Internet Voting: Will We Cast Our Next Votes Online?

Jeremy Epstein
SRI International

If I Can Bank Online, Why Can't I Vote Online?

This simple question is at the crux of many discussions of Internet voting. In short, online banking has checks and balances, visibility, liability, and recourse. If an unauthorized banking transaction occurs, you can see it in your statement. The bank is responsible for losses, and has the ability to reverse an erroneous transaction. And, above all, you and your bank both know that the transaction was on your account, and where to return the money!

With voting, your votes might be incorrectly tallied, but that's not visible to you. Your local election authority should not be able to tell which ballot is yours. And once your ballot is incorrectly tallied and the election results are finalized, there is no way to reverse or redo that tallying. Cryptographic voting methods can help with visibility by providing a Web site where voters can go after the election to verify that their votes were included in the total. However, there are limitations in that the underlying technology is too complex for typical voters to understand.

Also, the externalities are different. Because US banks are responsible for losses over $50 (presuming the customer informs them promptly), they have a significant motivation to secure their systems. Even so, there have been numerous examples of financial theft through fraud that takes advantage of inherent holes in Internet security, not even counting fraud that uses the Internet, such as phishing. With Internet voting, even a voter who can detect that his or her vote was recorded incorrectly will have very little recourse.

So What Is Internet Voting?

The term "Internet voting" refers to two rather different approaches: casting a vote using an ordinary computer that is not dedicated to voting (for example, at a home, an office, a cybercafé, or a library), or kiosk voting, using a dedicated computer to cast votes.

In both cases, the votes are transmitted over the Internet, but the difference between dedicated and nondedicated computers is critical. In the kiosk model, dedicated systems have the potential of being correctly configured and free of

Related Resources:

Reports

A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE) Jefferson D., Rubin A.D., Simons B., Wagner D.

Software Review and Security Analysis of Scytl Remote Voting Software Clarkson M., Hay B., Inge M., Shelat A., Wagner D., Yasinsac A.

Articles

RIES - Rijnland Internet Election System: A Cursory Study of Published Source Code Gonggrijp R., Hengeveld W., Hotting E., Schmidt S., Weidemann F. *E-Voting and Identity (LNCS 5767)*

Conferences and Workshops

Electronic Voting Technology Workshop (EVT)/Workshop on Voting Technology (WOTE): an annual multidisciplinary workshop focused on topics central to electronic voting

Reviews

malicious software. By contrast, ordinary computers are nondedicated systems that must be presumed to be under the control of someone other than the user, via malware, other computers on an open network, or software update services. This short essay considers only the use of nondedicated systems, although many of the issues raised are also applicable to dedicated systems. While such topics as online voter registration; online availability of blank ballots; policy issues, including certification of systems for Internet voting; and legislative and/or policy changes that might be needed to allow Internet voting are important considerations, they are outside the scope of this essay.

Advantages of Internet Voting

Internet voting is claimed to have several advantages over traditional precinct-based voting or voting by mail. First, it offers an opportunity for increased participation, especially by young people who are overall less likely to vote, but are comfortable with the Internet. However, in elections thus far using the Internet, this promise has not been fulfilled. To date, the most direct comparison between Internet and traditional elections is a neighborhood board election in Honolulu; the first election with Internet voting had turnout down 83 percent compared to the previous comparable election, although there may have been other contributing factors besides technology [1].

Another purported advantage is that Internet voting would allow military and overseas voters to obtain blank ballots, and to cast their ballots closer to Election Day. Due to mailing times and unreliable delivery, such voters' ballots are frequently not received, and voters must typically cast their ballots 30 days or more prior to the election. Voter convenience might also increase with Internet voting, as voters won't have to take the time to visit a polling location. However, for voters without home or work Internet access, this might not be an improvement.

Many voters with disabilities, who have been historically underserved, may benefit from greater accessibility. More sophisticated computers and accessories (for example, text-to-speech and sip-and-puff systems) could be used, without the expense of equipping every machine with such capabilities. Internet voting could also lower costs, as the number of poll workers and even polling locations would be reduced. Thus far, pilots of Internet voting have been much more expensive than traditional voting technologies [2], but economies of scale can reduce that in the future.

The Voting Threat Model

When thinking about the security of any system, it's important to think about the potential adversaries, including their skills and motivations. Voting has a very long history of adversaries deliberately tampering with elections, regardless of the technology used. In the case of voting systems in general, threats can come from insiders such as election officials and poll workers, technology vendors, and voters acting individually or in groups. In addition, Internet voting introduces as adversaries people who are not directly part of the election process, including anyone in the world with an Internet connection. Opportunities and motivation could come from individuals, organizations, or governments. While there have not (to date) been known attacks on online voting systems, related attacks have clearly shown motivation, including successful penetrations of both the Obama and McCain campaign Web sites during the 2008 US presidential election.

Evaluation of electronic voting
Volkamer M., Springer International Publishing, 2009.

Analyzing Internet voting security
Jefferson D., Rubin A., Simons B., Wagner D. *Communications of the ACM* 47 (10), 2004, pp. 59-64.

A coercion-resistant Internet voting protocol
Meng B. *ICSNC 2007* (Proc. of the 2nd International Conference on Systems and Networks Communications), Aug 25-31, 2007, p. 67.

No form of voting is completely secure, completely private, or easy for all voters to use and understand. We should not expect Internet voting to meet all of these goals. However, in considering Internet voting, we should ensure that it is no worse than forms of electronic or paper-based voting systems in use today, such as precinct count optical scan (PCOS) and vote by mail (VBM). In a PCOS voting system, the voter marks a sheet of paper that is scanned in the precinct and becomes the official ballot for recounts. PCOS voters commit their ballots for delivery through a system that is vulnerable to a small number of people, many of whom are known insiders. By contrast, in most Internet voting schemes, the voter commits his or her ballot to a delivery channel that is vulnerable to an unknown but large number of unknowable people worldwide. With VBM, voters are sent paper ballots to mark and return to the government. Voter fraud (including bribery, coercion, and suppression) is limited to the number of people who can physically obtain the actual VBM ballot. With most Internet voting schemes, voter fraud becomes feasible to anyone who can obtain (or guess) the voter's credentials, as well as anyone who can find vulnerabilities in the online voting system. Such vulnerabilities may include attacks on the voting computer that sends the electronic votes, the election server that receives the votes, or the networks connecting them.

General Problems with Internet Voting

Potential problems with Internet voting fall into several categories, many of which are related to issues with voters' computers. Does the machine represent the voter's intent? Displaying a summary can help, but voters tend not to review summaries, even if displayed accurately. In addition, malware could vote on behalf of a user. Estimates commonly claim 30 to 60 percent of all home and business computers are infected with some form of malware. While that malware isn't focused on voting, reconfiguring a botnet like Conficker to cast votes on behalf of voters would be simple--and changing even two percent of the votes can sometimes be enough to flip the election. Another issue is compatibility: Is the voting software compatible with voters' computers? While computers are more likely to be updated than in years past, thanks to automated and mandatory patching, there are a surprisingly large number of variations of configurations -- as anyone who isn't using Windows with Internet Explorer can attest when running across numerous web sites that just don't work. Internet voting could also make it easier to coerce voters or buy their votes. In a technique used in Estonia, a voter could cast as many ballots as desired, but only the last one was counted [3]. With this scheme, vote buying or coercion only works if you can prevent the voter from casting a replacement ballot.

Also of concern is how elderly, low-income, and rural voters (who are much less likely to have personal computers and Internet service) can cast Internet votes. Dedicated voting sites with computers can be set up, but this replicates the problems of traditional precincts, and provides separate-but-unequal access. Library computers are reasonably common, but are typically set up to minimize privacy to discourage inappropriate Web surfing; this is at odds with the right to a secret ballot. While greater accessibility for the disabled is a possible advantage, as noted above, many of these voters do not have access to such technologies; Internet voting could disenfranchise them. Finally, how can the privacy of the voter's action be guaranteed? Voters who use their employers' computers to vote may be monitored, as keystroke logging and similar technologies are frequently (and legally) used in the workplace.

Another set of issues crops up on the server side, where votes are collected. A major concern is securing the system against potential attacks from anywhere on the Internet. Attacks aren't limited to attempts to tamper with votes and tallies, but also include denial of service attacks that prevent voting in the first place. Also, how can insider attacks by election officials or technology vendors be detected or prevented? Cryptographic voting schemes can help here, but are extremely difficult for voters and election officials to understand. We all know that bugs commonly affect software, and voting is no exception. What if bugs in the vote totaling software cause incorrect results? Finally, vote counting needs to be transparent, so voters will have confidence that the correct person is selected. Or, as Dan Wallach famously said, "The purpose of an election is not to name the winner, it is to convince the losers that they lost."

Other issues relate to voter authentication. For example, how does the voter identify and authenticate herself? Common identifiers such as social security numbers or driver's license numbers are frequently misused as authenticators. Smartcards could be used for this purpose if they were uniformly available to all eligible voters. We need to know who a voter is without connecting her to her ballot: authentication needs to be separated from voting.

As a result of the above challenges, many computer scientists have opposed moves toward Internet voting. The SERVE report (www.servesecurityreport.org) is among the better-known critiques of Internet voting that describe the above issues in depth. Also, a group of prominent computer scientists have set forth recommended requirements for Internet voting in a public letter at http://www.verifiedvoting.org/article.php?id=5867.

2010 in Review, and 2011 Looking Forward

In mid-2010, the Federal Voting Assistance Program (FVAP) and the US Election Assistance Commission (EAC) convened a workshop of scientists and election officials to discuss Internet voting technologies and solutions. The result was a deadlock, with scientists insisting that Internet voting is unsafe, and election officials mostly arguing that non-Internet solutions are inadequate for overseas voters.

The 2010 Congressional elections marked a turning point in the use of Internet voting. Thirty-three states allowed military and overseas voters to download blank ballots. A handful of states allowed the return of marked ballots by email, generally with voters explicitly waiving their right to a secret ballot.

Most importantly, the District of Columbia (DC) performed a groundbreaking experiment in which they created an open-source system for ballot download and return, and for a few days invited the public to investigate its security. Of the major categories of attacks described above, only server attacks were allowed. A team from the University of Michigan broke the system within 36 hours, installing code that retrieved all votes already cast, and modified the software so that all future votes were cast for a series of fictional characters. To ensure that no one missed this hack, the software was modified to play the Michigan "fight song" after each vote was cast.

The DC system was built by a well-trained staff, and the code quality was significantly better than commercial offerings. The fact that it was broken so quickly

was a demonstration that Internet voting is unwise, and DC appropriately backed off from their plans to allow online ballot return.

Despite the DC experiment results, West Virginia proceeded with their plan to allow online ballot return using proprietary software that has not been subject to any public security tests, relying entirely on the vendor's assurances and the mistaken belief that proprietary software is more secure than open source by virtue of being secret.

In early 2011, FVAP convened a second workshop of scientists to develop recommendations for state and local election officials to use in procuring blank ballot distribution systems. That effort, expected to result in a report by June 2011, is intended to solve the "easy" part of the problem in time for the 2012 elections. [I am unaware whether this report was ever written; it was never released.]

Five More Years -- And Little Progress

This essay was originally written in 2009, and updated (as noted above) in 2011. This update, in 2016, reflects an environment with minimal changes over the past five years. Approximately 30 states still allow overseas military voters to cast their ballots over the Internet (mostly by email, with a few using web forms). To my knowledge, if any of these states have performed a security assessment of their systems (and I am unaware of any such assessments), they have not been released to the public.

There have been no reported breaches of Internet voting systems, but such breaches would not be detected unless someone was explicitly looking for them. FBI reports indicate that the average web site break-in (for example, of e-commerce or government web sites) is not discovered for three to six months after the attack; if an election system is wiped after the election is certified, it is unlikely that any successful attacks would ever be discovered. Hence, it is hard to draw comfort from the lack of any reported problems.

Voter authentication was a concern in 2009, and is still a concern in 2016. While some localities use postal mail to send authentication tokens (for example, a PIN), others email the information, meaning that an adversary who takes control of a voter’s email account would have all necessary information to authenticate as the voter.

Political parties have experimented with holding primaries using the Internet, without any serious attention to security risks, or even to reliability. For example, the Utah Republican primary in 2016 suffered from usability problems, overloaded systems, and insufficient technical support, as well as the potential for a voter to both vote online and in person, due to lack of synchronization of voter rolls. (See http://www.standard.net/Government/2016/03/22/Utah-Republicans-complaints-issues-online-caucus-voting-GOP-Presidential.html) Since the 2016 presidential primaries have been much more contentious than most years, it is difficult to discern whether Internet voting had any impact on turnout, but as can be seen in the Utah example, any results should be treated with a large grain of salt. In 2012, a third party (Americans Elect) attempted an online presidential primary, but without significant attention to security. The seemingly small impact of the effort probably provided a measure of security through irrelevance.

Some states have recognized risks, but have addressed them by shifting responsibility to the voter. For example, Alaska allows any voters to vote using the Internet; however, they must also sign a waiver that they are giving up their right to a secret ballot. A recent study by EPIC shows that nearly all states have a constitutional or legal requirement for secret ballots, but rely on a wide range of methods for waiving those rights by voters using the Internet. Whether such waivers are in fact legal is a subject of some debate.

On the positive side, as a side effect of the Snowden revelations, an increasingly large fraction of emails are now encrypted from point to point, reducing the risks of tampering at certain stages. However, emails are not encrypted end to-end (with rare exceptions), so tampering at various waypoints is still possible. Unfortunately, this does nothing to address the risks of tampering before the ballot is sent or once it is received.

Several states have looked at using common access cards (CAC), which are smartcards issued to military members and contractors, as a way to encrypt and digitally sign emails, as well as to provide authentication. However, at the time of this writing, no states are using CAC cards for voting, although South Dakota at one point used a photograph of a CAC card for authentication (which provides no security).

In 2015, the US Congress removed the requirement for the Federal Voting Assistance Program (FVAP) to provide methods for Internet voting. Once that requirement was waived, FVAP released the sanitized results of a study it had performed several years earlier of commercial Internet voting products; the study was vague, but indicated that the products were vulnerable to attack. (Whether the study was released voluntarily or in response to a Freedom of Information Act (FOIA) suit by EPIC is unclear.)

Public understanding of the risks to computing systems has continued to grow, highlighted by large break-ins compromising credit cards (for example, Target), medical records (for example, Anthem’s 78 million records), and government systems (for example, the Office of Personnel Management compromise of all federal workers). There is no doubt that security risks continue to grow, but without a corresponding growth in protection for Internet voting.

In summary, the risks are greater than they were when this essay was written, but some states continue to proceed with Internet voting, seemingly oblivious to the increasing tide.

Research Needs

Over the past ten years, a handful of Internet voting pilot programs have been implemented around the US and in other countries, as well as a few full-fledged elections in Europe. In many cases, the elections were driven by research in cryptographic voting technology, which can address some (but not all) of the problems described above. As the US Congress and many states are moving toward encouraging Internet voting (especially for military and overseas voters), research is needed to address a few key questions.

First, can the general public understand or believe in cryptographic voting techniques enough to be satisfied that their votes are counted and legitimate? This question primarily addresses a need for usability testing: While there has been

significant research into the mathematics of cryptographic voting, preliminary studies indicate that voters do not understand how the vote counting works, or how to perform the necessary steps for a voter to ensure that the vote counting is accurate. While understanding is not always necessary--most people don't understand how a jet engine works, but continue to get on airplanes--voting must be understood since it is the basis of democracy.

Second, can we come up with noncryptographic schemes that meet the needs for privacy and security, and are easier for the public to understand? Many of the Internet voting systems in use today are based on noncryptographic schemes, but they do not have the properties of provable accurate counting. On the other hand, they can be understood reasonably well by voters. This highlights a critical research topic: finding a middle ground, where the voting system can be understood and also trustworthy.

Third, are there ways to address the disconnect between what the voter sees on the screen and how his or her vote is cast, so the voter doesn't have to trust the software to represent his or her intent? The solution to this question is perhaps the most difficult, as it requires finding methods that allow proof from the vote collecting system back to the human, not the software, that the votes were cast as intended. To do this successfully, both the technical aspects (How can we make it happen?) and the human factors aspects (How will users respond? Will they be able to perform the necessary steps correctly?) must be addressed.

Accomplishing the above research requires significant investment in both technical and usability research, including large-scale human subject tests. However, human subject tests are particularly difficult for voting technologies, because the factors that motivate voters must be replicated in the experiment, without compromising voter privacy in a real election. Voters can't be told which candidate to vote for in a real election to judge the efficacy of a voting technology, and, in a simulated election, they won't have the same motivation to ensure that their candidates are selected.

Conclusion

Internet voting continues to gain public attention, due to market pressures, such as the demand for easier voting by military voters and the desire of younger voters to vote online, just as they do everything else online. Issues with long lines in elections (especially the 2012 presidential election) have galvanized political interest in the topic, but have not helped solve the technical or policy problems. Researchers have the opportunity to ensure that the systems built and fielded meet the requirements of usability, security, privacy, accessibility, reliability, and transparency. These opportunities certainly include demonstrating and educating the public and elected officials about areas where Internet voting is inferior from a security and privacy perspective to other forms of voting. But there are also opportunities for performing the technical work necessary to minimize those weaknesses, and to ensure that the improvements are both comprehensible for trust, and practical for real-world use.

Acknowledgements

The original version of this paper was prepared with support from ACCURATE: A Center for Correct, Usable, Reliable, Auditable and Transparent Elections, under National Science Foundation Grant Number 0524111.

Created: Dec 21 2009
Last updated: Sep 15 2016

References

1) Vander Veen, C. "Honolulu Cuts Costs with First All-Digital Election in the US," *Government Technology*, October 29, 2009. http://www.govtech.com/e-government/Honolulu-Cuts-Costs-With-First-All-Digital.html.

2) Dunbar, J. "Internet Voting Project Cost Pentagon $73,809 per Vote," The Center for Public Integrity, Washington, DC, August 9, 2001, http://projects.publicintegrity.org/telecom/report.aspx?aid=297.

3) Austein, M. "Voters in Estonia Cast Ballots Online," IIP Digital, Washington, DC, July 3, 2008, http://iipdigital.usembassy.gov/st/english/article/2008/07/20080703124442mnietsua4.710025e-02.html#axzz4KjBwP52E.