on Communications Path

Unfortunately, none of the above risk mitigation strategies address the possibility of an attack on the communications path between the client and the server. In order for Internet voting to be secure, not only must the client and the server each be impenetrable from any sort of attack, the communications path between the client and the server must be reliable, robust, and secure. This requires both the maintenance of an authenticated communications link between the client and the server and the preservation of the confidentiality and integrity of data being transported. Digital signatures and other cryptographic techniques currently exist for ensuring that both the secrecy and the integrity of data is preserved while in transit, so that ballots are protected from prying eyes and from unauthorized manipulation while being transported from the user’s browser to the elections server.\(^70\) However, there are no known means for guaranteeing the maintenance of an authenticated communications link.

Poll site and kiosk voting can circumvent this problem by incorporating the functionality of a DRE into each machine, so that if communication with the server is interrupted, votes can be stored on each individual machine for later tabulation. However, remote Internet voting necessitates a reliable communications link because it is undesirable to store votes on a personal computer for ballot secrecy and other practical reasons. There are numerous ways an attacker can disrupt or fake an authenticated communications link, including a denial of service (DOS) attack, spoofing, and a Domain Name Service (DNS) attack.

4.3.1 Denial of Service Attack

There are two methods for launching a denial of service (DOS) attack. One is to flood the network connection of a web server with junk data, thus preventing legitimate data from passing through. Another is to swamp a web server with useless tasks, thereby taking up all of

\(^70\) Done.
its computational resources so that it cannot respond to connections from legitimate users. Even worse than a DOS attack launched from one machine is a distributed denial of service (DDOS) attack, in which many machines collaborate to mount a joint attack on the target. This can be accomplished by first taking control of many computers in advance, through one of the delivery mechanisms discussed earlier (such as viruses or worms). Once infected, these computers become “zombies” or “slaves” that obey all subsequent commands from the master machine, allowing the attacker to overwhelm its target with a simultaneous flood of data or requests.

With current technology, there is no way to prevent a determined DOS attack, nor is there any way to stop an attack once it has been launched without closing down all unrelated and legitimate communications. Past experience with DOS attacks further demonstrates their existence as a real and present threat capable of wreaking havoc. In February 2000, a massive DDOS attack shut down many of the main portals of the Internet simply by installing and executing publicly available attack scripts.\textsuperscript{71} This attack required little skill to launch, meaning a determined adversary or team of adversaries could do much more damage. The ease with which DOS attacks can be perpetrated has resulted in their becoming quite commonplace: according to the Cooperative Association for Internet Data Analysis, there are, on average, four thousand DOS attacks on the Internet every week.\textsuperscript{72} When Canada provided remote Internet voting as an option for its National Democratic Party (NDP) leadership convention in 2003, thousands of voters were unable to log on and cast their ballots due to a DOS attack that paralyzed the central server.\textsuperscript{73} Though this disruption lasted less than an hour, causing little more than temporary

\textsuperscript{71} Rubin.
inconvenience and frustration, a determined DOS attack persisting throughout Election Day could easily disenfranchise millions of voters. While an extended voting window can help to alleviate the extent to which DOS attacks are a problem, it cannot eliminate the possibility that they will affect a large portion of voters, as experience has demonstrated the common tendency to wait until the last day to vote.

4.3.2 Spoofing and Man-in-the-Middle Attacks

Spoofing involves deceiving a user in order to gain access to information or resources. In the context of remote Internet voting, attackers can spoof the web page of the election server by tricking voters into believing that a fake web page is the legitimate voting site. This type of attack can be accomplished by social engineering means, such as sending out mass e-mails telling users to vote by clicking on a link that takes them to a fake voting site. The attacker could then simply drop the votes, resulting in lost votes, or collect voting credentials to steal their votes. Such an attack can also easily be launched on any public or institutional computer: the attacker can program the computer to simulate a valid connection to an election server without actually making any connection. In this way, many votes could be lost or altered, possibly affecting the results of an election.

A man-in-the-middle attack is a type of spoofing that involves intercepting and manipulating traffic between a user’s browser and a legitimate web server. Secure sockets layer (SSL) is the standard procedure currently used to protect the confidentiality of Internet transactions. It works through a “handshake,” in which the user’s browser and the server exchange session keys for encrypting data. A vulnerability of SSL is that an attacker can intercept the traffic going between the user’s browser and the server, pretending to be the server
to the user and pretending to be the user to the server. Rather than exchanging session keys with each other, the server would exchange a key with the attacker, who would exchange his or her own key with the user’s browser. Thus the user would unknowingly encrypt all information using the attacker’s key, so that the attacker can decrypt, read, and alter the message before encrypting it with the server’s key to send to the server. By intercepting and controlling all communication between the user and the web server, the attacker is able to monitor and modify the data that the web server receives, compromising both the secrecy and the integrity of the ballot in a remote Internet voting system.

The only way to protect against a man-in-the-middle attack with SSL (and against spoofing in general) is to verify that the server’s digital certificate has been validated by a certificate authority (CA). Because CAs play such a vital role in ensuring communication with legitimate servers by acting as trusted third parties, any lapse in their identity verification destroys the security of SSL. The real setback, however, is the fact that the average Internet user is not familiar with this technology. Even though a combination of SSL and digital certificates allows one to distinguish legitimate servers from malicious ones, most voters lack the technological expertise to verify the authenticity of a server certificate and to check the active ciphersuites to ensure that strong encryption is used. In fact, the vast majority of users would not be able to distinguish between a web page with an SSL connection to the legitimate server and a web page of a malicious server, if the two looked exactly the same.

4.3.3 Domain Name Service Attack

An attacker could also target the Domain Name Service (DNS), which acts as the address book of the Internet, maintaining a mapping from Internet Protocol (IP) addresses, which

---

75 Rubin.
computers use to reference each other, to domain names, which people use to reference websites. A DNS attack could be a form of DOS or a type of spoofing, depending on the tactic taken by the attacker. A DDOS attack on the DNS could disenfranchise voters by preventing users from being able to access the voting site. Even worse, cache poisoning, a known vulnerability of DNS, would allow an attacker to change the information available to hosts about the IP addresses of computers, so that when users try to reach the election server, they are directed to the wrong site. In other words, a user who follows the instructions for remote Internet voting and types in the domain name of the election server may receive a page that looks exactly like the real voting site but is actually a fake site controlled by an attacker. While detailed instructions on how to check the validity of a site’s digital certificate can be provided, it is unlikely that all or even most users will take the time to follow them.

The underlying reason that DOS, spoofing, man-in-the-middle, and DNS attacks are so easy to perpetrate and difficult to defend against is that security was not a priority when the Internet was originally designed in the late 1970s. Instead, the primary design goals were scalability, ease of use, communication performance, and reliability. As a result, the basic data transmission, naming, and routing protocols (known as TCP/IP) created for the Internet then and still in use today rely on the open, forgeable source addresses on each packet being transmitted and depend on the voluntary cooperation of thousands of corporations around the world to keep its naming and routing infrastructure consistent. Lacking a security architecture, it is unsurprising that the Internet is riddled with general vulnerabilities. The fact that the routers and servers that act as the backbone of the Internet are merely computers with their own array of security vulnerabilities only exacerbates the precariousness of the Internet as a medium for

---

70 Lemos.
77 Rubin.
communication. The myriad of risks associated with reliance on such an unreliable communications path make remote Internet voting inherently insecure.

5. Social and Political Ramifications

Regardless of how secure an Internet voting system may be, there are those who oppose Internet voting for a variety of other reasons. For the most part, their criticism is focused on remote Internet voting. Because remote Internet voting would be a radical departure from conventional polling place voting, they are concerned about the social and political consequences of implementing such a system. In particular, remote Internet voting could have a negative effect on minority representation, on public confidence, on the deliberative nature of American legislation, and on the general character of elections.

5.1 Equal Access

One of the main arguments against remote Internet voting is that it would favor those who have Internet access at home. Even if kiosks are provided at public places, such as traditional polling places, shopping malls, and libraries, those who are able to vote without leaving the comfort of their homes are afforded greater convenience. Some would argue that making the act of voting easier for some voters and not for others is the same as levying a poll tax against those who do not have Internet access. Another possible harm could be that the higher level of convenience for those who have home Internet access would translate into greater voter turnout among that portion of the population, thus diluting the votes of those who must still travel to a polling place or other location to cast their ballots.

On the other hand, the existing voting system cannot be said to be fair to poor and minority communities either. The U.S. Commission on Civil Rights found that poorer and

---

79 Governor’s Task Force on Election Procedures, Standards and Technology.
minority communities more often utilized less modern equipment that was prone to overvotes and other errors than their wealthier, white counterparts.\textsuperscript{81} If implemented statewide rather than on a precinct by precinct basis, a remote Internet voting system would allow voters throughout the state to cast their ballots by the same means. While requiring all precincts to use and maintain the same type and quality of equipment could achieve the same goal, it would require the mass simultaneous purchase of voting equipment.

Another question that has been raised concerning accessibility involves the cost of digital certificates. For voter authentication purposes, digital certificates are a necessary part of many proposed Internet voting schemes, but few computer users own digital certificates today. Thus, requiring a digital certificate to vote would greatly reduce the number of people who could vote online. In order to make Internet voting available for the general public, any mechanism necessary for security would have to be provided by the government free of charge. This is not entirely improbable in the foreseeable future. Various states and federal agencies have already begun considering digital signature legislation that would provide a digital certificate to any citizen who requested one.\textsuperscript{82}

In order to evaluate whether an Internet voting system would have a discriminatory effect, it is necessary to understand exactly how widespread Internet access is and whether certain portions of the population do in fact have significantly greater access to the Internet. According to U.S. Census data in August 2000, 41.5\% of all households had Internet access, an increase of 58\% since 1998.\textsuperscript{83} This rapid growth in Internet usage is expected to continue for some time, so it is not unlikely that Internet access at home will one day become as

\textsuperscript{81} Bederson, Lee, Sherman, Herrnson, and Niemi.
\textsuperscript{82} Department of Defense Washington Headquarters Services FVAP.
commonplace as having a telephone and a television at home is now. Moreover, the statistics are even more optimistic when considering Internet access at any location, rather than just at home: approximately 92% of the voting age population already has some form of Internet access. Though a digital divide remains, the fact that Internet access has rapidly increased among most groups of Americans, irrespective of income, education, race, location, age, or gender suggests that eventual digital inclusion may be a realizable goal in the not-too-distant future.

Nonetheless, several factors currently play a significant role in the likelihood that one has access to the Internet. Individuals with a disability are half as likely to have Internet access as those who are not disabled, and the rates of Internet access are even lower for those with impaired vision or problems with manual dexterity. Thus, a remote Internet voting system may not actually provide the disabled with much increased access. In addition, a recent study by the U.S. Department of Commerce found that income remains a significant factor in Internet accessibility. Education continues to play a considerable role as well: those who have received higher levels of education are significantly more likely to have access to the Internet at home. Race is another powerful determinant of Internet access. Currently, white voters have more Internet access than most ethnic minorities, and this disparity is particularly evident when comparing white voters to black and Hispanic voters.

Age is also an important factor determining the likelihood of Internet access. Those who are 50 years of age or older are far less likely than their younger counterparts to have access to the Internet. Some advocates of Internet voting point out that rates of voter participation have traditionally been the highest among those who are 65 and older and the lowest among 18- to 25-

---

84 Done.
85 U.S. Department of Commerce.
86 Phillips.
Since many of those who are least likely to vote are also the most likely to use the Internet on a regular basis, Internet voting could have a balancing effect on voter participation. Generally speaking, those who are young, affluent, well-educated, and white are more likely to have regular access to a computer connected to the Internet than their older, poorer, less-educated, minority counterparts. However, these demographic trends are changing rapidly. For example, senior citizens have experienced the highest rate of growth in Internet access and usage among all age groups—53% growth. Similarly, Internet access in black and Hispanic households has increased two-fold in just twenty months. Additionally, as the price for computers and Internet Service Providers (ISPs) decreases, the income gap is expected to shrink. By the time remote Internet voting can be implemented, the demographics of Internet access may be quite different.

In any case, there are several ways to address issues of unequal access. For the most part, concerns about unequal access are focused on remote Internet voting, which requires voters to procure voting equipment on their own. To alleviate any such inequity, election officials can provide voting booths with computers dedicated exclusively for voting in regular polling places and at other convenient public locations. Alternatively, they may take measures to ensure that computers that are already installed in public facilities are made available to the public during each election period. One drawback of the latter approach is that computers in public facilities may not provide adequate privacy for the voter and may be more vulnerable to viruses as well as to remote monitoring and control.

Furthermore, with any approach that merely provides physical access to the necessary machinery for Internet voting, critics remain concerned about the disparity in voters’ familiarity

---

87 California Internet Voting Task Force.
89 U.S. Department of Commerce.
with computers and Internet applications. This disparity could affect the ease with which individuals are able to vote and their likelihood of making an error. For example, older adults, who tend to take a longer time and make more errors when performing computer-based tasks, may find Internet voting to be an intimidating experience. Studies have shown that those who use computers frequently tend to feel more comfortable with a computer-based voting system and find it easier to correct mistakes while voting on a computer. For this reason, Internet voting should be introduced as a supplementary option rather than as a replacement for conventional voting methods.

Several federal and state laws mandate equal access to the voting process. In particular, Section 5 of the Voting Rights Act of 1965 prohibits any change in the voting process that would result in more racial discrimination in voting than currently exists. Thus, any Internet voting system must ensure that it does not adversely affect minority voters. To date, all lawsuits against small scale Internet voting experiments have been defeated, suggesting that the courts do not perceive Internet voting as adversely affecting minority, low income, or elderly voters, so long as alternative voting options remain available and computers with Internet access are provided for those who would not otherwise have access.

5.2 Public Acceptance

Because elections are the means for voicing the will of the people, the legitimacy of a democratic government hinges on whether people accept election results as valid. The debacle with butterfly ballots and hanging chads in Florida during the 2000 presidential election demonstrated the importance of voting technology and public perceptions of its fairness. The method by which people vote has a direct effect on their willingness to accept election results as

---

90 Bederson, Lee, Sherman, Herrnson, and Niemi.
91 California Internet Voting Task Force.
92 Done.
legitimate; only with a high degree of confidence in the accuracy, reliability, and security of voting technology is it possible to maintain public faith in the democratic process. Therefore, it is essential, not only that Internet voting be made accessible, user-friendly, and secure, but that the general public believes this to be the case. After all, if the average person has no means to verify that his or her vote was captured and counted accurately, the fact that a small number of mathematicians and computer scientists are able to analyze and prove that the voting system is reliable and secure may not be enough to overcome general public skepticism and to maintain public confidence in the system.

Some public opinion polls show a significant amount of concern among the general population about the security risks inherent in Internet voting. An ABC News poll, for example, found that 69% of all Americans believe that making Internet voting secure from fraud will take “many years” or will “never happen.” In another survey, 85% of respondents believed that an Internet voting system would be at least as secure as existing voting systems, but the remaining 15% did not even trust an Internet voting system to record the votes they intended to cast. This widespread lack of confidence is a serious issue that should be addressed before any Internet voting system is implemented.

On the other hand, some surveys reveal almost unanimous support for Internet voting. An Internet voting pilot project in Phoenix in 2000 found that 97% of respondents preferred Internet voting over existing systems. To a large extent, support for or opposition against Internet voting reflects not only security concerns but also the comfort level that people have with Internet applications and with computers in general. A nationwide poll reported that only 19% of the population over 65 would support Internet voting even if it would be secure from

---

93 California Internet Voting Task Force.
94 Bederson, Bonshin, Sherman, Herrnson, and Niemi.
95 Done.
fraud; likewise, a statewide survey by the Public Policy Institute of California found that while approximately 60% of those aged 18 to 34 look favorably upon Internet voting, 71% of those over 65 oppose it. Clearly, older adults who generally are less familiar with computers and the Internet tend to disapprove of the idea of an Internet voting system, while younger, more Internet-savvy adults tend to support an Internet voting scheme.

There are several measures that can be taken to increase public confidence and comfort with Internet voting. Once the technical obstacles to security have been surmounted, voter education is important for increasing public awareness about the means by which Internet voting is protected from both outside and inside attack. Public education campaigns demonstrating how to vote over the Internet, whether through television commercials or free instructive software, can also alleviate anxiety by increasing voters’ familiarity with the voting process.

Some of the distrust and discomfort with Internet voting may be due to the loss of transparency when vote capture, storage, and tabulation are accomplished invisibly with electronic bits in a machine. While voting technology has typically become less transparent over time, evolving from a public show of hands to machine-counted optical scan ballots, Internet and electronic voting in general is such a closed and opaque process that critics have dubbed it “black box voting.” Making all levels of the Internet voting process open and transparent—from the method of encryption used to the source code for vote tabulation—and conducting random or small-scale audits of votes and equipment, even when a recount is not called for, can help to increase public faith in the system. Ultimately, the best way to improve voter trust would be to provide a simple means for personally verifying that one’s vote has been correctly counted (without violating ballot secrecy), but this is a challenge that has yet to be solved.

96 California Internet Voting Task Force.
5.3 Direct Involvement

Internet voting, by lowering the cost of holding an election, may make it possible to conduct elections more frequently. This may result in citizens becoming more directly involved in government decisions. By providing the opportunity for civic participation on a more regular basis, more frequent elections could help to counter the growing political apathy among Americans. It may be that many eligible voters do not exercise their right to vote because the relatively infrequent occurrence of elections leaves them feeling removed from the political process. If elections were held more frequently, voters could participate in the political process on a more regular basis, and they may also feel more compelled to vote because the smaller, more concrete issues brought up in referendums are of more obvious importance and relevance to their daily lives.

At the same time, increased direct involvement in government decisions has the potential to undermine the deliberative nature of the American political system. More frequent elections would allow politicians to decide all difficult or controversial issues by popular vote. In moving from a system of representative government to a direct democracy, the policy expertise and reflection that takes place in the legislature would be lost. Therefore, increased direct involvement may prove to be more detrimental than beneficial.

5.4 Character of Elections

In addition to concern about the political consequences of greater direct involvement in government, some fear that Internet voting would eliminate the ceremonial aspect of voting and that the loss of this civic ritual would diminish the significance of the act. Certainly, remote Internet voting is less of a public act because it does not involve physically going to a polling place.

---

98 Internet Policy Institute.
99 Coleman.
place to cast a ballot, but the same is true for absentee and other by-mail ballots. There are those who would argue that these by-mail voting schemes do in fact result in a loss of social capital and perhaps even lower rates of civic participation, but further research is necessary to prove or disprove such claims. However, simply because voting with a few key strokes or a few clicks of the mouse would replace punching a hole in a card or moving a lever does not necessarily mean that the act of voting would become less of a ritual. After all, the ritual of voting has been evolving since its inception. Early American elections used simple methods such as a public show of hands or the placing of beans in a box. Since then, voting technology has undergone considerable change, from pre-printed paper ballots to optical scanning systems, and many of these changes have improved elections by introducing ballot secrecy and making it more difficult to rig an election by stuffing ballot boxes. Hence, though public confidence and comfort is important, fear of change in and of itself ought not to be an impediment to the implementation of new voting technology.

6. Past, Present, and Future

While political and social scientists have speculated on the possible ramifications of Internet voting, both private and public organizations have embarked on small scale experiments in Internet voting. These pilot projects have provided much valuable insight into the social and technical obstacles to such a voting system. Based on these experiences and the potential for breaches in security, experts have come to varying conclusions about the feasibility of Internet voting and offered recommendations for improving the current voting system.

101 California Internet Voting Task Force.
6.1 Pilot Projects

The first Internet election in American political history took place in Alaska on January 24, 2000. Through VoteHere.net, over three thousand voters in three remote election districts were given the option of casting ballots through the Internet for the Republican Party’s presidential straw poll. Disappointingly, less than a hundred votes were actually cast online. Since then, various organizations and government agencies have experimented with their own Internet voting pilot projects.

Following Alaska’s non-binding virtual straw poll was the first binding political election to include Internet voting—Arizona’s 2000 Democratic presidential preference election. Leading up to and during the election, this remote Internet voting system experienced several difficulties, ranging from legal challenge to system compatibility issues. Nonetheless, it accomplished its chief goal of increasing voter participation and thus demonstrated the power of Internet voting to draw non-voters to the virtual polls. In the same year, for the November 2000 general election, the Federal Voting Assistance Program (FVAP) implemented another small-scale remote Internet voting experiment. The Voting Over the Internet (VOI) Pilot Project was designed as a proof of concept demonstration, involving less than one hundred participants, mostly overseas military personnel. Despite hitting several snags, FVAP assessed the VOI project to be a success that required further research and expansion to explore scalability and security issues.

103 Done. See Appendix I for more details.
104 Department of Defense Washington Headquarters Services FVAP. See Appendix II for more details.
As a follow-up and extension of the VOI project, FVAP embarked on the Secure Electronic Registration and Voting Experiment (SERVE).\textsuperscript{105} Originally, SERVE was designed to allow thousands of military personnel and overseas citizens to vote remotely through the Internet for the 2004 primary and general elections. Due to intense criticism by computer scientists, however, this experiment was never fully implemented. Many of the security vulnerabilities cited by these experts are inherent to current PC design and Internet infrastructure rather than specific to the SERVE system. Nonetheless, political parties and entire governments have continued to forge ahead with remote Internet voting schemes. Despite security flaws, Michigan’s Democratic Party went ahead with its plans to allow remote Internet voting in the 2004 presidential primary. As a result, over 46,000 voters cast their ballots online, a tremendous increase over past caucuses.\textsuperscript{106} Likewise, European nations, such as Switzerland and Estonia, continue to view Internet voting as holding great promise and have persisted with their plans to provide remote Internet voting in local and nationwide elections.\textsuperscript{107}

6.2 Feasibility of Internet Voting

Experts generally agree that poll site and kiosk Internet voting can be responsibly implemented in the near future.\textsuperscript{108} Though poll site and kiosk voting systems do not provide the expedience that remote Internet voting offers, they can provide some degree of greater convenience by allowing voters to vote at a whichever site they find most convenient—whether it is a traditional polling place, shopping mall, or public library—rather than restricting them to their home precinct as is currently the case. Securing such a voting system is feasible because

\begin{itemize}
  \item \textsuperscript{105} Jefferson, Rubin, Simons, and Wagner. See Appendix III for more details.
  \item \textsuperscript{106} Internet votes alone would have been the third largest caucus turnout and twice the size of the 2004 caucus turnout. Stacey Range, “Internet Voting Wins Praise of Party Leadership,” \textit{Lansing State Journal} 8 Feb. 2004, online, Internet, 18 Feb. 2004.
  \item \textsuperscript{108} National Science Foundation, “Internet Voting is No ‘Magic Ballot,’ Distinguished Committee Reports” (6 Mar. 2001), online, Internet, 11 Feb. 2004
\end{itemize}
election officials are able to maintain some control over the voting equipment and physical environment. Thus, voting clients can be protected from malicious software, and for poll site systems, voter authentication and ballot secrecy can be enforced in the conventional manner. Additionally, several schemes have been suggested for providing a voter-verified audit trail, and if the communications path to the server is disrupted for any reason, poll site and kiosk machines can function as DRE devices, storing ballots for later tabulation. Insider attacks remain a possible threat but one that many experts believe can be mitigated to an acceptable level of risk with open source code, “white hat” hacking efforts, and rigorous testing.

Whether it is technologically possible to design a secure remote Internet voting system is somewhat more controversial. While there is general consensus in the computer science community that remote Internet voting should not be implemented at this time, some experts believe that it is technologically possible to develop a remote Internet voting system that is at least as secure from vote-tampering as the current absentee ballot process in the near future. Others are convinced that numerous security risks exist in any remote Internet voting architecture which cannot be solved by any technological innovations in the foreseeable future. As a result, the likelihood that a hacker or team of hackers could successfully subvert the results of an election by launching a large-scale attack is far too high to be acceptable. As portrayed by a vehement opponent, remote Internet voting would allow people “to cast their votes from a computer full of insecure software that is under the direct control of several dozen software and hardware vendors and run by users who download programs from the Internet, over a network that is known to be vulnerable to total shutdown at any moment.” In addition to concerns about the inability to provide a secure election, many experts cite social reasons for holding

109 California Internet Voting Task Force.
110 Rubin.
back, such as the fact that a digital divide still exists and even those who have access to the Internet may not feel comfortable voting over the Internet.

Taking a cautious but more optimistic stance are a small group of computer scientists who see electronic voting as an improving technology with great potential despite its problems today\textsuperscript{111} and social science researchers who recognize that the technical obstacles to Internet voting are significant but do not believe them to be insurmountable.\textsuperscript{112} After all, the technology already exists for strong identity authentication, both for the voter and the election server, through digital certificates. It is conceivable that in the next few decades, digital certificates may become such a common part of everyday life that it would no longer be unreasonable to expect voters who wish to vote online to take the precaution of checking the server’s digital certificate and thus thwart any spoofing, man-in-the-middle, or DNS attacks. In addition to providing clear and easy-to-follow instructions on how to verify whether a site is legitimate, one could imagine a system which required voters to watch a five-minute film clip demonstrating this authentication process before they could receive or activate their government-issued digital certificate. Public education campaigns through newspaper advertisements and television commercials are also an effective means of reaching the general public.

The reliability of the communications path is of utmost concern because storing ballots on individual computers could threaten ballot secrecy and would create practical problems in ensuring that votes are delivered in time for tabulation. Internet communication could be disrupted in a variety of ways: DDOS attacks could crash routers, hosts, and election servers, or unintentional failures, such as server manager mistakes, network congestion, and power outages, could take place. Fortunately, there are several ways to greatly mitigate these risks and to

\textsuperscript{111} Caltech-MIT Voting Technology Project.
\textsuperscript{112} Done.
prevent them from unduly interfering with one’s ability to cast a ballot. Redundant Internet Service Provider (ISP) capacity, backup power sources, geographically separate backup servers, alarms, and redundant network paths all reduce the risk of a successful DOS attack. Extending the voting window beyond one day to a week or two before Election Day can help to reduce the threat as well. As a final safeguard, the option of remote Internet voting could be made available only up until the day before Election Day, so that those who tried unsuccessfully to vote online at the last minute could still go to a polling place or kiosk the next day to cast their ballots.

Short of requiring biometric verification, vote-selling through the sale of credentials remains a possibility. A completely automated vote-buying system can be prevented with challenges requiring one to type in the letters or numbers appearing as a visual graphic on the screen, but some large scale fraud can still occur. As noted earlier, if digital certificates become widely used and serve multiple purposes the way driver’s licenses function today, the likelihood that one would compromise his or her digital certificate merely for vote-selling purposes would decrease substantially. Moreover, some might argue that vote-selling is not really such a grave concern since it requires a large number of voters to be complicit.

Hence, the two greatest challenges remote Internet voting faces today are providing a voter-verified audit trail and preventing viruses, worms, Trojan horses, and any kind of monitoring or remote control program from recording or altering users’ votes without their knowledge. Because there are so many ways for malicious software to attack a personal computer, whether through email, website visits, or backdoors in commercial software, it would be irresponsible to simply allow voters to assume the risk that their votes may not be correctly counted. It is possible that a unique operating system could be designed exclusively for voting
purposes and distributed for free. Though this could circumvent many of the problems concerning malicious software residing on PCs, it introduces several additional complications, including the increased level of technological expertise required to vote online, the difficulty faced by those using public or shared computers in gaining authorization to install such a system, and the problem of delivering this system to voters in the first place. Alternatively, secure remote Internet voting could be accomplished if the next generation of personal computers widely adopted were designed with hardware support to enable a trusted path between the user and the election server, so that malicious code would be unable to monitor or subvert the normal operation of applications. Efforts such as the Trusted Computing Platform Alliance (TCPA) work toward this goal.

The more reliable and secure a voting system is, the less there is a need for a voter-verified audit trail. Even so, such an audit trail would be desirable, both to catch any attempts at vote manipulation and to boost public confidence in the system. Thus far, no one has been able to design a remote Internet voting system that would allow each voter to verify that his or her votes has been captured, transmitted, and counted correctly, but with researchers like Rebecca Mercuri and David Chaum working toward a solution, the possibility of a breakthrough remains.

6.3 Recommendations

Even if all of these technical challenges could be surmounted and digital inclusion eventually attained, the question remains, is it worth it? Are the potential benefits of Internet voting really worth the time, cost, and effort necessary to reach this goal? Most of the advantages of poll site and kiosk Internet voting systems, such as increased accuracy and easier access for the disabled, can also be realized through DRE machines not connected to the Internet.

---

113 California Internet Voting Task Force.
114 Rubin.
As for remote Internet voting systems, the benefit of convenience alone is probably not worth such expenditure. Though a significant impact on voter turnout would be a compelling reason to pursue remote Internet voting, it is disputed whether Internet voting would increase voter participation in the long run. Both the experiences of other countries and pilot projects lasting longer than one election can aid in assessing this potential benefit. Ultimately, however, the most persuasive case for implementing remote Internet voting lies with those who face the greatest difficulty voting by conventional means—servicemen and other overseas citizens. Those who serve in the military or on diplomatic missions dedicate their lives to their country, and it is patently unfair that many of them find themselves disenfranchised for this very reason.

Regrettably, with the current state of technology, it is not possible to provide secure and reliable remote Internet voting for military personnel and overseas citizens. Without a reliable method for defending against DOS attacks, a remote Internet voting system could result in the disenfranchisement of this segment of the population; unlike voters residing in the United States, they cannot simply go to a polling place to cast their ballots after experiencing difficulty with online voting. Fortunately, there are feasible alternatives for facilitating voter participation among military personnel and overseas citizens, and these solutions can benefit the general population as well. Two possibilities are remote Internet voter registration and a print and mail option.

6.2.1 Internet Voter Registration

Unlike Internet voting, Internet voter registration does not have the problems associated with protecting secrecy. Malicious code or a man-in-the-middle attack could still interfere with the registration process, but without the secrecy requirements of Internet voting, e-commerce-style security measures, such as paper receipts and comprehensive electronic logs, can be
implemented to detect such interference. DOS attacks are also less of a concern since voter registration usually takes place over a longer timeframe. While Internet voter registration would not provide the degree of convenience that Internet voting could offer, its potential benefits are substantial—expediting the process of voter registration, increasing voter registration, and improving the accuracy of voter registration rolls.

Most election officials agree that inaccuracies in voter registration rolls are currently the gravest threat to the integrity of the electoral process. Between 1995 and 1998, more than four million duplicate registrations were found, suggesting that millions of duplicates continue to exist undetected. It is also disturbingly easy to register fraudulently and to use outdated registrations to vote multiple times, whether by registering one’s pet cat or by voting for a dead person. In addition to facilitating voting fraud, inaccurate or outdated registration rolls can prevent eligible voters from voting. According to estimates by the Census Bureau, three million registered voters did not vote in the 2000 presidential election due to problems with their registrations.

Many of these registration problems stem from the decentralized nature of registration rolls. With the average American moving once every five years, many of these duplicate registrations result when individuals move and register at their new locale without notifying their previous voting precinct of their move. Unifying voter registration statewide would produce much cleaner, more accurate registration rolls, and an Internet voter registration system with access to registration rolls from any jurisdiction within a state would be an efficient and effective means for accomplishing this goal. Such a computerized system would go hand in hand with the

---

115 Internet Policy Institute.
116 Done.
117 Caltech-MIT Voting Technology Project.
118 The Governor’s Task Force on Election Procedures, Standards, and Technology.
development of better databases (perhaps assigning a numerical identification for each voter) and
the creation of a system allowing voters to check the status of their registration online.

Some experts have cautioned against allowing Internet-based voter registration due to the
potential for automated fraud. However, even if all first-time registrations were manually
processed according to current procedures, allowing subsequent updates over the Internet would
decrease both the administrative burden of local election officials and the number of duplicate
registration due to citizen mobility. After voters provide a manual signature for the initial
registration, election officials could provide them with digital signatures or other means of
remote identity authentication to allow status checking and future updates online. Allowing
voters to simply update their address online once, rather than having to notify both the new
precinct and the previous precinct of their move, would greatly alleviate the problem of duplicate
registrations. While this increased convenience and accuracy is beneficial for the general public,
it is particularly helpful for overseas military personnel and citizens. By providing a quick and
easy way to update one’s mailing address, an Internet voter registration system would reduce the
number of mailed ballots that are returned as undeliverable, a common problem for those
deployed on short-term assignments.

6.2.2 Print and Mail Option

Another alternative, which can be implemented in conjunction with Internet voter
registration, is to provide a website with the functionality of a remote ballot printer. Such a
website would provide instant delivery of a blank ballot to any citizen at any location with
Internet access, and since the ballot would be printed out, the voter would have the chance to
verify the choices indicated on the ballot before sending it in for tabulation. Thus, malicious

---

119 National Science Foundation.
120 Department of Defense Washington Headquarters Services FVAP.
software residing on the computer could not alter ballot contents without the knowledge of the voter. Once the ballot has been printed and verified, it would be mailed to election officials, according to current absentee ballot procedures. This print and mail option would have the additional benefit of providing a paper audit trail for random audits or recounts. While this system relies on the Internet as a communications path for downloading the ballot, as with voter registration, ballot downloading can take place early and over a long period of time, without requiring the voter to decide on candidates and issues far in advance. Such an option, in conjunction with Internet voter registration, would greatly decrease mail transit time by reducing the number of postal delivery trips from three to one, and this increased expedience would be particularly valuable for overseas military personnel and citizens.\textsuperscript{121}

7. Conclusion

Upon evaluating the myriad of security risks associated with remote Internet voting, it would be irresponsible to forge ahead with such a scheme at this time. Not only could a denial of service attack easily disenfranchise those who attempt to vote online, malicious software residing on personal computers could monitor and even subvert ballot contents without voters’ knowledge. Combined with the absence of a voter-verified audit trail, such vulnerabilities create an unacceptably high level of risk for large scale vote manipulation. However, various alternatives exist for expediting the voting process, making it more convenient and more accurate while providing an acceptable level of security with current technology. These include Internet voter registration and a print and mail option, both which would aid those who experience difficulties voting with current absentee procedures. In addition, voter education should be pursued. Such educational outreach programs can include distribution of training videos, deployment of sample voting machines at community and civic events, distribution of sample

\textsuperscript{121} Konrad.
ballots or ballot software through the media and public institutions, radio and television public
service announcements, and provision of videos for continuous play at polling places on Election
Day. Not only have such programs been shown to increase voter turnout, they increase accuracy
by ensuring that voters know how to cast their ballots properly.122

More research on Internet voting and other means for improving the current voting
system would be beneficial as well. The current level of election expenditures is so low that this
category does not even appear on the list of activities reported in the Census of Governments. In
fact counties and cities spend more than ten times as much on solid waste management and on
parks and recreation than they do on elections.123 With more funding, the federal government
could establish a National Elections Research lab similar to the one in Brazil, which has proven
to be both innovative and successful.124 Though electronic and Internet voting pose significant
risks, we must not to be deterred by these risks because “there is an even greater risk that inertia
might leave us in our current dilemma. We should not tolerate things as they are; the
inadequacies of our voting system threaten our democracy.”125

122 The Governor’s Task Force on Election Procedures, Standards, and Technology.
123 Caltech-MIT Voting Technology Project.
124 Garfinkel.
125 Caltech-MIT Voting Technology Project.
Additional Sources


Online. Internet. 5 Feb. 2004


Internet. 11 Apr. 2004


Appendix I: Arizona’s 2000 Democratic Primary

Prior to Arizona’s 2000 Democratic primary, all registered Democrats were mailed a randomly generated seven-digit alphanumeric code. In combination with a series of challenge questions based on voter registration information, this code allowed the remote Internet voting system to accomplish identity authentication. Voters were provided the option of voting remotely through any computer connected to the Internet in addition to the conventional methods of casting ballots by mail and at regular polling places. Election.com designed the system with a combination of database design, cryptography, oversight, and audit trails to protect the secrecy and security of ballots. Once a voter cast a ballot, all identifying information was removed from the ballot contents and stored, encrypted, in separate tables that could not be merged. Electronic transactions, such as voting, accessing the database server, and updating versions of software, were logged to create an audit trail, and a series of redundant servers and electrical power systems protected the voting system from power outages, DOS attacks, and other failures.

Even so, there were technical glitches which became apparent only after the system was put into operation. A network router crashed due to hardware malfunctions, and redundant equipment failed to respond. Though this was repaired in less than an hour, other problems occurred. Some voters with Macintosh computers were not able to cast Internet ballots because their software was incompatible with the voting security system. Others experienced difficulties because they were using older versions of Netscape Navigator that had Y2K-related bugs. Internet voting faced legal obstacles as well. The Voting Integrity Project sued to prevent Internet voting, claiming that it would have a disenfranchising effect on ethnic minorities because white voters were significantly more likely to have Internet access than African-
American and Hispanic voters were. In the end, the U.S. District Court ruled against them and allowed Internet voting to proceed.

Despite these difficulties, the primary goal was to increase voter turnout, and this experiment was a resounding success in this respect. Tens of thousands of new voters were drawn to vote online. Approximately 14,000 Arizona Democrats voted on the first day of Internet voting alone, exceeding the total number of ballots cast in the 1996 primary. By the end of the primary, 41% of all ballots had been cast remotely through the Internet. At the same time, this success cannot be entirely attributed to the new online voting system. The publicity from the lawsuit and the novelty of the experiment probably attracted some number of new voters. Additionally, the Arizona Democratic Party had increased the number of polling places by 35% from the last presidential preference election and had invested considerable effort in an extensive education and outreach program for voters. Nonetheless, this pilot project demonstrates the profound impact that Internet voting can have on voter participation when implemented in concert with a large-scale educational campaign.
Appendix II: Voting Over the Internet Pilot Project

Initiated by the Federal Voting Assistance Program (FVAP), the Voting Over the Internet (VOI) Pilot Project was a small-scale, limited-scope feasibility study allowing military service members, their dependents, and other overseas citizens in fifteen counties to register and to vote through the Internet for the November 2000 general election. Volunteers were mailed CD-ROMs containing custom software for enabling VOI-specific functionality. Ninety-one individuals used the VOI system to register to vote absentee, and eighty-four citizens actually voted using the VOI system. These participants consisted almost entirely of military servicemen because the system achieved identity authentication through Department of Defense Medium Assurance Public Key Infrastructure (PKI) digital certificates, which were available only to those in the military services.

This remote Internet voting system consisted of three main components: citizen workstations from which voters cast their ballots, a central FVAP server which served as a single point of entry for all data requests and activities on the system, and a Local Election Official (LEO) server segment. Though the FVAP server was judged to have increased the security of the entire system by providing an alarm against intrusions and a comprehensive audit trail for all system transactions, it was also a potential single point of failure that could have been vulnerable to hacking. In fact, the FVAP server was unavailable for short periods several times, and one LEO server failed temporarily on Election night.

There were other problems as well. Dependence on postal delivery for CD-ROMs greatly reduced the expedience that the Internet voting system was created to provide. The alternative—providing software for download through e-mail or a web site—runs the risk of spoofing, particularly for a larger scale implementation. Once they had received the CD-ROMs,
a considerable number of users experienced difficulties because they were using computers that they did not own and thus lacked the authorization to install the necessary software. While the PKI digital certificates provided a strong means of authentication, it also created numerous unexpected difficulties. Many voters did not receive their digital certificates until after the deadline had already passed for absentee registration, and the project was saved only because they had already submitted the conventional paper absentee registration forms as a precaution. Additionally, almost half of the digital certificates issued had to be reissued because voters had either forgotten their passwords or had allowed their certificate to expire by failing to “fulfill” it within thirty days (by accessing the PKI website and downloading the certificate to a floppy disk).

This pilot project revealed the downside of relying on passwords and on software that had to be physically delivered and then installed, particularly when a large segment of the population relies on computers that they do not own. While FVAP deemed the project largely a success, it also acknowledged the weaknesses of the VOI system, including its vulnerability to denial of service attacks and to malicious software at the citizen workstation. Though no attack was believed to have taken place, a larger scale implementation would receive more attention and thus would be expected to attract hackers.
Appendix III: Secure Electronic Registration and Voting Experiment (SERVE)

Under the auspices of the Department of Defense, FVAP designed the Secure Electronic Registration and Voting Experiment (SERVE) as an expansion of the VOI project. At the same time, this experiment served to fulfill a Congressional mandate to conduct an electronic voting experiment and to report on the feasibility of this technology in facilitating voter participation for those covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). Planned for deployment in the 2004 primary and general elections, SERVE would have allowed military personnel and overseas citizens in fifty counties in seven states to register and to vote remotely through the Internet and was expected to handle up to 100,000 votes.

Despite including various security mechanisms, such as the encryption of ballots using public key cryptography, this remote Internet voting system was deemed unacceptably insecure by four computer scientists in the Security Peer Review Group (SPRG). These experts attributed SERVE’s security vulnerabilities to three fundamental design choices. First, its reliance on the Internet as a link between the client and the server left it susceptible to DOS, spoofing, and man-in-the-middle attacks. Secondly, allowing voters to cast ballots on private PCs running proprietary commercial software made SERVE vulnerable to virus attacks and privacy violations through monitoring or remote control programs. Finally, since SERVE itself consisted of proprietary software and relied on COTS software, it was vulnerable to bugs, security holes, and insider fraud. Having found these security problems to be inherent to any remote Internet voting system, they strongly recommended abandoning the entire experiment. As a result of their critique, SERVE was never implemented.