

Comments—NBP Public Notice #20

RE: GN Docket Nos. 09-47, 09-51, and 09-137.

I would like to comment on Internet elections. I am a senior software consultant, and the author of CountedAsCast.com.

I initially wrote these comments in 2008 to a ministry of the German government that was implementing a pilot project for Internet voting. Within a few months, they decided not to proceed with the pilot project as scheduled. Then, on March 3, of 2008, the German Constitutional Court banned any voting system that could not be retraced by citizens without technical knowledge, including Internet voting.

Much of what I have to say is stated in the SERVE report (www.ServeSecurityReport.org). I agree with that assessment and I will add some thoughts.

Please note that in the interest of time I am not going to add many references to statements made here. If there is a need for explanations, I will be glad to provide them.

BASIC CONCEPTS

Let's start with some important concepts.

- A democratic election requires that all phases of the election are open to observation by the public. Nobody, and no machine, should be collecting and counting votes in secret.
- A basic principle of (computer) security is : trust nobody.
- Computer security experts say that the greatest threat comes from insiders.
- Since all data, software and firmware can also be manipulated or erased electronically, including the program that does the manipulating, we cannot trust an all-electronic system. It can erase all evidence of whatever it's done.
- A “voter-verified [paper] audit trail ... is the only readily available effective defense against programmed insider attacks.” [SECURE report, section 1.6, pg 9]
- Since no system will every be 100% secure, we need as many layers of protection as possible, including timely auditing before announcing the final results.
- No amount of testing will ever discover a Trojan horse hidden in software. You have to know how to activate the hidden code, in order to detect it.
- Experiments have shown that a well hidden Trojan horse can be extremely

difficult to find, even if programmers have access to source code.

- The Internet was not built with security in mind, and home PCs very vulnerable. Both are very vulnerable to many kinds of attacks that are not possible on dedicated voting systems.
- Apparently successful elections do not guarantee that future ones will be secure.
- New systems have problems the first few times they are used on a large scale.

UNITED STATES

The security principle that holds here is : trust nobody. There are good reasons for this.

- Stealing votes has existed in the US since at least the 1800's. Some examples are massive vote buying in the late 1800's in the big cities in the East, and preventing blacks from voting in the South. There is clear evidence that at least votes if not entire elections were stolen in Florida in 2000, and in Ohio in 2004.
- The voting machine companies have often been controlled by people who have a biased interest in the outcome of elections, be it Senator Chuck Hagel (ES&S), partisan supporters of a specific candidate (Wally O'Dell, republican CEO of Diebold), and perhaps left- or right-wing Venezuelans (Sequoia).
- The three owners of the company that was bought by Diebold, Global Election Systems, were convicted of stock fraud on the Toronto stock market. They hired a convicted cocaine trafficker, John Elder, to help build a voting system. He hired Jeffery Dean, who had 23 convictions for embezzlement. Some of Mr. Dean's computer code is still in the Diebold machines that we vote on today.
- All four vendors selling voting systems in California have at one point or another, misled government officials and the general public about their systems.

The conclusion here is that we cannot blindly trust the software in the machines.

It has become clear over the past few years that voting systems do fail. Sometimes votes disappear, or the totals are wrong or the voters cannot vote. This is either because of bugs or human error or because of internal or external attacks. The conclusion is that we must have paper ballots in order to check what happened. As a response, more and more states such as California, Florida, Ohio, and New Mexico have been discarding their expensive, all-electronic, paperless systems and moving to simpler systems using paper ballots.

ALL-ELECTRONIC, SECRETIVE ELECTION SYSTEMS

When you have an all-electronic election system, run by the very for-profit company who built the system, you are asking for serious trouble. Probably not in little elections, and maybe not even in the first decade with national elections, but at some point, somebody is going to take advantage of the fact that it is very possible for a few people to steal votes in a very important election, and not leave a trace of evidence. With an all-electronic system, seats of power in government can be stolen, and nobody would know it, nor be able to do anything about it, because all of the evidence can be erased.

Currently Congress and various governmental agencies are considering putting its trust in election systems running on secret software built by for-profit companies. Those companies might or might not have a financial interest in results of local elections. However, a for-profit company will certainly have an interest in the results of future national elections. This raises the risks. Even if the company itself is not involved, a few rogue employees at some future date could take control of local or national politics. A mistake now can be disastrous.

All data, software, and firmware can be manipulated. People may be happy banking online. But banking transactions are not anonymous, they leave a trail. Votes are anonymous and untraceable. That makes a big difference.

I worry most about insider attacks, especially on the vulnerable central databases. This is the easiest way to steal votes. But difficulty would not prevent skilled hackers from penetrating the system from the outside if the stakes were high enough. This is especially true with Internet voting.

INTERNET VOTING

We are having great difficulty in the United States protecting dedicated voting machines with physical chain-of-custody procedures of the type that banks might use, and with election workers watching the machines at all times. Internet voting is worse.

What the SERVE report points out (page 32) is that Internet itself is not highly secure. Also, votes would be cast from vulnerable PCs owned by naïve users, cybercafes, employers, and other places where unobserved hackers would have all the time they need to figure out how to break into the system and manipulate votes. These skilled hackers, by the way, may be in the former Soviet Union, the Middle East, or other parts of the Third World - out of the reach of the rule law. They may even work for clandestine parts of any government or organization that finds it useful to rig elections.

“The troubles with SERVE derive from three fundamental design choices: It uses the Internet heavily, with all of the vulnerabilities that implies (e.g., denial of service, spoofing, phishing, and man-in-the-middle attacks). It relies on voters using private, unsecured PCs with proprietary, commercial software configured to accept mobile code, with all of the vulnerabilities that implies (e.g., virus attacks, various kinds of privacy violations). And SERVE itself is proprietary software, with all of the

vulnerabilities that implies (e.g., security holes, bugs, insider fraud)”
[SERVE report, pg. 28]

OTHER CONCERNS

- In the United States, we may be using private, secretive software, but it is government employees and citizen volunteers that conduct our elections. When company employees are both programming and running the machines, it increases the risk of vote fraud.
- We need to be very careful that proposals for new Internet voting laws are written by experts independent of the company that is creating the software. The software must not be allowed to define the law. The 2002 HAVA law was essentially written by company lobbyists, and it is terrible.
- Engineers are usually optimistic about their work. As with any new system, there can be problems with the system crashing under stress from millions of users, or from denial of service attacks. What is the backup plan if there is a meltdown such as those we have seen in the United States? How do you recover if votes are lost, or there are too many, or people are not allowed to vote?
- While vote-by-mail has serious problems, the SERVE report points out that with Internet voting, the problems of vote selling, intimidation, advertising, deception, identification theft, and double-voting can become automated on a large scale, and it can be done targeting certain classes of voters. [SERVE, pages 8-12]
- Much of the “testing” conducted on the machines in the US was a proven sham. Care must be taken that testing of Internet systems is independent and thorough.

RECOMMENDATIONS

I would like to make the following recommendations as to how to proceed. We start with the assumption that the system is programmed by embezzlers, and act accordingly. This is what good banks do.

- We must conduct a complete technical review of any proposed voting system, as has been done in California, Ohio, Maryland, and elsewhere. The review would be conducted by independent technical experts, and include a review of the source code, and penetration testing.
- Because bugs and hidden code can be extremely difficult for a small team of people to find, the source code must be disclosed to the public - on the Internet. We must also have the assurance that the disclosed source is indeed the source code that is running on the machines. Disclosed/open source follows the principle

that all aspects of an election must be open to public inspection. A company that chooses to hide its trade secrets should not be involved in a public election.

- Because all electronic data, software and firmware can be manipulated, at least by insiders, there must be a way to include a secure paper audit trail in the system. This is what the SERVE report states, and I agree. Without a paper ballot, the system should not be used.

THE ROAD AHEAD

The situation with Internet voting is one that we have seen already: There was intense political lobbying, misrepresentations, and even lies from various officials. The vendors emphasized the testing, and made claims about “world class security”, but they resisted a complete review of their secretive systems. They also claimed that all programmers and election workers are honest, which cannot be true. Finally, they attacked the sanity, motives, patriotism, and expertise of skeptics, including computer professionals that questioned their systems. When they had no defense left, they attacked the messengers. In the end, the California and Ohio reviews proved that the skeptics were right.

Voting on the Internet has the same problems that we have seen in the United States with paperless, secretive voting machines, plus it uses a network and PCs that in their very architecture are not secure. They are also subject to all kinds of attacks and scams that even dedicated election systems do not have to deal with. At least with a paper ballot-based system you have a chance to recover from problems.

With Internet voting, the future of the United States is potentially at risk. It is important not to make a mistake.