Testimony against SB1515

Senate Committee on Rules

Tuesday, February 18, 2014 8:30 AM

Members:

Sen. Diane Rosenbaum, Chair
Sen. Ted Ferrioli, Vice Chair
Sen. Bruce Starr
Sen Lee Beyer
Sen. Ginny Burdick

I urge a NO vote on Senate Bill 1515.

As a former software engineering professional with approximately 30 years of active experience in development and quality assurance, I strongly urge a NO vote on Senate bill 1515. Internet/online voting may sound great, and non-professionals may believe security is good enough for elections, but I can assure you – we are not there yet, and may never be to a level of security that we need for secure, repeatable, auditable election results.

I will use the words of experts below in explaining the reasoning for my statement above, but would also like to add that it is our due diligence to certify security and accuracy of election computers. The counting machines we use now are in some cases 20 years old, because the federal certification of simple counting equipment may take up to 10 years. We will NEVER be able to certify the security of home computers, laptops, tablets, and smart phones of millions of voters, as well as library and other public access sites.

The following statements have been prepared by experts in the field of computer internet security. I would also refer you to the binder full of detailed articles and papers handed out today.

Respectfully,
Sandy Raddue
Beaverton, OR
sraddue@electionoregon.com
www.electionoregon.com

"Within 36 hours of the system going live, our team had found and exploited a vulnerability that gave us almost total control of the server software, including the ability to change votes and reveal voters' secret ballot."
Attacking the Washington, D.C. Internet Voting

"Because of the difficulty of validating and verifying software on remote electronic voting system servers and personal computers, ensuring remote electronic voting systems are auditable largely remains a challenging problem, with no current or proposed technologies offering a viable solution."
Security Considerations for Remote Electronic UOCAVA Voting, NIST, February 2011

"The return of voted ballots poses threats that are more serious and challenging than the threats to delivery of blank ballots and registration and ballot request. In particular, election officials must be able to ascertain that an electronically-returned voted ballot has come from a registered voter and that it has not been changed in transit. Because of this and other security-related issues, the threats to the return of voted ballots by e-mail and web are difficult to overcome."
A Threat Analysis on UOCAVA Voting Systems, NIST December 2008

"Most of the security problems with Internet voting are generic to any PC and Internet application, and fundamentally have no effective solutions. This is why the majority of all email transmitted over the Internet is spam, and an estimated 50% of all Internet-connected PCs in the world are infected with malicious software, despite more than a decade of effort and immense investment by the world's high technology companies in trying to fix these problems. It is not just that no solution to the problems of Internet voting has yet been deployed. The real problem is that no fundamental solution is possible using the current Internet protocols and the current PC hardware and software platforms."
Comment on the May 2007 DoD report on Voting Technologies for UOCAVA Citizens, Aviel Rubin, David Jefferson, Barbara Simons, 2007

"The transmission of voting materials by unsecured email is a concern from both a privacy and security concern. Email traffic … is easily monitored, blocked and subject to tampering. In addition, the publication of e-mail addresses of voting officials subject those offices to attack, effectively blocking voters."
Independent review final report for the Interim Voting Assistance System (IVAS), Aug. 2006

"Because the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear."
SERVE voting system security report, 2004

"Remote Internet voting systems pose signicant risk to the integrity of the voting process, and should not be elded for use in public elections until substantial technical and social science issues are addressed. The security risks associated with these systems are both numerous and pervasive, and, in many cases, cannot be resolved using even today's most sophisticated technology."
National Science Foundation Internet Voting Report, 2001

"[The] broad application of Internet voting in general faces several formidable social and technological challenges. …They include providing adequate ballot secrecy and voter privacy safeguards to protect votes from unauthorized disclosure and to protect voters from coercion; providing adequate security measures to ensure that the voting system (including related data and resources) is adequately safeguarded against intentional intrusions and inadvertent errors that could disrupt system performance or compromise votes; providing equal access to all voters, including persons with disabilities, and making the technology easy to use; and ensuring that the technology is a cost-beneficial alternative to existing voting methods, in light of the high technology costs and security requirements, as well as the associated benefits to be derived from such investments."
Elections: Perspectives on Activities and Challenges Across the Nation, GAO, October 2001

"Our concerns about early and remote voting plans are even stronger as we contemplate the possibility of Internet voting. In addition to the more general objections, the Commission has heard persuasive testimony that Internet voting brings a fresh set of technical and security dangers all its own. This is an

idea whose time most certainly has not yet come."
National Commission on Federal Election Reform, Aug. 2001

"Remote Internet voting poses serious security risks. It is much too easy for one individual to disrupt an entire election and commit large-scale fraud."
Voting: What is, what could be,
Caltech-MIT Voting Technology Project, 2001

"[T]echnological threats to the security, integrity and secrecy of Internet ballots are significant. The possibility of "Virus" and "Trojan Horse" software attacks on home and office computers used for voting is very real and, although they are preventable, could result in a number of problems ranging from a denial of service to the submission of electronically altered ballots."
California Secretary of State's Task Force on Internet Voting (2000)

Computer Technologists' Statement on Internet Voting

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, leaking information about votes to enable voter coercion, preventing or discouraging voting, or performing online electioneering. Existing methods to "lock-down" systems have often been flawed; and even without that problem, 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 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.

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

Don Gotterbarn
Director, Software Engineering Ethics Research Institute, Computer and Information Sciences,
East Tennessee State University
http://csciwww.etsu.edu/gotterbarn

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/

John Sebes
Co-Director, Open Source Digital Voting Foundation
Chief Technology Officer, TrustTheVote Project
http://www.osdv.org/who

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/

Questions and Answers on the "Computer Technologists' Statement on Internet Voting"

Q: Who is behind this statement?
A: The primary author is David Dill, Professor of Computer Science at Stanford, with extensive input and editing from a number of others. This is also the position of VerifiedVoting.org on internet voting, and VerifiedVoting.org will help to publicize it.

Q: Why this statement at this time?
A: Serious proposals to use internet voting keep coming up. There have been several internet primaries in the last few years, including a primary conducted by Democrats Abroad in 2008. Furthermore, internet voting schemes are being promoted for the general election in 2008, including a proposal by Okaloosa County, Florida, and the State of Alabama.

In many cases, these schemes have been deployed without due consideration of the technical challenges,based on unsupported assertions by vendors that the systems are "secure". Independent experts need to speak out.

Q: Is this an anti-internet voting statement?
A: No. Some of the people who have endorsed it are working on internet voting methods. The statement is intended to be a warning: internet voting is not as easy to do safely as some people seem to think. Before we move to it, we need an informed public debate so the people know what they're getting into.

Q: What explains the enthusiasm for internet voting?
A: Currently, most of the momentum seems to be coming from the difficulties that Americans overseas, especially in the military, have voting. The mails are inefficient, so absentee ballots take a long time to reach the voter and a long time to return.

We understand this problem, but it seems clear that the situation can be made a lot better for overseas voterswithout internet voting. First, a system could be set up where any voter can print a ballot obtained over the internet (or obtain a remotely printed ballot at a military facility or embassy), which would eliminate half the mail problems, and difficulties with local elections offices that mail ballots late. Second, marked ballots could be returned by express mail or (better) by military transport or in diplomatic pouches, after being appropriately signed and sealed. This year, Federal Express is offering discounts to overseas voters for returning ballots. Finally, laws in some states could be modified to make the time constraints on ballot arrival less stringent, to reduce the risk that ballots will not be counted. In voting, there has been a tendency to look for technical solutions to problems that are mostly non-technical. We believe that is happening again with internet voting.

Alternatively, someone could come up with an internet voting scheme that is at least as safe as current overseas ballots, and convince the rest of us that it actually is secure and doesn't have other harmful effects.

We do not feel that it is appropriate to "enfranchise" voters by providing them with a system that may allow their votes to be lost or stolen undetectably.

Q: The statement asks that the "principles of operation" of the system need to be disclosed. What does that mean? Does it require open source?
A: We're going by analogy with low-tech voting systems. For example, to understand why a fully

manual paper ballot voting system can be trusted, people have to know how the ballots are handled, how polling places are run, etc. For example, if there are multiple poll workers present in each polling place at all times, it's harder for someone to "stuff" the ballot box. If hand counts are conducted in public view, it's less likely that the counts are erroneous.

We don't need to know everything about a system to know whether it is trustworthy. For example, most people would not feel that they need to know how computerized typesetting works before they marked a paper ballot. In fact, if you have to know a lot of complex details to understand whether a system can be trusted, that system probably can't be trusted.

The statement asks that the things we need to know to trust a proposed internet voting scheme be revealed. This is a problem because many schemes are being proposed where the details of operation are secret.

Some of us think "open source", or, more precisely, public disclosure of source code is a good idea. However, source code disclosure is neither necessary nor sufficient for trustworthy voting. Even when source code has been carefully inspected, it is very easy to overlook program bugs or malicious behavior in the system. It is also very difficult to make sure that the program running on a particular voting system matches the source code that was reviewed (vs. "acting the same" for certain test cases). Finally, errors and malicious changes can exist in parts of the system that are not in the source code, including low-level firmware and the hardware itself.

In a nutshell, if the security of a system depends on source code review, the system is not secure.

Q: Are you implying vendors or election officials are dishonest?
A: No, not any more than wanting bank statements implies that my bank is dishonest. Almost all trust in modern society is based on checks and balances (e.g., auditing requirements). Without the accountability that follows from checks and balances, systems become inaccurate and often dishonest. Classical election procedures are based on checks and balances, with the knowledge that elections are important and that unscrupulous people may seek to commit fraud. The same principles need to be maintained in new election systems.

Q: As someone without a strong technical background, why should I have to rely on a bunch of computer scientists to tell me whether I can trust my elections?
A: Maybe you shouldn't (however, the statement at least insists that there should be enough disclosure so that a technical person you trust can review the scheme and tell you what he or she thinks about it). If you have non-technical concerns about internet voting, this would be a good time to speak up. As the statement notes, we are NOT saying that the decision whether to use internet voting is a purely technical decision – just that it needs to be a technically INFORMED decision. The technical challenges of internet voting are currently being minimized, often by people who simply don't understand them.

We're calling for an in-depth, public debate on the technical and NON-TECHNICAL issues in internet voting before adopting it. It's very possible that a technically sound internet voting scheme could be rejected for non-technical reasons, including other issues such as whether internet voting might disenfranchise legal voters who cannot easily access the internet.

Q: Isn't this statement at odds with the position of some of the people involved that only "voter verified paper ballots" should be used in elections?

A: The statement is a floor, not a ceiling. Endorsing it is definitely NOT an endorsement of internet voting or voting that uses electronic ballots. It says that internet voting should NOT be deployed unless certain minimum conditions -- with which we believe most technologists would agree -- are met. It does not imply the internet voting or electronic ballots can be used safely, or ever should be used.

Q: Why doesn't the statement demand (my favorite requirement)?
A: The statement is focused on the technical problems of internet voting, and sets out minimal conditions that represent a consensus of those endorsing it. The decision about whether or not internet voting should be used depends on many issues, including whether it has (your favorite requirement).

The main goal of the statement is to prevent deployment of internet voting without due consideration of the risks. It also calls for the ability of the general public to participate in the decision of whether or not to use internet voting -- including you, should you choose to argue for (your favorite requirement).

Internet Voting

Proposals to conduct voting pilots using real elections continue to reappear both in the U.S. and elsewhere, seemingly independent of warnings from computer security experts. While the appeal of Internet voting is obvious, the risks, unfortunately, are not, at least to many decision makers. While very few votes have ever been cast in American elections directly through a web interface, many states already allow military and overseas ballots to be returned via fax and email. Yet voted ballots sent via Internet simply cannot be made secure and make easy and inviting targets for attackers ranging from lone hackers to foreign governments seeking to undermine US elections.

Further Reading

ACM: Internet Voting in the United States

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

What About Email and Fax?

Report on Internet Voting in Estonia

ACM Brief: Internet Voting and Uniformed and Overseas Citizens absentee Voters (pdf)

Despite that, as states provide electronic delivery of blank ballots, some are using the Internet for return of voted ballots via email attachments. Vendors of online election software, with a vested interest in selling their products, of course downplay the inherent risks and promise the oxymoronic "Internet security". But experts in computer security maintain that nothing sent over the Internet is secure. Voter's personal computers, from which emails are sent, are easily and constantly attacked by viruses, worms, Trojan Horses and spyware.

Once a voted ballot is emailed, it moves between many different servers located all over the planet, and is subject to compromise by anyone with access to any of those machines. And the election official on the receiving end has no way to know if the voted ballot she received matches the one the voter originally sent, no matter how well secured their county computer services may be, and no matter how much has been spent licensing software and upgrading their systems.

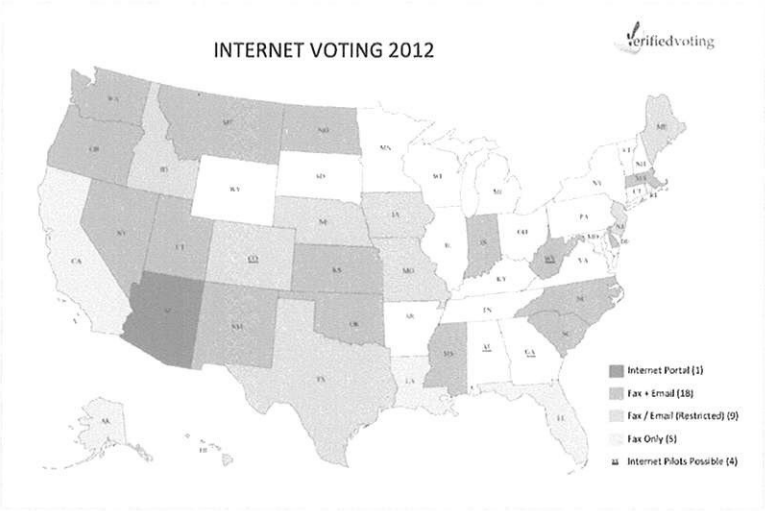
There is no way to guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future. Anyone from a disaffected misfit individual to a national intelligence agency can remotely attack an online election, modifying or filtering ballots in ways that are undetectable and uncorrectable, or just disrupting the election and creating havoc. There are a host of such attacks that can be used singly or in combination. In the cyber security world today almost all of the advantages are with attackers, and any of these attacks can result in the wrong persons being elected, or initiatives wrongly passed or rejected. Continue Reading

Computer Technologists Statement on Internet Voting

In 2008, Verified Voting founder David Dill organized the Computer Technologists' Statement on Internet Voting. The Technologist's Statement warns against "pilot" Internet voting projects and describes the severe challenges that must be met if an Internet voting system is to justify public confidence.

Read The Computer Technologists' Statement on Internet Voting

Current Status of Internet Voting in the United States



Both e-mailing voted ballots and transmitting them through a Web portal are forms of "Internet voting." And with the proliferation of Internet fax services, we can presume that many voted ballots returned to election officials via fax have in fact been transmitted through the Internet. Internet voting thus can mean voting from an Internet browser in one's personal computer, or by email attachment, or electronic fax, remote kiosk, or other means of remote electronic transmission. A voted ballot sent through the Internet is no more verifiable than a polling place ballot cast on a paperless direct-recording electronic voting machine – and in fact is exposed to a far greater number of security threats including cyber-attacks such as modification in transit, denial of service, spoofing, automated vote buying, and viral attacks on voter PCs.

In all, 32 states allow military and overseas voters to return ballots electronically. Yet 22 of these states require that voting systems at home use paper ballots or provide voter-verifiable paper records. We cannot overstate this fact: the technological reasons that 35 States have moved toward paper ballots or voter-verifiable paper records for all voters at home and 10 more provide them for voters in at least some counties also apply, with even greater urgency, to voted ballots returned to State and local election officials electronically from outside the country. Of the 32 States that allow electronic return of voted ballots, only New Jersey requires military and overseas voters to return a paper ballot in addition to sending their ballots to election officials in electronic form. This option provides verifiability, if the ballot of record for audits and recounts. Currently no State allows the transmission of voted ballots for stateside voters. You can view the specific provisions for the electronic submission of voted ballots in each of the States at the right of this page.

The Military and Overseas Voter Empowerment (MOVE) Act of 2009

There's no question that voting for military and overseas voters needs to be improved. Too often absentee ballots are not received in time, if at all. Returning voted ballots from voters in hard to

reach places (for example remote military outposts) in time to meet state election deadlines is difficult. These are real problems and 2009 saw efforts to improve ballot access for overseas voters kick-started by passage of the Military and Overseas Voter Empowerment (MOVE) Act, passed as an amendment to the Defense Authorization bill. The MOVE Act addressed many problems facing overseas voters. It required that election officials provide ballots to military and overseas voters 45 days in advance of the election. Election officials must also make applications and blank ballots available electronically. Except for the issues raised by the remaking of ballots in some States, this is an excellent provision that allows technology to expedite the voting process but does not endanger the verifiability of the election. In addition, the MOVE Act established a system through which absent military voters are able to return their voted ballots by expedited mail through the U.S. Postal Service for free. But while the MOVE Act calls for electronic distribution of election materials, it is notably silent on the subject of return of voted ballots, with good reason.

Following enactment of MOVE, as states sought ways to meet new requirements for electronic delivery of ballots to voters deployed or living overseas, some states reached beyond the requirements of the Act. These states started providing electronic channels for return of voted ballots from voters: fax, email and Internet portals for uploading of voted ballots, and in some cases "online mark and send." The States are under *no* Federal requirement to permit electronic return of voted ballots, but many do so despite the major security risks. In addition, opportunity for error arises through the "remaking" of returned ballots, whether printed or electronic, onto optical scan ballots by election officials in order to insert the copies into the tabulating scanner. Ballots may be remade if the voter returns a printed and marked copy of an electronically received blank ballot, or if a completed ballot is returned electronically to election officials. In both cases the paper version of the "ballot" election officials receives or prints out currently cannot be scanned. There is little information about how widespread the practice of remaking electronically transmitted UOCAVA ballots is, and it may depend on how many UOCAVA voters vote in a given jurisdiction. For more information and citations see Counting Votes 2012 (PDF)

David Jefferson on Internet Voting:

Barbara Simons: Why can't we vote online?:

Internet Voting Reports

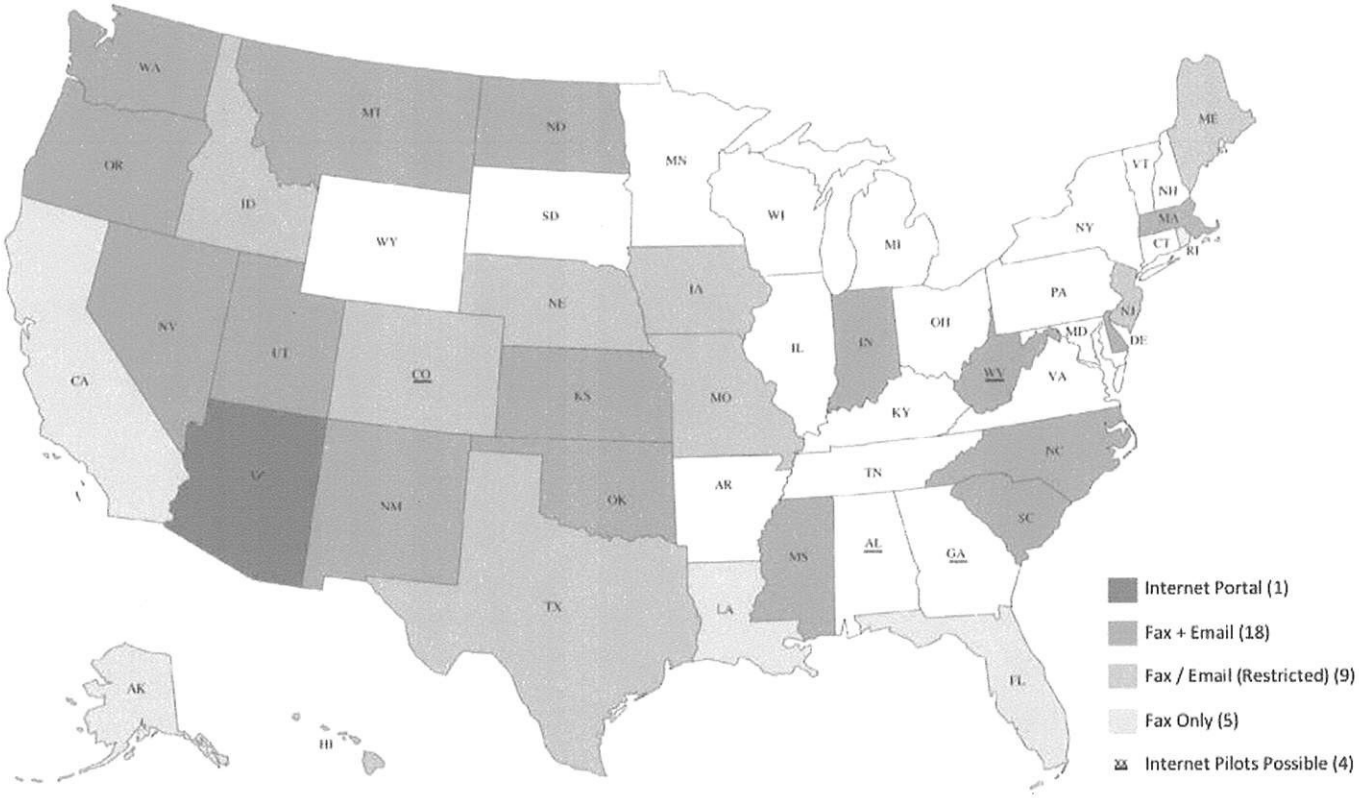
"Within 36 hours of the system going live, our team had found and exploited a vulnerability that gave us almost total control of the server software, including the ability to change votes and reveal voters' secret ballot." Attacking the Washington, D.C. Internet Voting

Technology Review on Internet Voting

Presented to
Oregon Legislature
Senate Committee on Rules
Feb. 18, 2014
by
Sandy Raddue
www.ElectionOregon.com

INTERNET VOTING 2012

verifiedvoting



Moore: Online balloting: good intent, bad law

Justin Moore | Posted: Friday, February 7, 2014 12:00 am

This week the General Assembly has been considering an important election-reform bill that could greatly affect the security of the ballots of our troops and the integrity of elections in Virginia. HB 759 would allow military voters to send marked ballots back over the Internet via email. The bill is intended to address the very real challenges facing military voters, but allowing ballots to be returned over the Internet creates extraordinary risks both to the votes of our men and women in uniform and to the electoral infrastructure of our state.

The Internet provides great opportunities, but also tremendous risks. The skill and stealth of hackers continues to outpace our ability to secure Internet-based services. Target, Adobe, Sony, Google, Apple, Facebook, Citigroup and others have all been victims, as have the Department of Defense and the State of South Carolina. Government security experts are raising increasingly urgent warnings regarding computer attacks. The rise of organized, well-funded, state-sponsored hackers has made the cyber world less secure now than ever before. Gen. Keith Alexander, head of the National Security Agency and the Department of Defense's U.S. Cyber Command, stated that between 2009 between 2011 there was a 1,700 percent increase in computer attacks against American infrastructure initiated by criminal gangs, hackers and other nations.

At the direction of Congress, scientists at the federal National Institute of Standards and Technology (NIST) have been conducting research into the use of online systems for military voters. NIST has stated that with the security tools currently available, secure online ballot return is not feasible and that more research is needed.

For these reasons the Department of Defense (DOD) itself does not recommend states adopt Internet voting and instead recommends ballots be returned by postal mail. The DOD has also unequivocally prohibited state and local jurisdictions from using DOD grant money to transmit voted ballots over the Internet. In 2012 Virginia was awarded $1.8 million from the DOD to assist military voters, but these funds may not be used for any system or program that enables the electronic return of voted ballots because the security issues remain unresolved.

So why is the General Assembly moving ahead to adopt electronic ballot return for the military against the recommendation of both NIST and the Department of Defense? This bill is largely being driven by the fact that many other states allow some form of electronic ballot return for military voters, and the mistaken conclusion that this means it is safe. However, none of these states have any meaningful or effective audits by third parties in place to detect if fraud has occurred. Even with effective procedures in place, it is estimated that most computer attacks are not discovered for 14

months or more, and skilled attackers won't leave any trace of their intrusion.

Proponents of transmitting voted ballots online often make the comparison that if we can bank and shop online, we can send ballots over the Internet. But online banking is far from secure; according to the "JP Morgan 13th Annual Online Fraud Report," $3.4 billion was lost to online fraud, and merchants reported losing an average of 1 percent of online revenue to fraud. Commercial entities can detect fraud by using detailed knowledge of a user's behavior, and factor losses as a cost of doing business; election divisions can do neither.

Votes are anonymous, and elections can be decided by a tiny fraction of a percent, as was demonstrated recently in Virginia's attorney general contest.

HB 759 contains a great idea: a provision for the General Assembly to establish a Working Group to study the proposal for casting ballots online. The Working Group, to include the chief information officer, the chief information security officer and local election officials, is directed to report back to the General Assembly in 2016 on the feasibility and cost of developing an online ballot return system.

This is a good idea but the bill puts the cart before the horse — this step should happen before implementation of online ballot return. HB 759 should be amended to require the Working Group to complete its study before deciding whether to approve adoption of any online voting program.

The Working Group should also be strengthened by inviting scientists from the National Institute of Standards and Technology and security experts from Virginia's public universities. Each political party should also have the authority to do its own security review with outside experts. The Working Group's final report should be available to the public without redactions.

We should always be looking for ways to make voting more accessible for our men and women in uniform, but we should not rush to implement online voting against the recommendations of the Department of Defense. Our troops' votes must be kept secure.

OREGONLIVE

Frustrations mount as Oregon secretary of state databases remain offline after website breach

kate.brown.feb.7.2013.JPG
Oregon Secretary of State Kate Brown warned businesses Thursday about a fraudulent invoice making the rounds. *(Michael Lloyd/The Oregonian)*

Yuxing Zheng | yzheng@oregonian.com By **Yuxing Zheng | yzheng@oregonian.com**
Email the author | Follow on Twitter
on February 13, 2014 at 7:00 AM, updated February 13, 2014 at 3:34 PM

SALEM -- Frustrations are mounting more than a week after a **breach of the Oregon secretary of state's website** caused elections and business databases to go offline. State officials say they're still investigating how the intrusion from a foreign entity occurred and don't know when the databases will return.

The attack "appears to be an orchestrated intrusion from a foreign entity and not the result of any employee activities," the agency reported on its website this week.

The department's Central Business Registry and ORESTAR, the state's online campaign finance reporting system, were temporarily taken offline as a precaution after officials detected "an intrusion" around Feb. 4. Since then, business attorneys haven't been able to look up existing business names, and campaign finance officials have not been able to report transactions.

The outage could lead to missed deadlines and increased costs for businesses as attorneys spend extra time filing documents, said **Shawn Lindsay**, a business attorney and a Republican former state representative.

"I've tried calling Thursday, Friday and Monday," Lindsay said. On Monday "I was on hold for 30 minutes, and I never got through."

The breach also raises questions about the security of the agency's other databases, including the voters database, which contains personal information that isn't publicly available, Lindsay said.

The voters database is on a separate server and was not affected by last week's breach, state officials say. **Credit card data is also safe.**

Two campaign finance officials said Wednesday that ORESTAR's outage has had minimal effect on their work, though they will need to file thousands of transactions once the website returns.

Kevin Neely, co-owner of **C&E Systems**, said he has between 5,000 to 7,000 transactions to upload to the database. Neely, who is the treasurer for about 400 Democratic political action committees, said he has had to submit paper forms to create four or six political action committees since the outage began.

"People are understandably frustrated," Neely said. "There's no good time for an outage, but frankly, if there were a good time in an election year, this is when it'd be because most of our legislative candidates aren't raising money right now."

House rules prohibit representatives from raising money during the session, and senators follow a similar informal rule.

Neely and Carol Russell, the Bandon-based treasurer of many Republican political action committees, said they weren't worried about any missed deadlines.

"If anybody's concerned about deadlines, we're going to fully take into consideration that our website made things either difficult or not possible," said Tony Green, spokesman for the Secretary of State.

About 25 agency workers are investigating the breach, and officials are in the process of hiring outside experts to review security measures, he said. "The forensic exam is an incredibly laborious, highly specialized process," Green said. "We've had people working as many hours in a day as possible."

The agency is receiving about 1,100 calls a day, nearly twice as many as usual, and wait times are longer than usual, he said. **Business forms can be filed via fax, mail or email**, he said.

Officials reported the breach to the Oregon State Police, and the FBI have also been informed.

-- Yuxing Zheng

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

by David Jefferson, Computer Scientist, Lawrence Livermore National Laboratory [1. Analyses and views stated herein are drawn from expertise as a computer scientist working on national security applications and are my own. They are not to be ascribed to my employer, Lawrence Livermore National Laboratory, which takes no position on these issues.]], member, Verified Voting Foundation Board, Board of Directors, California Voter Foundation

There is widespread pressure around the country today for the introduction of some form of Internet voting in public elections that would allow people to vote online, all electronically, from their own personal computers or mobile devices. Proponents argue that Internet voting would offer greater speed and convenience, particularly for overseas and military voters and, in fact, any voters allowed to vote that way. However, computer and network security experts are virtually unanimous in pointing out that online voting is an exceedingly dangerous threat to the integrity of U.S. elections. There is no way to guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future. Anyone from a disaffected misfit individual to a national intelligence agency can remotely attack an online election, modifying or filtering ballots in ways that are undetectable and uncorrectable, or just disrupting the election and creating havoc. There are a host of such attacks that can be used singly or in combination. In the cyber security world today almost all of the advantages are with attackers, and any of these attacks can result in the wrong persons being elected, or initiatives wrongly passed or rejected.

There is no way to guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future
Nonetheless, the proponents point to the fact that millions of people regularly bank and shop online every day without apparent problems. They note that an online voting transaction resembles an ecommerce transaction, at least superficially. You connect your browser to the appropriate site, authenticate yourself, make your choices with the mouse, click on a final confirmation button, and you are done! All of the potential attacks alluded to above apply equally to shopping and banking services, so what is the difference? People ask, quite naturally, "If it is safe to do my banking and shopping online, why can't I vote online?" This is a very fair question, and it deserves a careful, thorough answer because the reasons are not obvious. The answer requires substantial development to explain fully, but in brief, in can be summarized:

1. It is not actually "safe" to conduct ecommerce transactions online. It is in fact very risky, and more so every day. Essentially all those risks apply equally to online voting transactions.

2. The technical security, privacy, and transparency requirements for voting are structurally different from, and actually much more stringent than, those for ecommerce transactions. Even if ecommerce transactions were safe, the security technology underpinning them would not suffice for voting. In particular, the voting security and privacy requirements are unique and in tension in a way that has no analog in the ecommerce world.

E-Commerce transactions are not, in fact, "safe"

Why do security experts say that ecommerce transactions are not safe when millions of people do them every day, mostly without problems? The question needs to be refined: "Safe for whom?" and "What degree of safety is required"? E-Commerce transactions may be relatively safe for consumers, but they certainly are not safe for financial institutions or merchants.[2. See http://www.mcafee.com/us/resources/reports/rp-financial-fraud-int-banking.pdf, p. 4] Banks, credit card companies, and online merchants lose billions of dollars a year in online transaction fraud despite huge investments in fraud prevention and recovery. People have the illusion that ecommerce transactions are safe because merchants and banks don't hold consumers financially responsible for fraudulent transactions that they are the innocent victims of. Instead the businesses absorb and redistribute the losses silently, passing them on in the invisible forms of higher prices, fees, and interest rates. Businesses know that if consumers had to accept those losses personally most online commerce would collapse. Instead, they routinely hide the losses, keeping the magnitude secret so the public is generally unaware. It's a good business strategy.

There are many techniques for ecommerce fraud that are directly applicable to online voting. A common pattern starts with theft of credentials, e.g. names, account numbers, credit card numbers, passwords, or the answers to personal challenge questions. The theft can be initiated through phishing scams, drive-by malware installation, or other means, and such tricks can just as easily be used to steal online voting credentials as well. Recently a new botnet named Zeus has been in the news that installs malware on PCs.[3. See http://en.wikipedia.org/wiki/Zeus_(trojan_horse)] Zeus is specifically designed to wait until you connect to your bank and then it steals your bank password or PIN as you type them into your browser. The botmasters use those credentials to transfer money out of your accounts and to fake your online financial statements to hide the theft (for a while at least). It makes no difference that you have a "secure" connection to your banking site because the malware operates inside your computer and can see and modify everything you type in the clear, before it is encrypted for transmission down the "secure" connection. There are now illicit businesses that help other people set up Zeus botnets, or rent time on a botnet already created.[4. See http://threatpost.com/en_us/blogs/new-service-helps-attackers-get-zeus-botnet-ground-011011]

Most people, however, are completely unaware of these threats.

Zeus exemplifies what could just as easily happen if online voting becomes widespread. Eventually someone, perhaps a partisan political operative or a foreign intelligence agency, will deploy a similar botnet to infect thousands of voters' computers and modify their votes invisibly as they are being transmitted. Again, having a "secure" connection to the remote election server will make no difference. There is no effective way to prevent such an attack, and no effective recovery. Banks, online merchants, and high tech companies that do business online have huge security budgets to defend themselves against cyber attacks, and even so they are frequently victimized. If these organizations with such great expertise and capability in computer and network security can be successfully attacked, then no voting system vendor or local election administration has any realistic chance of successfully defending against similar threats.

We have to recognize that the cost to the attacker of conducting a remote online attack

has declined drastically over the last few years as various programming templates, libraries, and toolkits for malware production have become widely available. One recent study demonstrated that it was possible to duplicate even very sophisticated attack vectors like Stuxnet, the malware that did great damage to Iranian nuclear facilities, in about two months time for under $20,000. We are now in a very different threat environment than we were even a few years ago.[5. See http://hosted.ap.org/dynamic/stories/U/US_TEC_HACKING_CONTROL_SYSTEMS?SITE=AP&SECTION=HOME&TEMPLATE=DEFAULT&CTIME=2011-10-23-08-23-54]

What level of security is sufficient to protect elections? The scale of fraud that ecommerce and electoral systems can tolerate are very different. In the ecommerce world if one out of every thousand ecommerce transactions is lost or is fraudulent it is not really a vital concern. Banks, merchants and purchasers routinely deal with online revenue losses over 10 times higher than that,[6. See http://www.mcafee.com/us/resources/reports/rp-financial-fraud-int-banking.pdf , p. 4] and have many tools to deal with the loss. As unjust and frustrating as it may be, no catastrophic global consequence ensues from a small ecommerce fraud rate. Ecommerce markets are relatively robust, i.e. not overly sensitive to small-scale losses. But in the voting world we are all familiar with the cases where, within about one decade, a senator, a governor, and a U.S. president were all elected by margins much smaller than one vote in a thousand. Small changes in vote totals sometimes have very big, even global consequences, and can push a whole city, state or nation in a new direction. Elections outcomes are thus very sensitive to small errors or frauds in a way that ecommerce systems simply are not. Election security is thus a matter of national security, and the security standards have to be designed to reliably prevent, detect, and correct even very small problems and attacks. That level of security and reliability is neither needed nor cost effective for ecommerce systems.

Voting security, privacy, and transparency requirements are structurally different from those for E-Commerce transactions

The second point of our argument is that the security, secrecy, and transparency requirements for online voting transactions are structurally very different from, and generally much stricter than, those for E-Commerce transactions. The security mechanisms that make ecommerce transactions relatively safe for (consumers at least) are not sufficient to guarantee the safety of online voting.

The first major distinction is that we can at least eventually detect E-Commerce errors and fraud, but we may never even know about online election fraud.[7. See http://servesecurityreport.org/paper.pdf] In the E-Commerce world problems are reliably detected because of such practices as receipts, double entry bookkeeping, and financial audit records kept by both sides of every major transaction. But in the online election world there are no receipts, no double entry bookkeeping, and no meaningful audit trail information. Security experts routinely call for an independent, end-to-end audit trail that can be used to verify that the electronic ballots received by election officials are identical to those the voters sent, and that none were forged, lost, or modified in transit. But the only reliable way to accomplish this with current technology is for voters to send paper copies of their ballots back to their local election officials along with a signed attestation, and for the officials to use those

copies in a formal risk limiting audit procedure.[8. For papers on audit procedures for elections a good place to start is http://statistics.berkeley.edu/~stark/Vote/#papers]

That would solve most of the security problems associated with online voting (though not the privacy problems). But most advocates of Internet voting oppose such a paper-based audit requirement because the additional burden on voters to mail back paper copies of their ballots and signed attestations is essentially equivalent to sending an ordinary paper absentee ballot. Yet without a meaningful end-to-end audit trail a well-constructed attack may lead to the attackers' choice of candidates being elected and there may well be no way to know that anything happened at all. Even if there is suspicion of a problem there will be no way to prove or disprove it. And because of ballot secrecy even if there were strong evidence that particular persons cast illegal ballots, or their ballots were tampered with, officials cannot know which ballots to remove from the count. Hence, fraudulent online voting will most often be undetectable and almost certainly uncorrectable even if detected.

Vote fraud is much less manageable than ecommerce fraud. There is no election analog to the natural business practice of "spreading the cost" or "spreading the risk". There is no way to pass on to other voters the "losses" due to illegal ballots cast by ineligible voters or attackers, or to recover votes changed by malicious software. There is no "insurance" that one can buy to cover those losses. There is just no way to compensate for damage done to an election.

There are several ways in which the security requirements for voting are strictly stronger than those for financial transactions. Eligibility checking is one. In the E-Commerce world essentially anyone including criminals, non-citizens, and minors, is allowed to buy and sell online. Non-human entities, e.g. corporations, government agencies, and estates, are free to engage in E-Commerce transactions as well. And there are usually no residency requirements for E-Commerce transactions. But all such factors play a role in determining eligibility to vote.

Then there is the issue of proxy transactions. In the E-Commerce world you can freely authorize someone else to act as your agent for purchases or funds transfers, or your may authorize others to spend funds from your accounts simply by giving them your credit card number and security code, and/or your PIN or password. By doing so you take responsibility for the consequent risk. For larger transactions you can accomplish the same thing by setting up a joint bank account, signing a contract, appointing a trustee or guardian, giving power of attorney, etc. But in the voting world you are never permitted to transfer your right to vote to anyone else, at least not in the U.S. No one is legally allowed to act as your proxy to vote for you, not even your spouse, and not even with your written permission.

The prohibition of double voting is a third election security requirement that has no analog in the E-Commerce world. A person is free to engage in as many E-Commerce transactions as he pleases but the rule of one person, one vote is fundamental. The double vote check is actually complex because it has to cover not just voting a second time online (which is easy to prevent), but also voting a second time by paper absentee ballot or in person at the polls.

Because of the need for eligibility checking, proxy vote prevention, and double vote prevention we are required to verify the actual identity of voters. In contrast for an E-Commerce

transaction we only have to verify that the person doing the transaction is authorized to use a suitable financial account, which is a much lower requirement. We need a strong identity verification procedure for online voting because if an attacker can figure out how to cast one illegal vote online through a weakness in the identity verification, then he can probably automate that attack to allow thousands of phony votes to be recorded. But reliably verifying the actual identity of a potential voter remotely through the Internet is a difficult and unsolved problem in the U.S. The U.S. does not issue national identity cards with private keys embedded in them, and even if it did today's computers and mobile devices are not equipped with devices to read them securely. Nor do election jurisdictions keep a database of faces, fingerprints, or other biometric data about registered voters, and once again even if they did computers today are not equipped to read and transmit them securely. It is not sufficient for the voter to just present a PIN number or password or the answer to a challenge question (e.g. "What city were you born in?"). Any such data might be given away, guessed, stolen, or sold, and thus does not constitute sufficient proof of identity because the danger of automated online buying and selling or stealing of such voting credentials is a major concern.

In most states voters prove their eligibility to vote when they register and then provide an ink signature sample for use later in authenticating the voter. Voters prove their identity when they vote, either at the polls or via paper absentee ballot, by duplicating that ink signature on record. Some states are now going further and requiring voters to provide photo ID documents at the time of voting. But we cannot get a wet ink signature from a voter through the Internet to compare against the registration records, nor can the voter present his or her face along with a matching photo ID or passport. As of now there is no reliable infrastructure in place to verify over the Internet the actual identity of a person sitting at a PC or holding a mobile device.

There is no comparable requirement for ecommerce transactions. No real proof of identity is required. All that is really required to do an online transfer of funds out of your bank account is knowledge of the name, account number, and password or pin associated with the account, but there is no check of the actual identity of the person doing the transaction. Or, as another example, consider that when you sign up for an ecommerce account, e.g. at Amazon.com, they ask for your name and address, but they do not ask for a picture, or an ink signature, or your driver's license, or passport or other proof of identity. They never really check those, and they have no way to do so. After creating an Amazon account all that is really required to make a purchase is reasonable evidence that you are in possession of some (any!) valid credit card, usually demonstrated by giving the name on the card, and the account number, security code, expiration date, and password or pin. If those numbers are validated by the credit card company and the account is not over its limit then the transaction is allowed. If the credit card turns out later to have been stolen, the problem will be sorted out after the fact.

The privacy requirements for ecommerce and voting transactions are also fundamentally different. An ecommerce transaction is generally symmetric between buyer and seller, with both parties in theory fully aware of all the details of what is being bought and sold, for what price, with what warranties, and who has what rights to void the transaction, etc. For larger transactions there is usually an exchange of official paper receipts with names, dates, prices, conditions, and other transaction details so that in case of a dispute either the buyer or seller can prove to a third party (e.g. a court) exactly what the transaction was supposed to be

so the dispute can be resolved.

But it cannot be the same with voting transactions. While the voter of course knows the details of his votes, election officials must not. Officials know the names of those who voted, and the contents of the cast ballots, but they are never supposed to know exactly who cast which ballot. This is a requirement for information suppression, a partial blindness on the part of one side in the transaction that has no analog in the E-Commerce world. Furthermore, although each voter knows how he personally voted and is free to tell anyone, he is not allowed to have any proof of how he voted that could convince a third party. This is the most powerful protection we have against the threat of vote selling and vote coercion, and is unique to voting. I know of no other security situation in which people are completely free to disclose a fact that they know (how they voted), but are not permitted to have any proof of that fact that can convince someone else that they are telling the truth. In tis respect voting privacy requirements are almost the opposite of E-Commerce privacy expectations in which both sides generally insist on possessing proof of the details of a transaction.

The unusual vote privacy rules have strong consequences that we cannot avoid. As noted earlier, if for some reason officials learn after the fact that a particular person has succeeded in casting an illegal ballot there is no way to find it to remove it from the count. In the U.S. and most other countries once a voting transaction is complete it cannot be undone even in principle because the information needed has been deliberately lost. In that sense a voting transaction is irreversible. In the E-Commerce world, however, we go to some lengths to make sure most transactions are reversible in case it is found to be erroneous or fraudulent, or if goods are damaged, or sometimes even if one party simply has second thoughts. Money and merchandise can be returned, and records can be corrected. For that reason people feel free to take prudent risks with online financial transactions based on the reputation of the merchant or the credit history of the buyer. But there is no concept of “reputation” or “credit worthiness” in the election world to help manage risk. These differing vulnerabilities to failures and fraud lead to very different security approaches in online transaction software. For election security there is a very strong imperative for up front, absolute prevention of errors and fraud. For ecommerce there is usually much reduced need for strong security barriers up front because problems can usually be corrected later.The flip side of privacy is openness or transparency. Once again, the requirements are completely different for E-Commerce and for online voting. In the ecommerce world a person buying something online is entitled to know everything about his particular transaction, but nothing about other people’s transactions. A buyer is not entitled to know how many other transactions there are, what the merchant’s revenues or profits are, who else the merchant sells to, or what price others pay for the same goods or services, and he has no right to audit the books of the merchant he is dealing with.

In the voting world, however, most of this is reversed. Complete election information is (or should be) open to all. Election officials report not just the names of the winners, but also exactly how many votes were cast and how many each candidate received down to the precinct level. The list of exactly who voted is also usually public, and in some jurisdictions so are the original ballot images. In principle all information bearing on the outcome of an election that does not compromise vote privacy is (or should be) public. Candidates, parties, and the public are entitled to participate in open audits, challenges, and recounts so that everyone, especially

losing candidates, can be satisfied that the election was conducted according to law and the votes were counted accurately. Election officials are thus accountable to candidates and voters for the integrity of every relevant detail of an election, whereas merchants are usually accountable only to buyers, and then only for each buyer's own transactions.

The pattern of motivation for fraud is profoundly different between the commercial and electoral worlds. In an E-Commerce situation all transactions are essentially independent. A buyer hasno particular incentive to spoil or tamper with another buyer's online purchase since two buyers rarely have conflicting interests. In any case the problem would almost certainly be detected and corrected. And it is hard to imagine a motive for another nation to bother messing with many Americans' E-Commerce transactions. But the situation is completely different with voting transactions. There is a powerful partisan incentive to block or change other people's votes, especially if it can be done without detection. The motivation to automate that process to affect thousands of online votes is that much greater. Such attacks can be done for tens of thousands of dollars or less, while the monetary value of changing the outcome of an election can be hundreds of millions of dollars or more, and the non-monetary value can be immense as well. With Internet voting the danger is actually much worse because anyone on Earth, including foreign governments, could derive great benefit from tampering with with U.S. elections, especially since it is unlikely they will be caught or brought to justice. Online voting is thus a national security risk in a way that E-Commerce simply is not.

The sum of all of these considerations is simple. The security, privacy, and transparency requirements for online voting are much more complex and stringent than they are for E-Commerce transactions. The acceptability of small losses and the strategies for managing risk are very different between the two. And it is hard to grasp the full implications of the fact that online elections might be compromised and the wrong people elected via silent, remote, automated vote manipulation that leaves no audit trail and no evidence for election officials or anyone else to even detect the problem, let alone fix it. These ultimately are the reasons we cannot provide satisfactory security for online voting even though we can for online commerce.

What About Email and Fax?

In recent years many States have begun to allow military and overseas voters to cast ballots by fax or as email attachments. Neither the Internet itself, nor voters' computers, nor the email vote collection servers are secure against any of a hundred different cyber attacks that might be launched by anyone in the world from a self-aggrandizing loner to a foreign intelligence agency. Such an attack might allow *automated* and *undetectable* modification or loss of any or all of the votes transmitted. While all Internet voting systems are vulnerable to such attacks and thus should be unacceptable to anyone, email voting is by far the *worst* Internet voting choice from a national security point of view since it is the easiest to attack in the largest number of different ways.

The computer security research community in the U.S. is essentially unanimous in its condemnation of any currently feasible form of Internet voting, but most especially of email voting. Verified Voting strongly urges legislators in states considering e-mail voting to request testimony from other *independent* computer network security experts who are not affiliated with or paid by any voting system vendor. Email voting is extremely dangerous in ways that people without strong technical background are not likely to anticipate.

Problems with the E-mail transmission of Voted Ballots

1. Lack of privacy: Emailed ballots are always transmitted essentially in the clear, never encrypted. (The exceptions to this generalization do not apply to email carrying ballots. The reasons for this are technical, but they will not change in the foreseeable future.) Most state statutes that allow email voting bill explicitly recognizes that it is impossible to guarantee vote privacy with email voting, and require voters, if they choose email their voted ballots to their election officials, to sign an affidavit waiving the anonymity of their votes. It is common for national intelligence agencies (including our own) to collect and store *all* email that crosses national boundaries, and that would include emailed ballots along with the names of the voters and related information. Also, many voters (including military voters) get their email service through their employers who legally reserve the right to inspect all incoming and outgoing email. So voters should be aware that their votes are *not* guaranteed to be private, and in many cases they are almost *guaranteed not* to be private.

2. Vote manipulation while in transit: –That email is not encrypted does not just compromise voter privacy. Without encryption, emailed ballots can be easily modified or manipulated *en masse* while in transit from the voter to the local election officials. Email is transmitted from router to router, and from forwarding agent to forwarding agent along the transmission path, through infrastructure that belongs to various corporations and national governments. It is trivial for any IT person who controls one of these routers or forwarding agents to filter, out of the vast stream of email, exactly those emailed ballots addressed for a chosen set of election email servers (such as county servers in one or more states that are of interest to the attacker), and then to automate a process to either discard ballots that contain votes she does not like, or replace them with forged ballots that she likes better, all the while keeping the voter's signed waiver and envelope attachments intact. **Such malicious activity would only result in a transmission delay on the order of one second or so.** This is anything but difficult. There are thousands of people in the

U.S. who have the skill and are in a position to do this *easily* for at least some ballots, and vastly more in other countries. Unless all of the received ballots are made public on a web site associated with the names of the voters who cast them there would be *absolutely no way* to detect this on-the-fly ballot manipulation. Neither the voter nor election officials would be able to notice any irregularity.

3. Server penetration attacks: Even in the ideal and highly unlikely instance that e-mailed ballots are strongly encrypted in transit from the voter to the election official; anyone in the world can mount a remote attack on the server collecting emailed votes. If the attackers are competent and determined there is essentially no chance that they will fail (despite the common overconfidence of the IT staffs running servers). Every major high tech company in the US, and most government agencies have been victims of such attacks, including RSA, Google, and the White House. These are organizations with security expertise and infrastructure dwarfing that of any voting system vendor or election administrator. Just last October the Washington, D.C. Board of Elections and Ethics (BOEE) was forced to cancel its planned November Internet election because security researchers proved that they could easily penetrate the BOEE network while sitting at the University of Michigan. They were able to take complete control of *all* the voted ballots and replace them all with phony ones. University of Michigan Prof. Alex Halderman, who led the team of researchers that conducted the DC hack, has published a concise account of the DC hack.

4. Ballot files can carry malware into the election network: Most state legislation enabling email voting does not specify what types of files the emailed ballots, and waivers must be. But for various reasons vendors and election officials almost always opt to allow PDF (Portable Document Format, by Adobe). Most people are familiar with this file type, of course, but it is not widely known to the general public that *PDF has one of the longest security rap sheets of any document type*. In particular, innocent looking PDF files are able to carry very dangerous *malware* that can open a backdoor to remote control of the election network. Once the vendor or local election officials set up a server to receive email ballots they are opening themselves up to a PDF attack that anyone on Earth can launch by sending a specially constructed PDF "ballot" that is infected with malware. Once the ballot is *opened* the malware instantly does its work. There are ways to partially ameliorate this vulnerability (but only partly). However, even partial ameliorations greatly increase the development cost and operational complexity of the vote collection infrastructure.

5. Voters' computers infected with malware: As if the unacceptable and largely immitigable risks described above were not enough to discredit email balloting, we have not yet addressed one of the most certain sources of malware: the voters' own computers. As most users of the Internet are now aware, our personal computers are routinely infected with malware from all over the world. If email voting becomes common I would fully expect that some enterprising malware designer will decide to create and spread *and sell (!)* a malware module that sits silently on a voter's computer doing nothing at all until he sends an email to one of the particular addresses that is used to collect ballots, at which point it will modify the To: address just as the email leaves the computer to send the ballot to the malware-designer's own shop for inspection and modification before forwarding it on to election officials at home. Again, I implore election administrators and lawmakers to reject assurances that such an attack is hard. It takes a little more skill than some of the other attacks, but it is much harder to detect and prevent than the attacks on vote servers, and is well within the competence level of the attackers who carried out the Google hack and numerous other attacks against highly protected corporate and government computer networks, If I were a cyber attacker in a country that is a U.S. rival I would use an attack like this (among others).

6. Denial of service attacks: Email can be subject to *denial of service* attacks. It is easy, for example, to have a million emails sent to the voting email address, vastly swamping the relatively

small number of legitimate ballots that a jurisdiction might expect and possibly crashing its server or overloading its routers. Anyone who owns or rents a large *botnet* (a collection of infected PCs controlled by one criminal or organization) can do this in minutes from the safety of overseas locations that are untraceable and out of reach of U.S. law. This might be just a huge nuisance attack. But if it lasts for the final hours of Election Day, the emailed ballots arriving during those hours will be delayed until it is too late to count them (as specifically mentioned in this bill) and thousands of voters can be disenfranchised. (A related denial of service attack happened in a Canadian election in 2003. Today it would be much easier to launch a much larger attack.)

7. Email ballots are unauditable; attacks are undetectable and irreparable: Email ballots, like those cast on paperless electronic voting machines in polling places, are completely unauditable in any meaningful way. There is no way, even in principle, to verify that the electronic ballot that arrives at the election server is the same as the one the voter intended to send. The above attacks (except for denial of service) are likely to be completely undetectable. The wrong persons might be elected, the wrong initiatives passed or rejected, and no one would ever know. Even if some attacks were somehow detected, *there is no way to know whose votes were modified or discarded*so there is *no way to repair the damage!*

8. Multiple simultaneous attacks: Like all other forms of Internet voting, email elections need not be attacked by just one person or organization at a time. Multiple independent attacks by people who may not even be aware of each other could be simultaneously directed at the same email election from anywhere in the world. This make effective defense, already essentially hopeless, even more difficult

9. These facts will not change: These vulnerabilities are facts about email voting. They are fundamentally built in to the architecture of email, of the Internet itself, and of the PCs and mobile devices that people vote from, and are not going to change for as far ahead into the future as anyone can see. Anyone's security claims to the contrary should be treated with extreme skepticism. No amount of encryption (even if it were used for some parts of the voting infrastructure), no amount of firewalling, no use of strong passwords or two factor authentication, no amount of voter signature checking, and no other security tricks of the trade are sufficient to materially change these facts.

Similar problems with FAX voting

The issues raised above security concerns specifically addressed email voting, but almost identical considerations apply to FAX voting. While FAX and email seem superficially different, they are in fact very similar from a security point of view. Faxes are sent unencrypted; they are forwarded from switch to switch within the telephony infrastructure of many private and national corporations; they are subject to absolutely trivial denial of service attacks. The similarity is so great that there is a FAX analog for every one of the email vulnerabilities listed above. Moreover, with the increasing popularity of Web-based services such as eFax, FAX is increasingly a Web-based, rather than a telephony-based, process, rendering distinctions between FAX and email voting less relevant each year.

The move toward Internet distribution of blank ballots

It is clear that overseas and military voters experience barriers that are largely associated with mail delays. While there are a number of cyber security issues regarding the electronic transmission of blank ballots to voters via the Internet, those issues are *much* more manageable than those for the electronic return of voted ballots. I suggest that election officials and lawmakers consider a program to reduce overseas mail delays by allowing voters to download blank ballots from a web server, then print them, mark them, and mail them back to local election officials. Such a process will eliminate at least one transoceanic mail delay and also eliminate the need to have accurate

addresses for military on the move in the field. It will go a long way to relieving the problems of overseas voters without endangering the security of the entire election.

For these reasons Verified Voting strongly urges states that do not currently provide for email voting not to start down that path. In my professional opinion this path leads only to a major risk to U.S. national security, exposing our elections to easy manipulation by anyone in the world.

David Jefferson is a computer scientist and researcher at Lawrence Livermore National Laboratory in California where he studies cyber security and ways to protect the nation's military, civilian, and government networks from cyber attack. He is also the Chairman of the Board of Verified Voting, and has been studying electronic and Internet voting for over a decade, advising five successive California Secretaries of State on voting technology issues.

 Download this page in PDF format

Verified Voting Blog: Report on the Estonian Internet Voting System

Sep 3 2011 » Barbara Simons

I visited Estonia in mid-July of this year at the invitation of Edgar Savisaar, the country's first prime minister and current mayor of Tallinn. Mr. Savisaar is the leader of the Centre Party, which placed second in recent national elections. The Centre Party and Mr. Savisaar have been questioning the outcome of the Internet voting portion of those elections. They invited me to Estonia because of a presentation I made at a European Parliament panel on the risks of Internet voting.

I told my hosts that I was happy to discuss the risks of Internet voting, but I would not comment on internal Estonian politics. When asked whether or not I thought the national election was rigged, I refused to comment, aside from saying that no one could prove that it was or was not rigged, because there is no way to conduct a recount of an Internet election.

The Internet portion of the 2011 election lasted from February 24 to March 2, with paper balloting conducted on March 6. The Internet vote was counted the evening of March 6. Estonian law allows complaints to be submitted only during the 3 days immediately following the procedure being challenged. Since Internet voting is considered separate from paper voting, the final day for submitting complaints about Internet voting was March 5. Graduate student Paavo Pihelgas was the only person who submitted a complaint by the deadline. (The Centre Party and independent candidates tried to file complaints, but they did not do so within the required 72 hour time frame).

Pihelgas asked the National Election Commission (NEC) to cancel the election results, since the possibility of election-rigging malware meant that there was no way to be sure that the voters' preferences had been correctly recorded. NEC rejected his complaint the following day, saying that they have all the necessary provisions to detect such cases, without specifying what those provisions are. When Pihelgas resubmitted his complaint, it was forwarded to the Supreme Court. The Supreme Court dismissed the complaint on March 21, say that the voter can file a complaint only when his/her rights have been breached.

I have communicated with several Estonians before, during, and after my trip. I have also read a report written by a team from the OSCE/ODIHR (Organization for Security and Cooperation in Europe/Office for Democratic Institutions and Human Rights) who observed the March 2011 election, and I have talked with a member of the OSCE/ODIHR team. Based on the information I have obtained, I have concluded that the Internet voting system used in Estonia is insecure.

1. There are a number of serious problems, as described by the OSCE/ODIHR report;

2. The voters' privacy (secret ballot) is vulnerable;

3. The voters' computers are vulnerable to election rigging malware;

4. There is an insider threat;

5. The server is vulnerable to attack from anyone/anywhere;

6. The system is not open or transparent;

7. There has been no security evaluation of the system by independent computer security experts.

The rest of this memo expands on the above concerns. To distinguish between OSCE/ODIHR report recommendations and my comments, I have italicized report comments and recommendations.

1. **The OSCE/ODIHR report.** Here are some of the problems uncovered by the report:

a) *NEC has no IT experts; they relied on the IT department of the Estonian Parliament (Riigikogu). The Report recommended that the NEC create in-house IT expertise and retain written records of all stages of the Internet voting process.* While the need for IT experts is obvious, the need for computer security experts is even greater.

b) *One programmer "verified" the software, but the results were secret. The Report recommended that the test results be published on a website.* We have since learned (this was unknown to the OSCE/ODIHR team) that the only source code audit was done by Martin Paljak, who became sick. Paljak may have given initial verbal feedback, but he did not provide a final written report.

c) *The project manager could update software without any formal procedure.* The project manager for electronic voting told Pihelgas that the last modifications to the voting application were made four days before the first day of election. This is a huge security vulnerability. The project manager could intentionally or inadvertently insert election rigging code into the software, or even trigger malware that had already been installed. There is no way to check or analyze any last minute code insertions.

The OSCE/ODIHR report recommended that formal procedures for software deployment be developed and deadline for updates be established. The report also recommended that maintenance of the Internet voting system during the entire Internet voting process be prohibited.

d) *The electronic ballots were destroyed on April 11.* This is because Estonian law requires all ballots to be destroyed within a month of the election. The result of the ballot destruction is that it is impossible to conduct any kind of post-election analysis of the ballots, something that clearly is undesirable.

e) *Although the Election Act indicates that NEC can invalidate the results of the Internet voting, it does not specify on what basis and under which circumstances the results of the Internet voting could be declared invalid. It also does not specify how voters should be informed that they have to recast their votes on paper on election day. The report calls for the creation of a disaster recovery plan.*

Even if the report recommendations were implemented, major problems would remain. If a successful attack (perhaps a Denial of Service attack, such as the one conducted by Russia against Estonia in 2007) were to occur just before the end of the election, people who had been planning to vote over the Internet may not have enough time to cast paper ballots. But even more serious is the possibility that an attack might be discovered, or even announced by the perpetrators, after a new government had been sworn in. What would happen then? How would the country react? Would the "losers" accept the new government? Would the previously announced winners allow a new election to take place? Would people question the results of previous elections that included Internet voting? How would Estonia's new and still developing democracy cope with

potential massive distrust?

And of course there is the ultimate threat, namely that the election is successfully rigged without detection. This could be done by attacking vulnerabilities in the system being used to collect and tabulate the votes and/or by planting election rigging malware on voters' computers.

2. The voters' privacy is not adequately protected. Quoting from *On applying i-voting for Estonian Parliamentary elections in 2011*, by Sven Heiberg (to be presented at VoteID 2011, September 28 – 30, Estonia; sent to me by Heiberg and quoted with permission):

> For example, anonymization of i-votes can only occur in the presence of at least 2 election officials, auditor and possible observers. All procedures are defined beforehand in written form, all actions and outcomes are recorded on tape. Without enforcing those regulations, IVS owner could manipulate the election results on large scale by adding or removing votes from the digital ballotbox without getting caught.

"Anonymization of ivotes" refers to the separation of voters' names from their ballots. (There is a cryptographic approach using "mixnets" for anonymization of votes that preserves the voter's anonymity. But that approach is complex and must be carefully implemented. I have confirmed that mixnets are not being used in Estonia).

Observing the anonymization process means watching a technician type a command that runs a program. But who know what that program does? How can you verify that there is not another copy of the ballots somewhere with voter names associated with them? Indeed, there should be another copy for backup purposes, or else the vote data is at risk of loss. Hence, anonymization must be a multistep
process something like:

1) From a copy of the i-ballots attached to voters names run a script that separates the ballots from the voters names, outputting two files, one with the ballots only and one with the names only.

2) Sort one or both of those files in random order to destroy any order correlation between the names in the name file with the ballots in the ballot file.

3) Run a check that no data has been lost or corrupted in this process.

4) Make several backups of the separated files.

5) Destroy ALL copies and backups of all ballots that have a name associated with them. This last step is essential, but inherently unverifiable. There is no way to prove that all such copies have been destroyed; it will likely be so difficult to find ALL of the copies normally made in the course of routine system behavior that as a practical matter it probably will not be perfectly accomplished.

It is inherently not possible to "observe" or verify that there is no remaining data somewhere that would allow reconstruction of the association between voters' names and their ballots. Vote privacy is not an observable or auditable property.

3. The voters' computers are vulnerable to election rigging malware. There are many examples of very clever viruses and worms, such as the Zeus virus, that have successfully stolen large sums of money from, for example, users' on-line bank accounts. Specially modified versions of Zeus are even available on the black market. It would be relatively straightforward to modify Zeus to steal an election. As Estonian cryptographer Helger Lipmaa says in his blog:

> Voter computers are an obvious problem: most of the people are computer illiterate, and are not able to check if their computers are not infected. Even if they have the newest antivirus (which we can't be sure of), that antivirus itself might not be able to detect a piece of new malware that has been written specifically for *that* election and is unleashed just before it.

(Note: in Estonia e-voting lasts for 3 days.) That malware could do a lot of damage, like hijack the connection between you and the ID card (basically letting the ID card to sign wrong votes), between the GUI and what actually happens inside the computer, etc. I would *not* be surprised if such a piece of software was written by a high-school kid.

4. There is an insider threat. In addition to the threat posed by the ability of the project manager to make software updates with no formal procedure, the OECD/ODIHR Report stated:

> "Daily update of the voter register during the voting period as required by the Election Act was performed together with the daily backup of data. The project manager accessed the servers for daily data maintenance and backup breaking the security seals and using a data storage medium employed also for other purposes.This practice could potentially have admitted the undetected intrusion of viruses and malicious software."

Besides the malware risk, the daily update could facilitate an attack that singled out voters likely to vote for a particular candidate. For example, such votes could be "lost". There is no way to check.

5. The server is vulnerable to attack. A serious China-based Internet attack on Google and dozens of other companies illustrates that even major corporate sites are vulnerable. The attack targeted Google intellectual property, including systems used by software developers to build code, as well as Gmail accounts of Chinese human rights activists. As many as 34 companies – such as Yahoo, Adobe, Juniper
Networks, defense contractor Northrop-Grumman, and Symantec, a major supplier of anti-virus and anti-spyware software – were targeted. The attacked companies employ large numbers of computer security experts and have considerable security expertise and resources.

Government sites, in the U.S. and elsewhere, are also vulnerable. In a March 2010 talk, U.S. FBI Director Robert Mueller said that the FBI's computer network had been penetrated and the attackers had "corrupted data." General Michael Hayden, former Director of the CIA and the National Security Agency, has stated: "The modern-day bank robber isn't speeding up to a suburban bank with weapons
drawn and notes passed to the teller. He's on the Web taking things of value from you and me."

Given how insecure the Internet is, it is unlikely that the server receiving the Internet votes in Estonia could resist all attacks coming from another country, political party, individual hackers, etc.

6. The system is lacking in transparency and openness. The OSCE/ODIHR Report states [emphasis added]:

> Firstly, the Internet voting project manager tested the software delivered by the vendor. This was, however, carried out **without formal reporting**. After that, the Cyber Defense League (CDL) conducted an exercise in January 2011 to test the software under given threat scenarios, and produced a report for the NEC that was made available to observers but not to the public. In February, the CDL tested the functionality of the Internet infrastructure under extreme conditions and decided to create a 'whitelist' that contained Internet addresses from where legitimate votes could be expected (including embassies abroad).
>
> In a parallel process, a programmer, who was contracted by the NEC, verified the software code. **The identity of the programmer and his report to the NEC was kept secret. It was not made available to the OSCE/ODIHR EAM, other observers or political parties.**
>
> .... Testing is a crucial exercise to find any deficiencies in the system. The NEC made a substantial effort to test various components of the Internet voting, including by members of the public. However, **reporting on the performed tests was often informal or**

kept secret.

Pihelgas had requested all reports. Recently, he learned that there is no written report of the testing conducted by the project manager. He has also learned that the CDL did not audit the software. Since the CDL report is being withheld, Pihelgas has filed an appeal with the Data Protection Inspectorate. He is hoping to receive a copy of the report.

7. There has been no security evaluation by outside experts. Anyone wishing to review the code or examine the system must sign a Non-Disclosure Agreement (NDA). Several prominent computer security experts have expressed an interest in examining the Estonian system, but none is willing to do so if an NDA is required. One possible exception might be a time-limited NDA that would give the operators of the system time to implement fixes before the report is released.

I want to thank my Estonian hosts for affording me the opportunity to learn more about the Estonian Internet voting system. Thanks also to those Estonians who provided me with technical information about the system, especially Paavo Pihelgas, Priit Kutser, Helger Lipmaa, and Sven Heiberg. Finally, thanks to David Jefferson for his very useful comments.

Categories: **Verified Voting Blog** | Topics: **internet voting**

2 Responses to "Report on the Estonian Internet Voting System"

Internet Voting and Good Governance | says:

09/14/2011 at 5:20 PM

[...] brings us back to the problem with Estonia as a dataset. Namely, the system's lack of auditability, transparency, and independent assessment, combined with unanswered security concerns has eroded voter trust in the system's integrity. If [...]

Curiosidades de la moderna Estonia | Historias del Este says:

10/16/2011 at 10:26 AM

[...] Report on the Estonian Internet Voting System – Verified Voting Blog [...]

Hackers Elect Futurama's Bender to the Washington DC School Board

Researchers hack the Washington DC electronic voting system, and elect Bender, the drunk robot from Futurama, as school board president.

Kevin Lee (PC World (US online)) | **03 March, 2012 07:52**

Electronic voting has earned a pretty bad reputation for being insecure[1] and completely unreliable[2]. Well, get ready to add another entry to e-voting's list of woes.

One Bender Bending Rodríguez[3] was elected to the 2010 school board in Washington DC. A team of hackers from the University of Michigan got Bender elected as a write-in candidate who stole every vote from the real candidates. Bender, of course, is a cartoon character from the TV series Futurama[4].

This was not some nefarious attack from a group of rouge hackers: The DC school board actually dared hackers to crack its new Web-based absentee voting system four days ahead of the real election. University of Michigan professor Alexander Halderman[5], along with two graduate students, did the deed within a few hours.

After looking over the e-voting system's Ruby on Rails software framework, Halderman's team discovered that they could use a shell injection vulnerability to get into the system. This allowed them to retrieve the "public key," which is used to encrypt the ballots. With the public key in hand, the hackers were able to change every ballot already in the system and replace any subsequent real ballots with fakes.

While the hackers were mucking about the system's server, they discovered other files that were not ballot-related in the /tmp/ directory. Among them was a 937-page PDF containing instructions to individual voters as well as authentication codes for every voter. If someone with malicious intent got their hands on these codes, they could use them to cast ballots as a real voter.

The researchers also managed to hack into the network, allowing them to gain access to other systems within the building. The team was able to get into the surveillance system, which gave them access to the security cameras. This allowed them to time their attacks so that the technicians would not notice the additional server activity.

When the team tried to get into the terminal server, they noticed there was an attack coming from Iran; they traced the IP address to the Persian Gulf University. The team realized the Iranians were getting in with one of the default admin logins (user: admin, password: admin). To stop the outside attacks the team blocked the offending IP address with iptables[6] (a piece of software for server admins) and replaced the admin password with something more challenging. The team also blocked similar attacks launched from New Jersey, India, and China.

For the team's pièce de résistance, the researchers replaced the "Thank you for voting" note with "Owned," and programed the site to start playing the University Of Michigan's Fight Song "Hail To The Victors![7]" 15 seconds later. Despite all this, the system administrators did not notice anything strange until two days later.

Halderman's closing statements on e-voting are that a single flaw in the configuration of the system could be fatal, and secure Internet-based voting won't be ready until there are significant fundamental advances in computer security. Be sure to check out the full paper on Attacking the Washington, D.C. Internet Voting System[8].

(pdf) via The Register[9] and Gizmodo[10]]

Like this? You might also enjoy...

- Nyan Cat and Other Memes Become Potential Lego Sets: Me Gusta[11]
- The World's First Cupcake ATM: The Best New Tech Product of the Year?[12]
- Researchers Develop a Speech-Jamming Gun That Will Shut You Up[13]

Get more GeekTech: Twitter [14]- Facebook [15]- RSS[16] | Tip us off[17]

References

1. http://www.infoworld.com/t/security/e-voting-still-insecure-even-paper-trail-177623
2. http://cityroom.blogs.nytimes.com/2010/09/14/problems-reported-with-new-voting-machines/
3. http://en.wikipedia.org/wiki/Bender_(Futurama)
4. http://en.wikipedia.org/wiki/Futurama
5. https://jhalderm.com/
6. http://en.wikipedia.org/wiki/Iptables
7. http://www.youtube.com/watch?v=mY3M_9I_Rg8
8. https://jhalderm.com/pub/papers/dcvoting-fc12.pdf
9. http://www.theregister.co.uk/2012/03/01/electronic_voting_hacked_bender/
10. http://gizmodo.com/5889838/hacked-dc-school-board-e+voting-elects-bender-president
11. http://www.pcworld.com/article/251154/nyan_cat_and_other_memes_become_potential_lego_sets_me_gusta.html
12. http://www.pcworld.com/article/251118/the_worlds_first_cupcake_atm_the_best_new_tech_product_of_the_year.html
13. http://www.pcworld.com/article/251096/researchers_develop_a_speechjamming_gun_that_will_shut_you_up.html
14. http://www.twitter.com/geektech
15. http://www.facebook.com/geektech
16. http://feeds.pcworld.com/pcworld/blogs/geektech/
17. http://www.pcworld.com/article/212336/got_a_geeky_news_tip_send_it_our_way.html

---