



February 15, 2009

Representative Nancy Todd, Chair, and Members of the
 State, Veterans, and Military Affairs Committee
 Colorado House of Representatives, General Assembly
 200 East Colfax Avenue
 Denver, Colorado 80203

Dear Chair Todd and Members of the State, Veterans, and Military Affairs Committee:

We wish to share with you some very important information on Internet voting, in preparation for your consideration of HB09-1205, "Concerning Voting by Members of the Armed Forces Serving Outside the United States."

Please click on www.servesecurityreport.org for the very readable three-and-a-half pages titled "A comment on the May 2007 DoD report on Voting Technologies for UOCAVA Citizens," by David Jefferson, Avi Rubin, and Barbara Simons, three outstanding computer security scientists. To quote two sentences: "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." But please take a couple of minutes to read the rest.

You will not find this paper quoted by the Department of Defense (DoD) or whoever else is behind the proposal for a "pilot project of Internet voting" as put forth in HB09-1205.

The December 2008 National Institute of Standards and Technology (NIST) report ("A Threat Analysis on UOCAVA Voting Systems," <http://vote.nist.gov/uocava-threatanalysis-final.pdf>), requested by the Election Assistance Commission, likewise advises against returning voted ballots over the Internet: "However, at this time there is no practical way to protect the integrity or confidentiality of emails from voters. Thus returned ballots would be at risk for eavesdropping and modification" (from "A Threat Analysis...", p. 61). To read about specific threats possible against Internet voting, see pages 42-46. To see the formidable list of measures that one would take to *try* to protect Internet voting, see pages 58-66.

The pilot project proposed in HB09-1205 will, if approved, be a waste of time and money; and even if it were not our money (to begin with), **the project, by operating during a real election, could jeopardize the accuracy of election results.** If Colorado were to attempt

to provide the impossible, i.e., sufficient security for Internet voting, this would ultimately involve more expense and trouble than it was worth—except, of course, for vendors making the profits and for anyone with an incentive to undermine our democratic voting system with false results.

The concerted push for overseas Internet voting on the part of the DoD and vendors reminds us of the push for un-auditable DREs, a debacle with many serious and unfortunate consequences for our elections. Like DREs without VVPATS, Internet voting is un-auditable and intrinsically subject to rigging. Will we get fooled twice?

Thank you for your attention to this matter, and for all your hard work for Colorado.

Sincerely,

The Board of Directors, Coloradans for Voting Integrity

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

David Jefferson¹, Avi Rubin², Barbara Simons³

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.

the weekly
Standard

Disenfranchised Over There

Let's defend the voting rights of those who defend us.

by Hans A. von Spakovsky & Roman Buhler

05/12/2008, Volume 013, Issue 33

Over the past 40 years, starting with the historic Voting Rights Act of 1965, Congress has sought to guarantee the right of every American citizen to vote. But there is still a large and significant group of Americans who are needlessly disenfranchised: the millions of men and women who serve abroad in our armed forces.

A survey by the Election Assistance Commission shows that of almost 1 million ballots requested in the last election by overseas and military voters, only about one third were successfully cast and counted. The most common reasons for this failure were that the requested ballots sent to voters were returned as "undeliverable" and that marked ballots were received too late to be counted.

Military personnel based outside the United States are still dependent on the mail to receive and cast their ballots. When an election official sends a ballot overseas, it can take three weeks (or more) to reach a soldier in Iraq or a sailor on a ship halfway around the world. Even if the soldier or sailor completes the ballot immediately, it may take another three weeks to get back. Many ballots simply do not get home in time.

The Pentagon spent millions on a high-tech solution that transmitted ballots over the Internet, but abandoned the effort because of serious security risks. Some states now allow completed ballots to be faxed to election officials from overseas voters, but many soldiers in the field don't have access to fax machines, and faxing ballots imperils the secrecy of the vote. Some states also allow ballots postmarked overseas before the date of the election to be received, unlike all other ballots, after the close of polls. Unfortunately, given the unreliability of some overseas postal authorities, this poses significant risk of fraudulently postmarked ballots, especially in a very close election.

Republican congressman Kevin McCarthy has just introduced the Military Voting Protection Act, which would require the Pentagon to collect absentee ballots overseas and deliver them stateside by express air transport. This could shorten the delivery time for overseas ballots from three weeks to only four days. It would mean that many thousands of ballots that were rejected in 2004 would count in 2008.

A more comprehensive solution, though, could be crafted from the historical example of the first absentee ballots cast by American soldiers. The election of 1864 was held in the middle of a civil war when large numbers of voters were fighting in the field. Wisconsin decided to allow its soldiers to vote absentee, and other states quickly followed suit. Rather than a slow and cumbersome ballot-by-mail process, the states simply set up polling sites in the field encampments of their soldiers. This was easier to do in 1864 when soldiers in many military units came from only one state or community. But modern technology should be able to overcome any obstacles today.

Imagine a system where Congress and the states coordinated an effort to set up early voting sites at or near military installations all over the world. Once a voter provides proper identification that matches his

or her name on the voter registration lists each state is required to maintain by the Help America Vote Act of 2002, an electronically uploaded ballot provided by that state could be printed out for the soldier. The ballots completed at each overseas early voting site could then be sent back to the appropriate election officials in the United States through express mail.

Except in extraordinary circumstances such as special forces teams in the field or sailors on ships far out at sea, ballots completed by the Friday before the election could be in the hands of local election officials by the close of polling on Election Day. Early voting sites and an express mail delivery system would enfranchise hundreds of thousands of military voters who today never get their vote counted.

And while establishing overseas early voting sites would take time, a system for express delivery of completed ballots from military bases and U.S. consulates could be implemented in 2008, if Congress and the president worked together. Surely, improving the voting rights of our men and women in uniform is a strong enough motivation.

Dwight Eisenhower, a general who went on to become president, once said that "the future of this republic is in the hands of the American voter." Those hands should include all of those who protect and defend this nation and fight to keep it free.

Hans A. von Spakovsky is a former commissioner on the Federal Election Commission. Roman Buhler is a former elections counsel for the House Administration Committee.