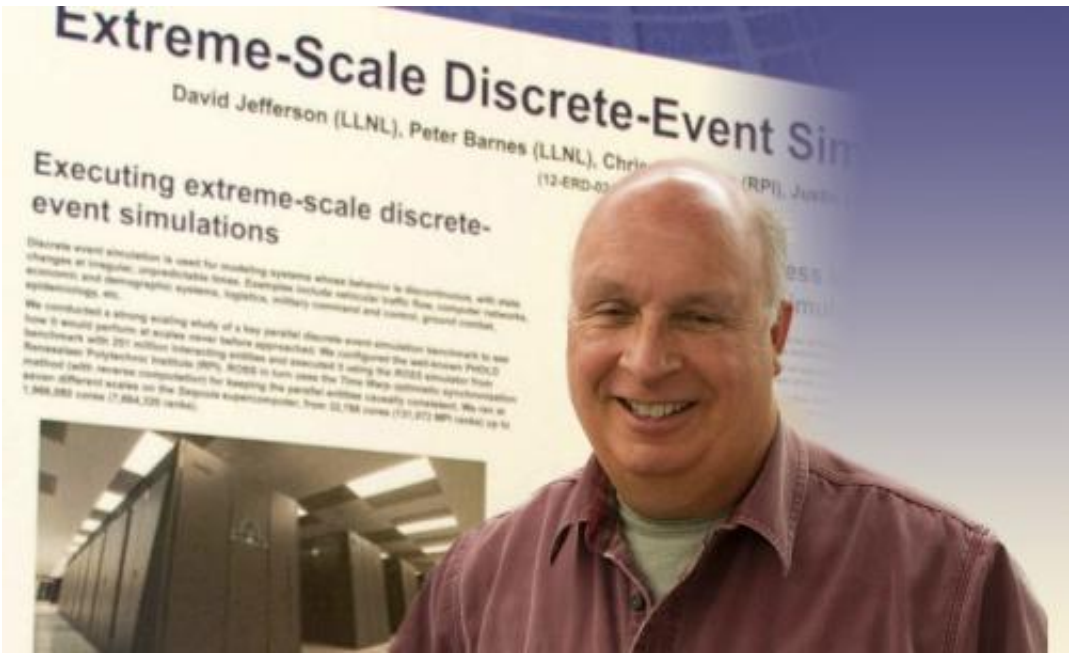
Security risks and privacy issues are too great for moving the ballot box to the Internet

March 11 2015



Lawrence Livermore computer scientist David Jefferson discussed his findings in a recent Computation Seminar Series presentation entitled “Intractable Security Risks of Internet Voting.” His study of Internet voting issues is independent of his Lawrence Livermore research work. Credit: Julie Russell/LLNL

Contrary to popular belief, the fundamental security risks and privacy problems of Internet voting are too great to allow it to be used for public

elections, and those problems will not be resolved any time soon, according to David Jefferson, who has studied the issue for more than 15 years.

Jefferson, a computer scientist in the Lawrence Livermore's Center for Applied Scientific Computing, discussed his findings in a recent Computation Seminar Series presentation, entitled "Intractable Security Risks of Internet Voting." His study of Internet voting issues is independent of his Lawrence Livermore research work.

Nonetheless, he reminded the audience that "election security is a part of national security," noting that this is a primary reason he is so passionate about this issue. "I am both a technical expert on this subject and an activist," Jefferson emphasized in his introductory remarks. "Election security is an aspect of national security and must be treated as such."

The view held by many election officials, legislators and members of the public is that if people can shop and bank online in relative security, there's no reason they shouldn't be able to vote on the Internet, Jefferson said. "Advocates argue (falsely) that Internet voting will increase turnout, reduce costs and improve speed and accuracy." They promote the idea that "you can vote anytime, anywhere, even in your pajamas."

Other benefits touted by advocates are simpler voting for military personnel, overseas voters, students and others away from home on election day, better access for some disabled voters, and various technical advantages of getting rid of paper ballots.

However, Jefferson says the security, privacy, reliability, availability and authentication requirements for Internet voting are very different from, and far more demanding than, those required for e-commerce, and cannot be satisfied by any Internet voting system available today or in the foreseeable future. Such systems are susceptible to "attack" or

manipulation by anyone with access to the system, including programmers and IT personnel, not to mention criminal syndicates and even nation states, according to Jefferson.

Yet, 33 U.S. states allow or have experimented with some form of online voting, he said. In most cases it is email voting, in which the voter's ballot, ID and legal affirmation are transmitted as attachments to an email message. While email voting is legal in many places, Web-based voting is the growing trend in most places.

Jefferson says all email voting systems are vulnerable to attack because ordinary email headers are completely forgeable, email uses no end-to-end encryption and email does not offer a reliable way to authenticate or verify a voter's identity. It also is subject to unpredictable delay, employing only a "best efforts" delivery system. Worst of all, email ballots can be modified surreptitiously in transit by any IT person who controls either an email relay or router in the path the email takes, or the final email server. Moreover, email can be manipulated by anyone in the world who can remotely compromise one of those systems, and such attacks are essentially undetectable and uncorrectable. Sending secure documents like ballots by email "would be like stapling a $100 bill to a postcard and expecting it to get to its destination unmolested." In addition, specially constructed PDF document attachments can inject malware into the receiving vote server, Jefferson said, concluding that "email voting is the worst voting system ever invented."

Newer Internet voting architectures are Web-based systems in which voting transactions superficially resemble ecommerce transactions. While better than email voting, Web-based systems are still riddled with intractable security problems, including client-side malware attacks, server-side penetration attacks, denial of service attacks, voter authentication attacks and network attacks of various kinds. Third-party vendors of such systems, unsurprisingly, deny or downplay any security

risks to the system, he said.

He notes that online shopping requires no strong authentication or verification of eligibility, only demonstration of the ability to pay. Criminals, foreign nationals, minors, or almost anyone are free to shop online. Proxy shopping transactions on behalf of someone else are perfectly legal, Jefferson said, whereas proxy voting definitely is not. Another requirement that sets voting systems apart from online shopping and banking is the need for "a system to be transparent while still protecting the secrecy of who cast which ballot." There is no comparable requirement for e-commerce. With online shopping, errors and fraud will eventually be detected and can usually be corrected later, but because of the secret ballot requirement voting transactions must be recorded accurately the first time since vote manipulation is not generally detectable or correctable. "Also, financial losses in e-commerce can be insured or absorbed, but no such amelioration is possible in an election," he said. "And of course, the stakes are generally much higher in a public election than in an e-commerce system."

At this time, there is not a reliable way to detect fraudulently modified vote transactions, Jefferson said. "Internet elections are essentially impossible to audit and there's no meaningful way to recount because there are no original indelible records of the voters' intent against which to compare the outcome. The only vote records are on the server, and they are highly processed electronic ballot images that have been operated on by millions of lines of code on the client device, during transit through the Internet and on the server and canvass systems."

Cyber security experts have demonstrated the vulnerability of both email and Web-based systems to penetration attacks on servers, Jefferson said. In one notorious case voting security expert J. Alex Halderman, a professor of electrical engineering and computer science at the University of Michigan, was able to hack into Washington, D.C.'s pilot

Internet voting system in 2010 and completely compromise it, even though officials expected attacks because it was an open test and they had invited anyone to probe its security defenses.

"We have no way in general of protecting systems from server attacks. It's a bad situation," Jefferson said. Not only can cyber criminals attack vendor networks and servers, they can attack voter clients' systems as well, he said.

The most sophisticated Internet voting systems to date, which are still subjects of research and not ready for deployment, use what are known as end-to-end auditable cryptographic protocols. These protocol use advanced cryptographic methods to offer some protection of vote privacy, prevent undetected loss of votes, prevent undetected changes in votes, prevent forged votes, prevent miscounting of votes, allow voters to verify that their vote is included in the count and allow anyone to verify that these properties hold for an entire election. Yet these end-to-end cryptographic systems also have their weaknesses, including the inability to address remote voter authentication and client side malware or to prevent denial of service attacks. They also do not totally protect vote privacy or prevent automated vote selling, Jefferson said. "In addition, no one but cryptographers understands how these systems work, and that's a problem for maintaining voter trust in a democracy."

Web-based has been used on several occasions in some U.S. states since 2000 and has expanded with the encouragement of organizations such as the DoD Federal Voting Assistance Program (FVAP), which spent $60 million since 2008 alone to develop and promote online voting.

Despite the concerns of security experts, the global tide appears to be moving in favor of Internet voting. Jefferson said critics of Internet voting are in a "David and Goliath" battle with well-organized groups of election officials, advocates for the military and disabled and well-

financed vendors selling online voting systems. "Much more money is being pumped into deploying Internet voting systems than into basic research on more secure voting systems."

Advocates point to the country of Estonia, which has committed to Internet voting for all elections, though Jefferson said that system was recently severely criticized in a study conducted by Halderman and several colleagues. Other countries that have experimented with Internet voting include Australia, Canada, Ecuador, Finland, India, Norway, Philippines, Spain, Switzerland and the United Kingdom. Support for Internet voting, however, is not universal. Germany and the Netherlands have made Internet voting illegal because of the security concerns, and there is at least widespread awareness of the security concerns even though there also is a lot of denial.

In the U.S., "the line of defense against Internet voting is thin" and is led by groups such as Verified Voting, Common Cause and scattered other "advocacy groups with shallow pockets" around the country.

Too many unresolved security problems with Internet voting remain to endorse its use, Jefferson said. "Internet voting is a serious threat to national security. Neither the U.S. nor any other democratic country should open the door to Internet voting—not now, and not in the foreseeable future—until such distant time as all of the fundamental security problems are satisfactorily resolved."

Provided by Lawrence Livermore National Laboratory