Statements about Internet Voting from Experts

Computer Experts Commissioned by the U.S. Department of Defense

In their 2004 report, a panel of experts commissioned by the Department of Defense to evaluate the DoD's Internet voting project addressed a commonly asked question in the section entitled "Why security for Internet voting is far more difficult than for e-Commerce." They said:[1]

> Many people mistakenly assume that since they can safely conduct commercial transactions over the Internet, that they also can safely vote over the Internet. First, they usually underestimate the hazards of online financial transactions, and are unaware of many of the risks they take even if they are careful to deal only with "secure" web sites through the SSL protocol. But they also assume that voting is comparable somehow to an online financial transaction, whereas in fact security for Internet voting is far more difficult than security for e-commerce. There are three reasons for this: the high stakes, the inability to recover from failures, and important structural differences between the requirements for elections and e-commerce.
>
> First, high security is essential to elections. Democracy relies on broad confidence in the integrity of our elections, so the stakes are enormous. We simply cannot afford to get this wrong. Consequently, voting requires a higher level of security than e-commerce. Though we know how to build electronic commerce systems with acceptable security, e-commerce grade security is not good enough for public elections.
>
> Second, securing Internet voting is structurally different from—and fundamentally more challenging than—securing e-commerce. For instance, it is not a security failure if your spouse uses your credit card with your consent; it is routine to delegate the authority to make financial transactions. But it is a security failure if your spouse can vote on your behalf, even with your consent; the right to vote is not transferable, and must not be delegated, sold, traded or given away. Another distinction between voting and ecommerce is that while a denial of service attack on e-commerce transactions may mean that business is lost or postponed, it does not de-legitimize the other transactions that were unaffected. However, in an election, a denial of service attack can result in irreversible voter disenfranchisement and, depending on the severity of the attack, the legitimacy of the entire election might be compromised.
>
> Third, the special anonymity requirements of public elections make it hard to detect, let alone recover from, security failures of an Internet voting system, while in e-commerce detection and recovery is much easier because e-commerce is not anonymous. In a commercial setting, people can detect most errors and fraud by cross-checking bills, statements, and receipts; and when a problem is detected, it is possible to recover (at least partially) through refunds, insurance, tax deductions, or legal action. In contrast, voting systems must not provide receipts, because they would violate anonymity and would enable vote buying and vote coercion or intimidation. Yet, even though a voting system cannot issue receipts indicating how people voted, it is still vital for the system to be transparent enough that each voter has confidence that his or her individual vote is properly captured and counted, and more generally, that everyone else's is also.

[1] "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)." January 20, 2004. By Dr. David Jefferson, Dr. Aviel D. Rubin, Dr. Barbara Simons, Dr. David Wagner. Pages 6,7. http://www.servesecurityreport.org/

> There are no such requirements for e-commerce systems. In general, designing an Internet voting system that can detect and correct any kind of vote fraud, without issuing voters receipts for how they voted, and without risking vote privacy by associating voters with their votes, is a deep and complex security problem that has no analog in the e-commerce world. For these reasons, the existence of technology to provide adequate security for Internet commerce does not imply that Internet voting can be made safe.

National Institute of Standards and Technology (NIST)

In 2008, the National Institute of Standards and Technology (NIST) wrote an analysis of thte threats to different types of voting systems currently provided for, and under consideration for, UOCAVA voters. Regarding the threats to returning ballots by email, NIST said:[2]

> In most instances, voted ballots returned via e-mail would reach election officials nearly instantaneously. Communications could, however, be disrupted by malicious parties. Denial of service attacks are a significant threat to e-mail-based voting systems. Attackers could flood election e-mail servers with large amounts of illegitimate traffic. This could not only prevent voters' e-mails from reaching election officials, but could also make it difficult for officials to distinguish between valid and invalid ballots.
>
> Eavesdropping is a potential threat whenever Internet communications is involved, and particularly with e-mailed communications, which are sent unencrypted. While eavesdropping is not a significant threat for ballot distribution, as that information is generally publically available, voted ballots must remain confidential. Voted ballots show how an individual voted, and may sometimes contain sensitive personal information about the voter. E-mails are significantly easier to intercept and modify in transit than other forms of communication. E-mails travel through telecommunications lines, network equipment and e-mail servers before reaching the intended recipient. Anyone with access to the infrastructure could read or even modify e-mail messages. In particular, e-mail servers often store messages for a short period of time before passing them on to the next server, or the intended recipient. System operators for these servers could intercept or modify e-mailed ballots. It is unlikely that election officials would be able to identify ballots that had been modified in-transit.
>
> Also, e-mailed ballots are at risk before and after they are sent to election officials. Voters' computers could be infected with malicious code capable of disrupting communications with an election official. Very sophisticated attacks may be able to modify digital ballots prior to e-mailing them to election officials. Malicious code would need to spread to a large number of personal computers before it would have a substantial effect on an election. The computer virus may be detected before election day, but there would be no way for election officials to identify affected ballots. Similar malicious code on election computer systems could have the same effect.
>
> E-mail does not provide any guarantee that the intended recipient will receive the message. The e-mail system relies on the DNS system to route e-mails to the proper servers. An attack on DNS servers could route e-mails to an attacking party. This would not only result in voter disenfranchisement, but also the loss of sensitive voter information. This kind of attack would require very sophisticated attackers focusing their efforts on major e-mail service

[2] "A Threat Analysis on UOCAVA Voting Systems." [NISTIR 7551], pages 42, 43 (pdf pages 48,49) http://vote.nist.gov/uocava-threatanalysis-final.pdf

> providers. There are no known reports of a similar attack being successfully conducted on e-mail or DNS servers. However, it is important to note that a recent vulnerability was discovered in DNS servers that could have been used to construct a similar attack. DNS servers were quickly patched before any significant attack took place.
>
> Less sophisticated, but equally effective, attacks may attempt to trick voters into sending their ballots to an attacker. That is, an attacker would contact a large number of voters, claiming to be their local election official and attempting to convince them to reply with their cast ballot. While a relatively small number of voters may be fooled, it is relatively easy and cheap to contact a very large numbers of voters.

Regarding the threats to returning ballots by a Web-based Internet system, NIST said:[3]

> Web-based Internet voting is a form of electronic voting. The election web server would need to be trusted to accurately record voters' selections. Defects in the voting system software, or malicious code installed on the voting system by hostile individuals, could cause votes to be recorded improperly, or could modify votes at a later time. Skilled hackers may find vulnerability in the voting system software that would grant them access to voter and ballot information. This could also lead to a loss of voter secrecy, or a loss of election integrity. Sophisticated attacks would leave little or no evidence.
>
> Election officials, or other individuals with physical access to voting system equipment, may be able to gain access to election information, including cast ballots. Sophisticated attackers may also be able to delete any audit records that would leave evidence of their attack.
>
> Denial of service attacks are significant threats to Internet-based voting systems. A successful denial of service attack would overwhelm the election web server with traffic, preventing legitimate voters from casting a ballot. It is very difficult to protect against denial of service attacks from an attacker with a large amount of resources. A successful denial of service attack generally requires access to a large number of computers with high-speed Internet connections. While an attacking organization may purchase these systems, it typically would use a Botnet. A Botnet is a collection of personal computers that have been infected with a virus that gives an attacker control of the computer. Control of Botnet-infected computers is sold on the black market, given nearly anyone with financial resources the technical resources to perform a denial of service attack.
>
> Many of the potential threats to a web-based Internet voting system involve attacks on equipment that are not under election officials' control. Attacks on the DNS system could lead voters to fraudulent web sites. These voters may unknowingly provide their voter credentials to a malicious party, who in turn could impersonate the voter on the legitimate election server. Malicious code installed on voters' personal computers could disrupt communications with an election web server, or even modify voters' ballot choices without their knowledge. A computer virus would have to spread to a large number of computers before it could have a substantial effect on an election. Antivirus vendors may be able to identify and offer protections against such viruses, but not until after some voters' computers have been compromised. Furthermore, election officials would have no guarantee that their constituents would use updated anti-virus software. Election officials would have little recourse but to assume that all received votes are valid, as there would be no way to identify ballots from compromised machines.

[3] NISTIR 7551, page 45 (pdf page 51) http://vote.nist.gov/uocava-threatanalysis-final.pdf

> Less sophisticated attackers may be able to trick voters into navigating to a fraudulent web site that would mimic the actual election site. This type of attack, known as phishing, involves sending a large number of messages to potential voters claiming to be from election officials. The message could instruct voters to log into the fraudulent web site to cast a ballot. While most voters would discard such messages, a small percentage of voters could fall victim to this attack, which is common in the banking industry.

NIST summarized its conclusions thus:[4]

> ***Use of E-mail for Return of Voted Ballots:***
> The use of e-mail to return ballots presents several significant security challenges. Several different computer systems are involved in sending an e-mail from a voter to an election official. Many of these systems, such as the voters' computers and e-mail servers, are outside the control of election officials. Attacks on these systems could violate the privacy of voters, modify ballots, or disrupt communication with election officials. Because other individuals or organizations operate these systems, there is little election officials can do to prevent attacks on these systems. The security challenges associated with e-mail return of voted ballots are difficult to overcome using technology widely deployed today.
>
> ***Use of Web for Return of Voted Ballots:***
> Casting ballots via the web poses a large number of security challenges that are difficult to overcome. Using this transmission method, voters would log into a web site and submit their selections on a web page. A great deal of trust must be placed in the software on the election server to accurately record votes, as there would be no opportunity for voters to directly verify that their ballots have been recorded correctly.
>
> Furthermore, like e-mail voting systems, a web-based system for casting ballots would rely on computer systems outside the control of election officials. Attacks on these systems, such as voters' computers, could significantly threaten the integrity of elections or the ability of voters to cast ballots. Less sophisticated attacks, such as phishing and spoofing, could trick voters into giving up their voting credentials to an attacker. Such attacks are common in the banking industry, and difficult to defend against. There have been and continue to be significant problems in this industry. Technology that is widely deployed today is not able to mitigate many of the threats to casting ballots via the web.

[4] NISTIR 7551, page 69 (pdf page 75) http://vote.nist.gov/uocava-threatanalysis-final.pdf

Computer Technologists' Statement on Internet Voting[5]

Election results must be *verifiably accurate* -- that is, auditable with a permanent, voter-verified record that is independent of hardware or software. Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the internet are to be verifiable. There are also many less technical questions about internet voting, including whether voters have equal access to internet technology and whether ballot secrecy can be adequately preserved.

Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting.

A partial list of technical challenges includes:

- **The voting system as a whole must be verifiably accurate in spite of the fact that client systems can never be guaranteed** to be free of malicious logic. Malicious software, firmware, or hardware could change, fabricate, or delete votes, deceive the user in myriad ways including modifying the ballot presentation, leak information about votes to enable voter coercion, prevent or discourage voting, or perform online electioneering. Existing methods to "lock-down" systems have often been flawed; even if perfect, there is no guaranteed method for preventing or detecting attacks by insiders such as the designers of the system.
- **There must be a satisfactory way to prevent large-scale or selective disruption** of vote transmission over the internet. Threats include "denial of service" attacks from networks of compromised computers (called "botnets"), causing messages to be mis-routed, and many other kinds of attacks, some of which are still being discovered. Such attacks could disrupt an entire election or selectively disenfranchise a segment of the voting population.
- **There must be strong mechanisms to prevent undetected changes to votes,** not only by outsiders but also by insiders such as equipment manufacturers, technicians, system administrators, and election officials who have legitimate access to election software and/or data.
- **There must be reliable, unforgeable, unchangeable voter-verified records** of votes that are at least as effective for auditing as paper ballots, without compromising ballot secrecy. Achieving such auditability with a secret ballot transmitted over the internet but without paper is an unsolved problem.
- **The entire system must be reliable and verifiable** even though internet-based attacks can be mounted by anyone, anywhere in the world. Potential attackers could include individual hackers, political parties, international criminal organizations, hostile foreign governments, or even terrorists. The current internet architecture makes such attacks difficult or impossible to trace back to their sources.

Given this list of problems, there is ample reason to be skeptical of internet voting proposals. Therefore, the principles of operation of any internet voting scheme should be publicly disclosed in sufficient detail so that anyone with the necessary qualifications and skills can verify that election results from that system can reasonably be trusted. Before these conditions are met, "pilot studies" of internet voting in government elections should be avoided, because

[5] "Computer Technologists' statement on internet voting." September 11th, 2008. http://www.verifiedvoting.org/article.php?id=5867

the apparent "success" of such a study absolutely cannot show the absence of problems that, by their nature, may go undetected. Furthermore, potential attackers may choose only to attack full-scale elections, not pilot projects.

The internet has the potential to transform democracy in many ways, but permitting it to be used for public elections without assurance that the results are verifiably accurate is an extraordinary and unnecessary risk to democracy.

-END---

Endorsements

The computer technology experts below endorse this statement. Affiliations are for identification only, and do not imply that employers have a position on the statement.

Alex Aiken
Professor of Computer Science, Stanford University
http://cs.stanford.edu/~aiken

Andrew W. Appel
Professor of Computer Science, Princeton University
http://www.cs.princeton.edu/~appel/

Ben Bederson
Associate Professor, Computer Science Department, University of Maryland
http://www.cs.umd.edu/~bederson

L. Jean Camp
Associate Professor, School of Informatics, Indiana University
http://www.ljean.com/

David L. Dill
Professor of Computer Science, Stanford University and Founder of VerifiedVoting.org
http://verify.stanford.edu/dill

Jeremy Epstein
Software AG and Co-Founder, Verifiable Voting Coalition of Virginia
http://www.visualcv.com/jepstein

David J. Farber
Distinguished Career Professor of Computer Science and Public Policy Carnegie Mellon University
http://www.epp.cmu.edu/httpdocs/people/bios/farber.html

Edward W. Felten
Professor of Computer Science and Public Affairs, Princeton University
http://www.cs.princeton.edu/~felten

Michael J. Fischer
Professor of Computer Science, Yale University, and President, TrueVoteCT.org
http://www.cs.yale.edu/people/fischer.html

Joseph Lorenzo Hall
UC Berkeley School of Information
http://josephhall.org/

Harry Hochheiser
Assistant Professor, Computer and Information Sciences, Towson University
http://triton.towson.edu/~hhochhei

Jim Horning
Chief Scientist, SPARTA, Inc., Information Systems Security Operation
http://www.horning.net/pro-home.html

David Jefferson
Lawrence Livermore National Laboratory
http://people.llnl.gov/jefferson6

Bo Lipari
Retired Software Engineer, Executive Director New Yorkers for Verified Voting
http://www.nyvv.org/bolipari.shtml

Douglas W. Jones
Professor of Computer Science, University of Iowa
http://www.cs.uiowa.edu/~jones/vita.html

Robert Kibrick
Director of Scientific Computing, University of California Observatories / Lick Observatory
http://www.ucolick.org/~kibrick

Scott Klemmer
Assistant Professor of Computer Science, Stanford University
http://hci.stanford.edu/srk/bio.html

Vincent J. Lipsio
http://www.lipsio.com/~vince/resume.pdf

Peter Neumann
Principal Scientist, SRI International
http://www.csl.sri.com/users/neumann

Eric S. Roberts
Professor of Computer Science, Stanford University
http://cs.stanford.edu/~eroberts/bio.html

Avi Rubin
Professor, Computer Science, Johns Hopkins University
http://avi-rubin.blogspot.com/

Bruce Schneier
Chief Security Technology Officer, BT Global Services
http://www.schneier.com/

Yoav Shoham
Professor of Computer Science, Stanford University
http://cs.stanford.edu/~shoham

Barbara Simons
IBM Research (retired)
http://www.verifiedvoting.org/article.php?id=2074

Eugene H. Spafford
Professor and Executive Director of CERIAS, Purdue University
http://spaf.cerias.purdue.edu/narrate.html

Michael Walfish
Assistant Professor of Computer Science, University of Texas, Austin
http://nms.csail.mit.edu/~mwalfish

Dan S. Wallach
Associate Professor, Department of Computer Science, Rice University
http://www.cs.rice.edu/~dwallach/

Luther Weeks
Retired Software Engineer and Computer Scientist
http://www.ctvoterscount.org/?page_id=2

Jennifer Widom
Professor of Computer Science, Stanford University
http://infolab.stanford.edu/~widom/

David S. Wise
Computer Science Dept., Indiana University
http://www.cs.indiana.edu/~dswise/