13

eVoting
by Phillip J. Windley, Ph.D.

If there's anything that the election of 2000 taught us, regardless of our feeling about the outcome, it was that elections are precarious things, run on unreliable systems using technologies and even procedures that left us all shaking our heads. I'd bet that there are very few computer geeks watching the fiasco unfold who weren't thinking: "give me a few weeks and I'd build something that worked." That's what we do: solve problems.

The lure of eVoting, or the application of digital technologies to voting systems, comes down to the simple idea that computers, and more recently, the Internet have have fundamentally changed other parts of our lives, so why not democracy as well. Since voting is one of the basic processes of democracy, it seems a natural candidate for electronic automation.

How voting works

In the United States, voting is a local issue. The Federal government certainly has a lot of say about voting through the Federal Election Commission, but in the end, its state and local officials who administer elections. In most states, the secretary of state's office runs an elections office that sets rules and administers statewide elections.

The actual elections themselves are usually the purview of the county clerk. Moreover, counties and municipalities bear the majority of the cost of managing elections. In 2000, the total county election expenditures were estimated at over $1 billion, or about $10 per voter.

Voting is more complicated than simply tallying votes. In fact, most of the work in an election occurs long before the voter ever steps into the booth. Voter registration requires large databases of voters, their addresses and geographic calculation of precinct and district information. Ballot preparation is a long process that is complicated by myriad rules and regulations. The election itself must be administered, usually with the help of a large, volunteer workforce that gets to practice about once per year. All of these activities, in addition to vote tallying, are part of a voting system.

After the election of 2000, Congress passed the Help America Vote Act (HAVA). The act changes the voter registration system, requires that all punch card systems be replaced, and calls for electronic voting methods that will enable disabled citizens to vote without assistance. These mandates and some Federal money have resulted in a large-scale replacement of old voting systems. HAVA also increased the role that the Federal Elections Commission plays in state and county administered elections.

While the goals of HAVA are laudable, the move to new voting systems has created a hey-day for voting system vendors and caused a number of people to be alarmed over some very real security and integrity questions.

Computerized systems have to work better, don't they?

Much as we'd like to believe that computerized systems work better than their non-computerized counterparts, that often isn't the case. The Caltech-MIT Voting Technology project found that of the five types of voting machines, hand-counted paper, mechanical lever machines, punch card ballots, optically scanned paper, and electronic voting machines, electronic machines have the second highest rate of unmarked, uncounted and spoiled ballots in presidential, Senate, and governor elections over the last 12 years. The only system that was worse was mechanical lever machines. Hand-counted and optically scanned paper have had the lowest rates over the same period.

So, while electronic systems may be more reliable than mechanical systems, and cheaper to administer than paper ballots, as electronic systems are currently deployed, they are not *better* in the sense that matters most: voting system integrity.

eVoting integrity

Integrity is the central question in any election. For democracy to work, citizens must believe that their vote has been counted correctly and that the system can and will find and correct mistakes. The question of integrity is a critical one to opponents of current eVoting systems.

California Secretary of State Kevin Shelley in an address to the Voting Systems Panel said:

> The core of our American democracy, members, is the right to vote. And implicit in that right is the notion that that vote

> be private, that vote be secure, and that vote be counted as it was intended when it was cast by the voter. I think what we're encountering is a pivotal moment in our democracy where all that is being called into question—the privacy of the vote, the security of the vote, and the accuracy of the vote. It troubles me, and it should trouble you.[1]

These three issues: privacy, security, and accuracy are at the heart of the eVoting debate.

Questions surrounding eVoting hinge on the fact that software errors, hardware malfunctions, and even malicious tampering are unavoidable and as a consequence, systems that use software for preparing ballots, managing elections, and counting votes should be built to mitigate these errors and should include processes that create audit trails and cross-checks.

Software has caused many problems with elections. VerifiedVoter.org cites several examples from the November 2003 election:

> In Fairfax, Virginia, testing ordered by a judge revealed that several voting machines subtracted one in every hundred votes for the candidate who lost her seat on the School Board.
>
> In Boone County, Indiana, a software glitch caused 144,000 votes to be counted from a pool of 19,000 registered voters. Corrected accounting showed just 5,352 ballots cast.[2]

These problems, reported by the press for just a single election cycle, raise the specter of other, undiscovered problems. Would we know if there was a problem?

There are two approaches that have been suggested for mitigating the problems with electronic voting systems. Neither is sufficient on its own to solve the problem, but taken together, along with careful election practices, they provide significantly increased confidence in electronic voting systems.

The first approach to the problem is called a "voter verifiable audit trail." The voter verified audit trail requires that electronic voting machines print out, before the voter's choices have been recorded, a tamper-proof paper ballot. The voter can verify that the choices on the paper ballot and the choices on the electronic screen are correct and then record the vote. The paper ballot is then deposited with elections officials and kept securely until after the electronic results have been certified. If there is a challenge to the election, or some other reason to suspect the results, the paper ballots would

[1] *Address to California Voting Systems Panel, December 16, 2003, http://www.verifiedvoting.org/kevinshelley2003dec16.asp*

[2]*(http://www.verifiedvoting.org/resources/hr2239_volunteers/Introduction-2-pages.htm*

be available for inspection and could be recounted as an independent, second record.

The primary objections to the voter verified audit trail are twofold: cost and complexity. Neither are problems that can be ignored, but both are solvable. The cost issue is obvious and the solution requires that voting integrity be prioritized higher than other government functions. The complexity issue is more difficult to solve. Voting is already a process that is confusing to many voters. Further, voting is usually administered at the precinct level by volunteers with little training and experience. A complicated process requires increased poll worker training and better facilities for educating voters at the polls about the process.

The second approach is to open up electronic voting system software to inspection by anyone who is interested. A scenario where an insider maliciously alters the software in an electronic voting system to throw and election is not far-fetched. Such an alteration would be difficult to detect because US courts have ruled that the source code used to run electronic voting systems can be considered a 'trade secret' and not open to public scrutiny. Malicious alterations could be clearly visible in the source code, but difficult to detect in the compiled code running on the voting systems.

Furthermore, not only are the national standards for testing and certifying electronic voting systems weak, but enforcement is lax. Testing of electronic voting systems is done in secret by small groups and the results are not open to the public. The results of these certifications are overseen by elections officials who, by and large, know very little about computer security.

Recently, the source code for Diebold's electronic voting system was leaked to the Internet. The system in question has been used to run elections in Georgia and other jurisdictions. This leak gave computer security experts a unique opportunity to perform an independent, scientific analysis of the source code to a production-quality electronic voting system by a major manufacturer. Three scientists from John Hopkins University, Tadyoshi Kohno, Adam Stubblefield, and Aviel Rubin, and one from Rice University, Dan Wallach, issued a report that concluded:

> Our analysis shows that this voting system is far below even the most minimal security standards applicable in other contexts. We highlight several issues including unauthorized privilege escalation, incorrect use of cryptography, vulnerabilities to network threats, and poor software development processes. For example, common voters, without any insider privileges, can cast unlimited votes without being detected by any mechanisms within the voting terminal. Furthermore, we show that even the most serious of our outsider attacks could have been discovered without the source code. In the face of such attacks, the usual worries about insider threats are not the only concerns; outsiders can do the damage. That said, we demonstrate that the insider

> threat is also quite considerable. We conclude that, as a society, we must carefully consider the risks inherent in electronic voting, as it places our very democracy at risk.[3]

This example highlights an important point: if a single closed system has the number and severity of errors found in this report, what serious flaws might other, closed electronic voting systems contain? Unfortunately, it is impossible to know since we have only the assurances of the vendors and certification boards.

Manufacturer objections to open source are twofold. The first is a red herring that questions the open source development methodology as a reliable means for creating voting systems. This confuses a development methodology with a result. Opening the source code of electronic voting systems to inspection by the public at large does not require that the company adopt an open-source development methodology.

The second objection comes down to a business question. If electronic voting system vendors open up their source code for public inspection, how can they maintain a competitive advantage? There are many companies who compete without keeping their source code a secret. MySQL and Redhat are examples. That said, as a society, we must ask ourselves whether maintaining the viability of a few corporations trumps our right to a voting system that we can trust. I'm confident that if elections officials required open source voting systems as a matter of gaining contracts, there would be companies who would find a way to do it and still prosper.

Internet Voting

A subtopic in eVoting that deserves special attention is the subject of Internet voting. Often, voters do not, or cannot, vote because of the inconvenience of getting to a polling place. They may be home bound, traveling, or even living in a foreign country. Of course, absentee voting is an option in these cases, but comes with its own set of problems. First, you have to be able to predict, usually weeks in advance, that you will be “absent” and request a ballot be mailed to you. Furthermore, you usually have to fill out extra paperwork, and mail it in with your ballot. This is not only discouraging to many who might otherwise vote, but can also be a source of delay in election results.

The Internet has done so much to change how we interact with other segments of society, it seems a natural choice for solving some of the absentee voter problems. Indeed, the Pentagon nearly put an Internet voting system, called SERVE, into place for the 2004 election. The rollout was

[3] Analysis of an Electronic Voting System, Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, IEEE Symposium on Security and Privacy 2004, *http://avirubin.com/vote.pdf*

suspended, however, after a panel of experts issued a scathing report on the security problems inherent in the scheme.

The concerns can be summarized as follows:

> [B]ecause SERVE is an Internet- and PC-based system, it has numerous other fundamental security problems that leave it vulnerable to a variety of well-known cyber attacks (insider attacks, denial of service attacks, spoofing, automated vote buying, viral attacks on voter PCs, etc.), any one of which could be catastrophic.
>
> Such attacks could occur on a large-scale, and could be launched by anyone from a disaffected lone individual to a well-financed enemy agency outside the reach of U.S. law. These attacks could result in large-scale, 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.
>
> The vulnerabilities we describe cannot be fixed by design changes or bug fixes to SERVE. These vulnerabilities are fundamental in the architecture of the Internet and of the PC hardware and software that is ubiquitous today. They cannot all be eliminated for the foreseeable future without some unforeseen radical breakthrough.
>
> We have examined numerous variations on SERVE in an attempt to recommend an alternative Internet-based voting system that might deliver somewhat less voter convenience in exchange for fewer or milder security vulnerabilities. However, all such variations suffer from the same kinds of fundamental vulnerabilities that SERVE does...
>
> Because the danger of successful, large-scale attacks is so great, we reluctantly recommend shutting down the development of SERVE immediately and not attempting anything like it in the future until both the Internet and the world's home computer infrastructure have been fundamentally redesigned, or some other unforeseen security breakthroughs appear.

Ultimately, based largely on this report, that is what happened—the Pentagon decided to scrap the system, at least for the 2004 election. Its certain that various jurisdictions will continue to experiment with Internet voting because the benefits seem so great, but without significant, unforeseen technical advances, many of which are antithetical to the very design and operation of the Internet, voting over the Internet is likely to remain infeasible.

A Call to Action

Voting systems are one of foundational technologies of our democracy, and make no mistake, whether digital or not, they are technologies. I think it’s safe to assume that no matter how problematic the current systems and processes are, electronic voting systems are not going away. As a computer professional, you have a unique perspective on how digital technologies can affect voting systems and getting involved isn't that difficult.

Here are some ideas about how to get involved:

Start with your county clerk and find out what election system your county uses and how it is certified. What issues do they face? Is there a way you can help them?

Meet with someone in the state election's office. Ask them the same questions. What is the certification process is your State? State elections personnel have a difficult assignment, but they're approachable and willing to listen for the most part. Keep your tone helpful, rather than belligerent and you'll learn something and have a chance to educate them along the way.

Engage your legislators. Send them an email and ask to meet with them. Help them understand the issues surrounding eVoting so that they're educated. Most legislators I've dealt with want to understand the technology implications, particularly on issues as fundamental as voting. You may not get much traction when they're in session, but few states have full time legislatures. Contact them when they're out of session and you'll likely find that you're knowledge and willingness to help are welcome.

Finally, a number of advocacy groups are working with government to create trustworthy voting system. Advocacy groups can always use volunteer help and there's room to make your voice heard.