Internet Voting: The National Security Risks

By Jim Soper[1] April 14, 2013

The main reasons why Internet voting is not ready for use in government elections are: 1) it is not safe; 2) it will not be safe any time soon; 3) even if it were "safe", it is not transparent; we cannot know what is really going on inside the machines, and should not trust the results; and 4) being paperless, we cannot independently check or recount the results, so there is no way to prove to the losers that they lost, nor to recover from the inevitable cyber-meltdown. Internet voting constitutes a real threat to how we form our government, and as such, should be treated as a serious national security risk.

Paperless electronic voting is fundamentally risky

- Even current voting systems are riddled with bugs and security problems.[2]
- Because computers are extremely complex, even with open source software, we do not and cannot know what is going on inside the machines. Keep in mind that:
    - The most pernicious vulnerability comes from the people that build or control the systems that collect and count the votes. Vendors program and install them. Thousands of election officials have insider access to them. Microsoft Windows, its frequent "updates", as well as the Chinese chips, motherboards and computers used in elections are never checked nor certified.
    - Extremely complex systems are vulnerable to both undetected hacks and bugs.
- Paperless voting systems offer no way to audit or recount the results, nor to recover when disaster hits. [3]

Paperless electronic voting on the Internet is reckless

- Voters' computers, be they microcomputers or cell phones, are not secure:
    - They are the targets of all kinds of viruses pretending to be, for example, bank or credit card websites. The Zeus virus is a very good example. [4]
    - The Android has become by far the most popular smart phone platform. "*In 2012, we identified more than 35,000 malicious Android programs, which is about six times more than in 2011*". [5]
- The most secure systems at Google, Adobe, Symantec, Yahoo, Juniper Networks, Charles Schwab, Visa, MasterCard have all been penetrated [6], as well as Nasdaq, the CIA, FBI, Pentagon. Interpol and NATO.[7]
- 3000+ county election offices, understaffed and underfinanced, do not have anywhere near these kinds of resources to protect county election computers from the Internet.
- In late September, 2010, Washington D.C. started a test of an Internet voting system. It took University of Michigan "wolverines" less than 36 hours to take complete control of everything - ballots, encryption codes, passwords, voter records, emails, the tabulator, network - everything.[8] This was a "hardened", encrypted system put together by very competent, professional staff. It still failed miserably.
- There is no known way to protect against massive denial of service attacks which can overwhelm central election computers on election day with trillions of requests. This is what happened in Canada in 2012.[9]
- We have no way to ensure that an electronic ballot was actually filled out by the intended voter.
- Internet voting would make both voter coercion and vote buying much easier.
- Keep in mind a worst case scenario: computer attacks in Los Angeles, New York, Miami, Philadelphia, Cleveland, Chicago and Dallas, with results completely flipped. Entire large states voting for the wrong party, and no way to correct it, because there is no paper.

Internet voting will not be secure for at least a decade, probably several, if ever.

- The Internet was not designed with security in mind. This is a permanent and fundamental weakness.

- To paraphrase Dr. David Jefferson, solutions to many of these problems are "*not even on the horizon*". [10]
- "*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*." - (NIST) [11]

Even if "secure", Internet voting is not transparent

- We cannot know what is going on inside. Most systems are private, therefore closed. In any case, they are far too complex to be able to check thoroughly, and incomprehensible to the general voting public.
- Being paperless, there is no way to check the results, nor to recover when things go wrong, and they will.

Computer Technologists' Statement on Internet Voting [12]

"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..."

... "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."

PS: Voting online is not the same as banking online

- Banking online is not "safe". It's insured. Banks lose billions of dollars every year to cyberattacks. They prefer to cover their losses rather than tell the public about it. [13]
- Voting online is less "safe", because your vote is secret. There is no receipt, no transaction number. Being secret, it's impossible to check, trace, correct or "refund".
- Ecommerce requires just an account number. Voting requires an exact identity check, harder to establish.
- A lone ecommerce attack might gain a few hundred thousand dollars. The potential gains for an election attack can be in the many billions of dollars, or control of Congress and/or the White House. The stakes are much higher with elections. This is about protecting our government, a national security issue.
- For a longer analysis, see "If I can shop and bank online, why can't I vote online?", http://electionlawblog.org/wp-content/uploads/jefferson-onlinevoting.pdf

PPS: Estonia's 2011 parliamentary election marred by e-voting results

- In 2011, Estonia's Center party won a plurality of the votes on paper, with 27.68%. But the secretive computers claimed they won less than 10% of the online votes, thereby throwing control of parliament to the Reform party.[14] With some justification, the Center party feels this election was rigged. There is no way to prove to the losers they lost because online votes are paperless. You cannot recount them.
- By the way, the Internet data was destroyed on April 11, 2011, because they admit it can be hacked.[15]

(1) Jim Soper is a former Senior Software Consultant in Artificial Intelligence. He currently teaches programmers how to write apps for websites, smart phones and tablets. He is also the author of CountedAsCast.com
(2) California Top To Bottom Voting Systems Review, http://www.countedascast.com/california/toptobottomreview.php
(3) Florida 'Missing' 18,000 E-Votes in Close Race, http://www.pcworld.com/article/127838/article.html
(4) Zeus (Trojan horse) http://en.wikipedia.org/wiki/Zeu_s_%28Trojan_horse%29
(5) 10 security stories that shaped 2012: The explosion of Android threats, http://www.zdnet.com/10-security-stories-that-shaped-2012-7000008576/
(6) Internet Voting in the U.S., http://cacm.acm.org/magazines/2012/10/155536-internet-voting-in-the-us/fulltext
(7) See the "Attacks" section of http://countedascast.org/internet-voting-reading-list/
(8) Hacking the D.C. Internet Voting Pilot, https://freedom-to-tinker.com/blog/jhalderm/hacking-dc-internet-voting-pilot/
(9) Internet Voting in the U.S., http://cacm.acm.org/magazines/2012/10/155536-internet-voting-in-the-us/fulltext
(10) Dr.Jefferson is a cybersecurity expert for Lawrence Livermore National Laboratory. These remarks are from a presentation made August 10, 2010, at a UOCAVA Workshop in Washington.
(11) Security Considerations for Remote Electronic UOCAVA Voting, http://www.nist.gov/itl/vote/upload/NISTIR-7770-feb2011-2.pdf
(12) http://www.verifiedvoting.org/wp-content/uploads/downloads/InternetVotingStatement.pdf
(13) http://www.mcafee.com/us/resources/reports/rp-financial-fraud-int-banking.pdf
(14) http://countedascast.files.wordpress.com/2013/04/estonian-parliamentary-election-2011.xls
(15) http://www.osce.org/odihr/77557, pg 12.:

> *"In Estonia, the data and the internet voting equipment need to be destroyed in order to preserve the secrecy of the vote in view of the ever-increasing computing powers available for a trialand-error decryption. Most important parts of the Internet voting system31 were destroyed on 11 April in the presence of the NEC members, the auditor and observers."*

This document and much more information is available at http://countedascast.org/internet-voting-risks/