Policy Brief 2011-04

We respectfully ask you to defend election integrity by amending HB11-1219.

The Board of Directors of Coloradans for Voting Integrity submits two amendments that will strengthen HB11-1219.

This CFVI Policy Brief gives the rationale behind the amendments. On the back page of this document, Appendix E presents suggested language for the needed amendments.

Thank you for your attention and your service to all Coloradans.

Sincerely,

Margit Johansson, Board Member
For the Board
Coloradans for Voting Integrity (CFVI)
(303) 442-1668

Coloradans for Voting Integrity is a collection of concerned Colorado citizens dedicated to fair, accessible, and verifiable and verified voting on the state and national level.

Board Members: Joe Richey, President, Boulder (Boulder County), CD 2, SD 18, HD 11; Margit Johansson, Corporate Secretary, Boulder (Boulder County), CD 2, SD 18, HD 13; Angie Layton, Treasurer, Louisville (Boulder County), CD 2, SD 17, HD 12; Harvie Branscomb, Unincorporated Eagle County, CD 2, SD 8, HD 61; Marilyn Marks, Aspen (Pitkin County), CD 3, SD 5, HD 61; Kathryn Wallace, Arvada (Jefferson County), CD 7, SD 19, HD 29.

Contact Coloradans for Voting Integrity at www.cfvi.us, richey80304@yahoo.com, (970) 963-1369, or
3938 Wonderland Hill Avenue, Boulder, CO 80304.

April 15, 2011

Dear Members of the Senate State, Veterans and Military Affairs Committee,

"Distance voting" using the mails or electronics is more vulnerable to manipulation than voting done with paper ballots and proper procedures in local polling places. Recently, efforts have been made to overcome some of the drawbacks of voting from a distance for absent uniformed service personnel and overseas civilians, and progress has been made in making the process timely and reliable.

In its present form, HB11-1219, Concerning the "Uniform Military and Overseas Voters Act," does little to improve the chances that the votes of these groups will be counted as intended and that all absentee ballots purportedly from these groups will be genuine.

We offer Committee Members two amendments to help improve the bill.

<u>AMENDMENT #1</u>: TO PROHIBIT THE ELECTRONIC TRANSMISSION OF VOTED BALLOTS.

- Voted ballots transmitted electronically[1] cannot be made secure with the present Internet, as eminent computer security experts warn in Appendix A.
- Just because some claim encryption secures Internet voting, that doesn't make it so, as a world-class encryption expert explains in Appendix B.
- Other steps being taken to ensure that absent military personnel and overseas civilians are able to vote, short of imperiling voted ballots, are briefly described in Appendix C.
- Hacking happens. Hacking of time-sensitive elections could be particularly devastating. Internet voting could be a gold mine for vendors and ruthless political operatives, but toxic to our democracy. See Appendix D for recent examples of hacking.
- Changes in HB1219 needed to reflect this amendment are given in Appendix E.

[1] "Electronically" includes use of facsimile (which now often utilizes the Internet for transmission), email, and other forms of Internet voting.

AMENDMENT #2: "COVERED VOTERS" SHOULD INCLUDE ONLY ABSENT UNIFORMED SERVICE PERSONNEL, NOT THOSE RESIDING IN THE U.S. COUNTY WHERE THEY ARE REGISTERED TO VOTE.

- The following should be removed: "A UNIFORMED-SERVICE VOTER," listed as a "COVERED VOTER" in 1-8.3-102(2)(a).
- Military service voters living in their home county do not require the special voting provisions offered the military who are absent from their home county during an election.
- The ULC's Uniform Bill (UMOVA) was originally titled a "Military Services and Overseas Civilian Absentee Voters Act" (italics added). The expansion to cover non-absentee military voters was proposed late in the bill's drafting and necessitated a title change, whereby the word "absentee" was removed, to the current "Uniform Military and Overseas Voters Act (UMOVA)."
- Inclusion of non-absent military as "covered voters" could cause considerable confusion for election officials, making their jobs more difficult than they already are.
- This expansion of covered voters could subject many more military voters to the insecurity of Internet voting.

APPENDIX A.

EXPERTS SPEAK OUT ON THE INSECURITY OF THE INTERNET FOR VOTING

1. Computer security experts have written the following rebuttal to the DOD report that promoted use of the Internet for UOCAVA citizens.

A comment on the May 2007 DoD report on Voting Technologies for UOCAVA Citizens

David Jefferson,[1] Avi Rubin,[2] Barbara Simons[3]

We have reviewed the Department of Defense report titled "Expanding the Use of Electronic Voting Technology for UOCAVA Citizens" of May 2007. We find the report quite troubling.

Although the report describes many laudable ways to simplify voting for overseas Americans, it also appears fundamentally to be advocating for "a complete Internet voting system", i.e. one that allows voters to cast their ballots on their own PCs and transmit them to the home jurisdiction over the Internet. The report estimates that it would take between 24 and 60 months to develop such a system, depending on recommendations and guidelines.

In 2003 the Department of Defense engaged our services to review its SERVE Internet voting project. The project was subsequently killed because of the numerous and fundamental security problems with it that we documented in a report we issued in 2004 (http://www.servesecurityreport.org). We are concerned that this new report appears to be trying to persuade readers that SERVE was a successful project and that Internet voting can be made safe and secure. Unfortunately, it does not accurately reflect the degree of concern that we and many others have expressed about Internet voting.

The new report includes (page 12) only the following selective quote from our report:

> We want to make it clear that in recommending that SERVE be shut down, we mean no criticism of the FVAP, or of Accenture, or any of its personnel or subcontractors. They have been completely aware all along of the security problems we described, and we have been impressed with the engineering sophistication and skills they have devoted to attempts to ameliorate or eliminate daunting security problems. We do not believe that a differently constituted project could do any better job than the current team.

These are about the only lines in our entire report that were not critical of the SERVE project. Those comments were intended to soften an otherwise harsh assessment, and to make it clear that it was the technology, rather than the people, that we were criticizing. The immediately following sentences from our report were not quoted, but they more accurately reflect the report as a whole:

> The real barrier to success is not a lack of vision, skill, resources, or dedication; it is the fact that, given the current Internet and PC security technology, and the goal of a secure, all-electronic remote voting system, the FVAP has taken on an essentially impossible task. There really is no good way to build such a voting system without a radical change in overall architecture of the Internet and the PC, or some unforeseen security breakthrough.

[1] Lawrence Livermore National Laboratory, d_jefferson@yahoo.com. [2] Professor of Computer Science, Johns Hopkins University, rubin@jhu.edu. [3] IBM Research (retired), Former President, Association for Computing Machinery, simons@acm.org.

In fact, no such security breakthrough has occurred, and we remain convinced that there is no way to secure Internet voting. Perhaps that is why the new DoD report resorts in some places to buzzwords instead of substance. For example, the report claims that roaming digital certificates will be used to combat certain threats. While that may sound good to general audiences, the use of such certificates does not address any of the serious problems identified in our SERVE report.

The IVAS system, deployed in 2006, was a modest successor to SERVE. Although it was reviewed favorably in the DoD report, it actually is more insecure than SERVE. IVAS involved email and fax and did not provide any encryption or authentication of ballots. Several parties, including an independent contractor, were in a position to tamper with or destroy ballots before they were received by local election officials. The DoD report cites surveys of local election officials saying that they would use IVAS again. But while such surveys may indicate interest by officials, they say absolutely nothing about whether such a system is actually secure. We believe it is not.

The current Internet and PC architectures are both such highly insecure platforms that it is essentially impossible to develop a secure system for voting in federal elections on them. From time to time some person or company claims to have "solved" the security problems of Internet-based elections. Such solutions typically deal only with some of the easier issues (voter authentication, secure ballot transmission) by using various encryption mechanisms. Invariably, the most difficult vulnerabilities are ignored, defined away, or addressed with ineffective gestures. Such vulnerabilities include insider attacks of various kinds, phishing attacks, DNS attacks, spoofing attacks, viral and backdoor attacks, distributed denial of service attacks, and automated vote buying and selling schemes. The purported mitigations listed on page 12 of the DoD report are examples of ineffective gestures; reading that list makes one wonder if the authors fully understand the gravity and complexity of the security issues.

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. We do not anticipate that the changes in the design of Internet and in PC hardware and software needed to support secure elections will be forthcoming within the foreseeable future, and certainly not within the five year time span contemplated in this report.

In our 2004 report we made the case against the SERVE Internet voting system. However, those arguments actually apply to any Internet voting system, and so we repeat them here (in slightly updated form):

a) Paperless electronic voting systems have been widely criticized elsewhere for various deficiencies and security vulnerabilities: that their software is totally closed and proprietary; that the software undergoes insufficient scrutiny during certification; that they are especially vulnerable to various forms of insider (programmer) attacks; and that they have no voter-verified audit trails (paper or otherwise) that could largely circumvent these problems and improve voter confidence. All of these criticisms apply directly to Internet voting systems as well.

b) In addition, Internet voting systems have numerous other fundamental security problems that generally leave them vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks, etc.), any one of which could be catastrophic.

c) Such attacks could occur on a very large-scale, and could be launched by anyone in the world, from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law. These attacks could result in widespread, selective voter disenfranchisement, and/or privacy violation, and/or vote buying and selling, and/or vote switching, even to the extent of reversing the outcome of many elections at once, including the presidential election. With care in the design, some of the attacks could succeed and yet go completely undetected. Even if detected and neutralized, such attacks could have a devastating effect on public confidence in elections.

d) It is impossible to estimate the probability of a successful cyber-attack (or multiple successful attacks) on any one election. But the attacks we are most concerned about are quite easy to perpetrate. In some cases there are kits readily available on the Internet that could be modified or used directly for attacking an election. And we must consider the obvious fact that a U.S. general election offers one of the most tempting targets for cyber-attack ever, whether the attacker's motive is overtly political or simply self-aggrandizement.

e) The vulnerabilities we describe cannot be fixed by better design of Internet voting software. They are fundamental in the architecture of the Internet and of PCs and their software. They cannot be eliminated for the foreseeable future. It is quite likely that they will never be eliminated without a wholesale redesign and replacement of much of the hardware and software security systems that are part of, or connected to, today's Internet.

f) An Internet voting system might appear to work flawlessly in 2008, or whenever it is first deployed, with no successful attacks detected. Unfortunately, but inevitably, a seemingly successful Internet voting experiment in a U.S. presidential election would be viewed by many as strong evidence that Internet voting can be reliable, robust, and secure. Such reasoning is as fallacious as a claim that our cities are safe from "dirty bomb" attacks because we have been living in cities for a long time and no such attack has ever occurred. Any apparently successful election using Internet voting would encourage expansion of the idea in future elections, as well as the marketing of Internet voting systems to jurisdictions throughout the United States and in other countries.

g) Just because no successful attack is detected does not mean that none has occurred. Unlike military attacks, many cyber attacks, especially if cleverly hidden, would be extremely difficult or impossible to detect, even in cases when they change the outcome of a major election. Furthermore, the lack of a successful attack in one election does not mean that successful attacks would be less likely to happen in the future. Quite the contrary; future attacks would be more likely, both because there is more time to prepare the attack, and because expanded use of Internet voting would make the prize of a successful attack more valuable. In other words, a "successful" trial of Internet voting is the top of a slippery slope toward even more vulnerable systems in the future.

h) We certainly believe that there should be better support for voting for our military and for citizens living overseas. Unfortunately, we are forced to conclude that it would be a very serious mistake to deploy an Internet voting system. Because the danger of successful, large-

> scale attacks is so great, we reluctantly recommend against any Internet voting until both the Internet and the world's home computer infrastructure have been fundamentally redesigned.

Compounding these problems, companies selling Internet voting systems almost invariably claim that the software is proprietary, and refuse to permit examination and evaluation of their systems by independent experts. We fully expect that if this project goes forward, whatever company wins the contract will make exaggerated security claims, as others have in the past, and decline to permit independent experts to attempt to verify those claims and publish the results.

We understand the importance of providing military and overseas U.S. citizens with the best possible access to absentee voting. Many of these people are putting their lives on the line to protect our country, and we support many of the measures in the new DoD report that will make voting easier for them. But, we would do them no favor by providing them with a flagrantly insecure and inauditable method of voting. We believe it would be irresponsible to put our democracy at risk by allowing votes to be transmitted over the wide-open and insecure Internet. (http://www.servesecurityreport.org/SERVE_Jr_v5.3.pdf.)

2. The National Institute of Standards and Technology (NIST) has concluded that the Internet cannot be made secure for voting at this time.

A Threat Analysis on UOCAVA Voting Systems

Andrew Regenscheid and Nelson Hastings

(National Institute of Science and Technology (NIST), NISTIR 7551, December 2008. See pages 39–46 and 68 and 69. http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf)

Excerpt from pages 42, 43:

6.3.4 Electronic Mail

In most instances, voted ballots returned via e-mail would reach election officials nearly instantaneously. Communications could, however, be disrupted by malicious parties. Denial of service attacks are a significant threat to e-mail-based voting systems. Attackers could flood election e-mail servers with large amounts of illegitimate traffic. This could not only prevent voters' e-mails from reaching election officials, but could also make it difficult for officials to distinguish between valid and invalid ballots.

Eavesdropping is a potential threat whenever Internet communications is involved, and particularly with e-mailed communications, which are sent unencrypted. While eavesdropping is not a significant threat for ballot distribution, as that information is generally publically available, voted ballots must remain confidential. Voted ballots show how an individual voted, and may sometimes contain sensitive personal information about the voter. E-mails are significantly easier to intercept and modify in transit than other forms of communication. E-mails travel through telecommunications lines, network equipment and e-mail servers before reaching the intended recipient. Anyone with access to the infrastructure could read or even modify e-mail messages. In particular, e-mail servers often store messages for a short period of time before passing them on to the next server, or the intended recipient. System operators for these servers could intercept or modify e-mailed ballots. It is unlikely that election officials would be able to identify ballots that had been modified in-transit.

Also, e-mailed ballots are at risk before and after they are sent to election officials. Voters' computers could be infected with malicious code capable of disrupting communications with an election official. Very sophisticated attacks may be able to modify digital ballots prior to e-mailing them to election officials. Malicious code would need to spread to a large number of personal computers before it would have a substantial effect on an election. The computer virus may be detected before election day, but there would be no way for election officials to identify affected ballots. Similar malicious code on election computer systems could have the same effect.

E-mail does not provide any guarantee that the intended recipient will receive the message. The e-mail system relies on the DNS system [11] to route e-mails to the proper servers. An attack on DNS servers could route e-mails to an attacking party. This would not only result in voter disenfranchisement, but also the loss of sensitive voter information. This kind of attack would require very sophisticated attackers focusing their efforts on major e-mail service providers. There are no known reports of a similar attack being successfully conducted on e-mail or DNS servers. However, it is important to note that a recent vulnerability was discovered in DNS servers that could have been used to construct a similar attack [13]. DNS servers were quickly patched before any significant attack took place.

Less sophisticated, but equally effective, attacks may attempt to trick voters into sending their ballots to an attacker. That is, an attacker would contact a large number of voters, claiming to be their local election official and attempting to convince them to reply with their cast ballot. While a relatively small number of voters may be fooled, it is relatively easy and cheap to contact a very large numbers of voters.

3. Computer technologists have stated their concerns about Internet voting; the introduction is quoted below.

Computer Technologists' Statement on Internet Voting

www.verifiedvoting.org/article.php?id=5867

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.

Endorsed by the following:

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

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

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

continued on next page

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

David L. Dill
Professor of Computer Science, Stanford Univ. 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 Univ.
http://www.epp.cmu.edu/httpdocs/people/bios/farber.html

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

Michael J. Fischer
Professor of Computer Science, Yale Univ., 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 Univ.
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 Univ.
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, Univ. of Iowa
http://www.cs.uiowa.edu/~jones/vita.html

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

Scott Klemmer
Assistant Professor of Computer Science, Stanford Univ.
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 Univ.
http://cs.stanford.edu/~eroberts/bio.html

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

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

Yoav Shoham
Professor of Computer Science, Stanford Univ.
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 Univ.
http://spaf.cerias.purdue.edu/narrate.html

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

Dan S. Wallach
Associate Professor, Department of Computer Science, Rice Univ.
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 Univ.
http://infolab.stanford.edu/~widom/

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

APPENDIX B

FALSE CLAIMS OF SECURE INTERNET VOTING THROUGH ENCRYPTION

In August 2010, Ronald Rivest, Viterbi Professor of Electrical Engineering and Computer Science at MIT and 2002 winner of the Turing Award—the "Nobel Prize" of computing—explained what encryption can and cannot do:

Encryption, he said, assures that an eavesdropper won't hear what is being sent, that what was sent by a PC is what is received at the other end. It doesn't ensure that what was sent by the PC was what the voter intended.

> "What I'm talking about is not attacks on the communication channel; they are attacks on the platform. The hard part here is the PC the voter is voting on, not the channel; you can use encryption for that. It doesn't protect from viruses and malware. It doesn't protect against malware that has been sent. It doesn't protect against viruses on the recipient election official's machine. Protecting communication channels is where we've made the most progress over the last three decades. We have not made progress with the PC's, such as protecting against insider attacks."

(From a discussion at the "UOCAVA Remote Voting Systems Workshop" in Washington, D.C.)

APPENDIX C

ELECTRONIC TRANSMISSION OF VOTED BALLOTS NOT NECESSARY

The model law for HB11-1219, the Uniform Law Commission's "Uniform Military and Overseas Voters Act", does not incorporate the electronic return of voted ballots for security and privacy reasons. This is justified in its Prefatory Note: "…using electronic transmission methods for just those steps in the absentee voting process prior to the casting of a ballot (such as registering to vote, requesting an absentee ballot, and receiving a blank ballot) can alone dramatically reduce the time required to permit these voters to vote successfully."

APPENDIX D

EXAMPLES OF INTERNET HACKING

1. The Center for Strategic and International Studies (www.csis.org) lists 64 significant hacks between May of 2006 and early January of 2011.
http://csis.org/files/publication/110103_Significant%20Cyber%20Incidents%20Since%202006_0.pdf

2. Assistant Professor J. Alex Halderman, a computer scientist in the Department of Electrical Engineering and Computer Science at the University of Michigan, describes below how he and his team executed the stunning hack of the Washington, D.C., Internet voting pilot project.

http://www.freedom-to-tinker.com/blog/jhalderm/hacking-dc-internet-voting-pilot

Hacking the D.C. Internet Voting Pilot

By J. Alex Halderman - Posted on October 5th, 2010, at 8:07 p.m.

The District of Columbia is conducting a pilot project to allow overseas and military voters to download and return absentee ballots over the Internet. Before opening the system to real voters, D.C. has been holding a test period in which they've invited the public to evaluate the system's security and usability.

This is exactly the kind of open, public testing that many of us in the e-voting security community — including me — have been encouraging vendors and municipalities to conduct. So I was glad to participate, even though the test was launched with only three days' notice. I assembled a team from the University of Michigan, including my PhD students, Eric Wustrow and Scott Wolchok, and Dawn Isabel, a member of the University of Michigan technical staff.

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 ballots. In this post, I'll describe what we did, how we did it, and what it means for Internet voting.

D.C.'s pilot system

The D.C. system is built around an open source server-side application developed in partnership with the TrustTheVote project. Under the hood, it looks like a typical web application. It's written using the popular Ruby on Rails framework and runs on top of the Apache web server and MySQL database.

Absentee overseas voters receive a physical letter in the mail instructing them to visit a D.C. web site, http://www.dcboee.us/DVM/, and log in with a unique 16-character PIN. The system gives voters two options: they can download a PDF ballot and return it by mail, or they can download a PDF ballot, fill it out electronically, and then upload the completed ballot as a PDF file to the server. The server encrypts uploaded ballots and saves them in encrypted form, and, after the election, officials transfer them to a non-networked PC, where they decrypt and print them. The printed ballots are counted using the same procedures used for mail-in paper ballots.

A small vulnerability, big consequences

We found a vulnerability in the way the system processes uploaded ballots. We confirmed the problem using our own test installation of the web application, and found that we could gain the same access privileges as the server application program itself, including read and write access to the encrypted ballots and database.

The problem, which geeks classify as a "shell-injection vulnerability," has to do with the ballot upload procedure. When a voter follows the instructions and uploads a completed ballot as a PDF file, the server saves it as a temporary file and encrypts it using a command-line tool called GnuPG. Internally, the server executes the command gpg with the name of this temporary file as a parameter: gpg [...] /tmp/stream,28957,0.pdf.

We realized that although the server replaces the filename with an automatically generated name ("stream,28957,0" in this example), it keeps whatever file extension the voter provided. Instead of a file ending in ".pdf," we could upload a file with a name that ended in almost any string we wanted, and this string would become part of the command the server executed. By formatting the string in a particular way, we could cause the server to execute commands on our behalf. For example, the filename "ballot.$(sleep 10)pdf" would cause the server to pause for ten seconds (executing the "sleep 10" command) before responding. In effect, this vulnerability allowed us to remotely log in to the server as a privileged user.

Our demonstration attacks

D.C. launched the public testbed server on Tuesday, September 28. On Wednesday afternoon, we began to exploit the problem we found to demonstrate a number of attacks:

- We collected crucial secret data stored on the server, including the database username and password as well as the public key used to encrypt the ballots.
- We modified all the ballots that had already been cast to contain write-in votes for candidates we selected. (Although the system encrypts voted ballots, we simply discarded the encrypted files and replaced them with different ones that we encrypted using the same key.) We also rigged the system to replace future votes in the same way.
- We installed a back door that let us view any ballots that voters cast after our attack. This modification recorded the votes, in unencrypted form, together with the names of the voters who cast them, violating ballot secrecy.
- To show that we had control of the server, we left a "calling card" on the system's confirmation screen, which voters see after voting. After 15 seconds, the page plays the University of Michigan fight song. Here's a demonstration.

Stealthiness wasn't our main objective, and our demonstration had a much greater footprint inside the system than a real attack would need. Nevertheless, we did not immediately announce what we had done, because we wanted to give the administrators an opportunity to exercise their intrusion detection and recovery processes — an essential part of any online voting system. Our attack remained active for two business days, until Friday afternoon, when D.C. officials took down the testbed server after several testers pointed out the fight song.

Based on this experience and other results from the public tests, the D.C. Board of Elections and Ethics has announced that they will not proceed with a live deployment of electronic ballot return at this time, though they plan to continue to develop the system. Voters will still be able to download and print ballots to return by mail, which seems a lot less risky.

D.C. officials brought the testbed server back up today (Tuesday) with the electronic ballot return mechanism disabled. The public test period will continue until Friday, October 8.

What this means for Internet voting

The specific vulnerability that we exploited is simple to fix, but it will be vastly more difficult to make the system secure. We've found a number of other problems in the system, and everything we've seen suggests that the design is brittle: one small mistake can completely compromise its security. I described above how a small error in file-extension handling left the system open to exploitation. If this particular problem had not existed, I'm confident that we would have found another way to attack the system.

None of this will come as a surprise to Internet security experts, who are familiar with the many kinds of attacks that major web sites suffer from on a daily basis. It may someday be possible to build a secure method for submitting ballots over the Internet, but in the meantime, such systems should be presumed to be vulnerable based on the limitations of today's security technology.

We plan to write more about the problems we found and their implications for Internet voting in a forthcoming paper.

3. Just this month, more than one million websites were hacked to change embedded links to lead site visitors to fraudulent sales sites. www.reuters.com/article/2011/04/01/hackers-idUSN0116927520110401

MALICIOUS WEB ATTACK HITS A MILLION SITE ADDRESSES
SEATTLE, April 1 | Fri Apr 1, 2011 5:21pm EDT
(Reuters) - More than one million website addresses have been compromised by a sophisticated hacking attack that injects code into sites that link to a fraudulent software sales operation.

The mass attack has managed to inject malicious code into websites' links by gaining access to the servers running the databases that power the Internet, according to the technology security company that discovered it.

Websense, which first found evidence of the attack earlier this week, has called it 'LizaMoon,' after the name of the site the malicious code first directed its researchers to.

On that site and others, users are shown a warning from 'Windows Stability Center' -- posing as a Microsoft Corp (MSFT.O) security product -- that there are problems with their computer and are urged to pay for software to fix it.

Microsoft has no product of that name. The company did not immediately have a comment on the attack.

Websense said some Web addresses related to Apple Inc's (AAPL.O) iTunes service were compromised. Apple did not immediately respond to a request for comment. (Reporting by Bill Rigby; editing by Andre Grenon)

APPENDIX E

AMENDMENT #1: CHANGES TO TEXT OF RE-ENGROSSED VERSION

1. DELETIONS (See ~~strikethrough~~):

Page 11, line 4, **1-8.3-111**. **Timely casting of ballot.** TO BE VALID, A BALLOT SHALL BE RECEIVED BY THE APPROPRIATE LOCAL ELECTION OFFICIAL NOT LATER THAN THE CLOSE OF THE POLLS, OR THE VOTER SHALL SUBMIT THE BALLOT FOR MAILING, ~~ELECTRONIC SUBMISSION,~~ OR OTHER AUTHORIZED MEANS OF DELIVERY NOT LATER THAN 7:00 P.M. MOUNTAIN TIME ON THE DATE OF THE ELECTION.

Page 11, lines 20-24. ~~**1-8.3-113. Transmission and receipt of ballot.** (1) A COVERED VOTER WHO REQUESTED AND RECEIVED BALLOT MATERIALS BY ELECTRONIC TRANSMISSION MAY ALSO RETURN THE BALLOT BY ELECTRONIC TRANSMISSION, AS SPECIFIED IN RULES PROMULGATED BY THE SECRETARY OF STATE.~~

2. ADDITIONS (See DOUBLE-UNDERLINED, ALL-CAPITAL TEXT*):*

Page 11, **1-8.3-113. Transmission and receipt of ballot.** COVERED VOTERS ARE PROHIBITED FROM RETURNING THEIR VOTED BALLOTS BY ELECTRONIC TRANSMISSION (INCLUDING FACSIMILE WHETHER VIA FAX MACHINE OR COMPUTER), AS THIS TRANSMISSION METHOD JEOPARDIZES ELECTION SECURITY AND VOTER PRIVACY.

AMENDMENT #2: CHANGES TO TEXT MUST REFLECT PREVIOUS DRAFT OF UMOVA MODEL LEGISLATION, AS PER MEMO FROM NATIONAL ASSOCIATION OF STATE ELECTION DIRECTORS (NASED).

To make this amendment, re-introduce “absent” to precede all references to “uniformed service voter” as they existed in the Uniform Law Commission's bill draft of October 2009. See Sections 2, 4, 6, and 9 through 18.