Internet Voting

Author : verifiedvoting

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. 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

US Vote Foundation: The Future of Voting: End-to-End Verifiable Internet Voting (2015)

Utah iVote Internet Voting Report (2015)

Online Voting: Rewards and Risks (Intel Security, 2014)

Developing a Framework to Improve Critical Infrastructure Cybersecurity (Verified Voting Public Commentary, 2013)

ACM: Internet Voting in the United States (2012)

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

What About Email and Fax?

Report on Internet Voting in Estonia (2011)

ACM Brief: Internet Voting and Uniformed and Overseas Citizens absentee Voters

Despite that, as states provide electronic delivery of blank ballots, some are using the Internet for return of voted ballots via email attachments, by digital fax or through a web portal. 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.

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.

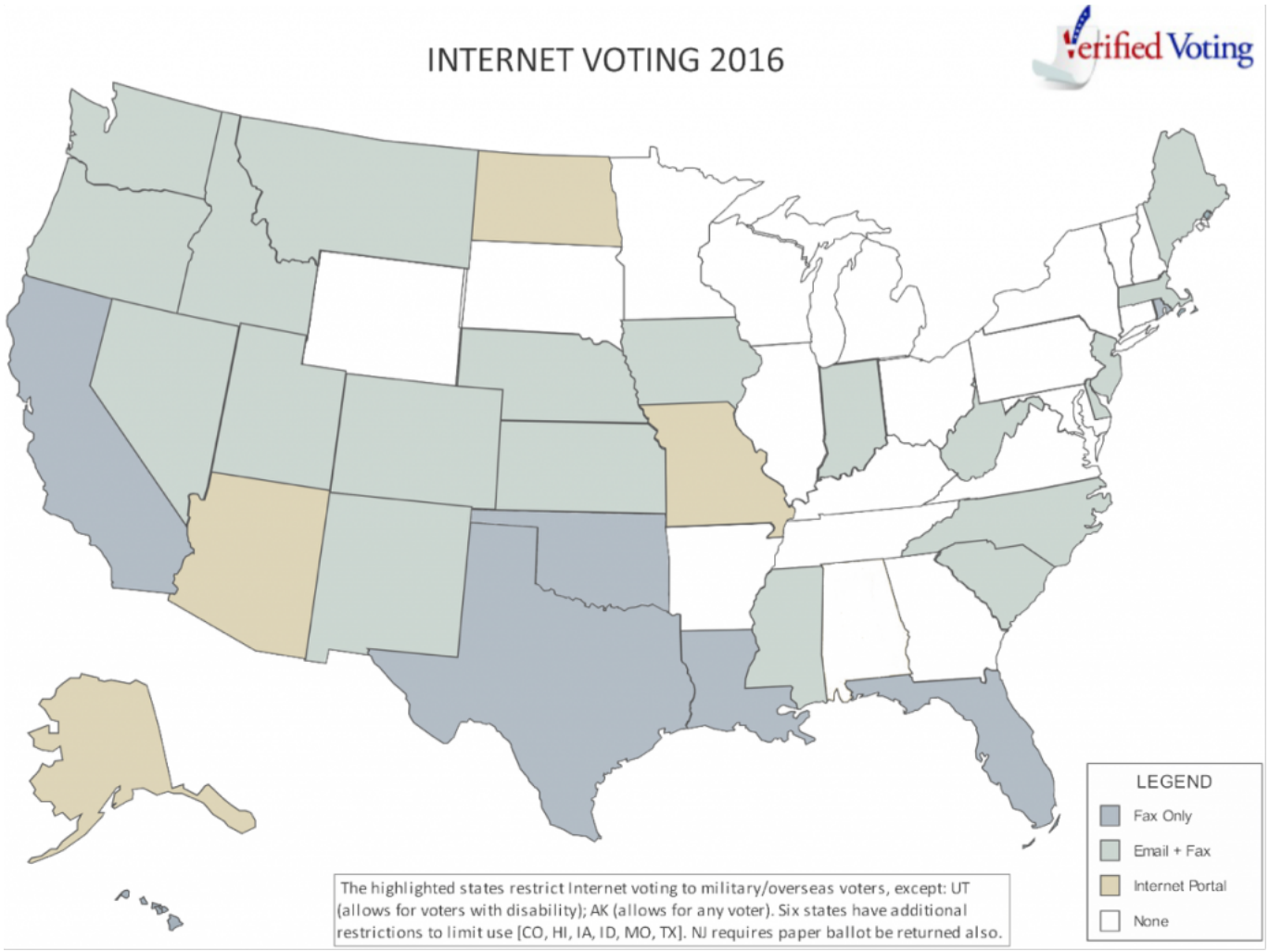
There is no way to guarantee that the security, privacy, and transparency requirements for elections can all be met with any practical technology in the foreseeable future. Anyone from a disaffected misfit individual to a national intelligence agency can remotely attack an online election, modifying 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, 31 states and the District of Columbia 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 the polls and 10 more provide them for voters in at least some counties also apply, with even greater urgency, to voted ballots returned electronically from outside the country. You can view the specific provisions for the electronic submission of voted ballots in each of the States at the right of this page.

Federal Efforts to Secure Online Voting for the Military

Researchers for the federal government have spent a decade and a half and over 100 million dollars to study online voting[1] and have attempted to conduct pilot projects, and concluded that it is currently not possible to ensure the security, privacy, auditability and integrity of ballots cast over the Internet.[2] For this reason, the U.S. Election Assistance Commission did not set security standards or guidelines for an Internet voting pilot project to be carried out by the Department of Defense (DoD) for military and overseas voters. There are no federal security guidelines because the federal government concluded online voting cannot be done securely.[3] Moreover, because federal researchers determined that secure online voting is not currently feasible, the DoD did not develop an online voting system for military voters. The conclusive evidence that online voting cannot yet be done securely led the federal government to abandon its effort to develop a secure online voting system for the military in 2014.[4]

Back in 2002 congress directed the DoD to develop an online voting demonstration project for the troops in the National Defense Authorization Act (NDAA). DoD developed the SERVE project, an online voting system slated to be deployed for the 2004 elections. After security researchers reviewed the system and warned that it was not secure, the deputy secretary of defense cancelled the SERVE project because DoD "could not ensure the legitimacy of ballots" cast through the SERVE system.[5] In response, congress amended the NDAA directive in 2005 and directed the U.S. Election Assistance Commission and the National Institute of Standards and Technology (NIST) to study the online return of voted ballots for the purpose of setting security standards so the Department of Defense may use them for the creation of a secure online voting system for military voters. NIST has documented several security issues that cannot be mitigated or solved with the cyber security safeguards and voting system protocols currently available. **Federal researchers concluded its research found that until these challenges are overcome, secure Internet voting is not yet feasible**.[6]

The overwhelming evidence that secure Internet voting *still* is not within our grasp led Congress to repeal that directive to the Department of Defense to pursue online voting for military and overseas voters in the 2015 National Defense Authorization Act. The question of how to develop a secure online voting system has been asked and answered by researchers at the federal government. Secure online voting is not yet achievable. Vendors of online voting systems may claim that their systems are secure but these security claims are backed solely by the vendors' promises and are completely unsubstantiated. ***Any claim by a for-profit vendor that it has developed a secure Internet voting system is in direct contradiction to the best assessment of federal researchers after years of research and analysis.***

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” even though the federal government chose not to pursue online ballot return because of the security risks. 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)