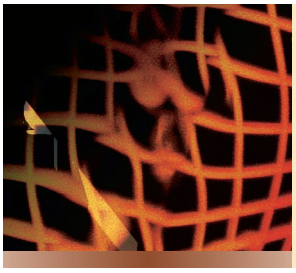
The Real Risk of Digital Voting?

William A. Arbaugh, University of Maryland at College Park

The 2004 US elections have come and gone. Regardless of whether the outcome left you feeling jubilant or forlorn, no digital disasters have yet revealed themselves.

Sure, the new electronic voting machines generated some glitches, crashes, blue screens, and a few magically appearing and disappearing votes. With the exception of blue screens, however, these problems are as old as the stories about dead people voting—sometimes twice. Only the machinery was new.

Does it have to be this way? Could we get a better system?



New machinery is only one part of a voting system and its risks.

SYSTEM SECURITY

The human element is usually the weakest point in a system's security, and this is also the case with voting. Using digital voting machines doesn't reduce the human factor; it only introduces a new venue for manipulating the voting process—albeit on a much grander scale.

Many computer scientists have expressed their concern with the security of digital voting machines, especially their lack of a voter-verifiable audit trail. These risks pose real threats that we must resolve.

To understand what system checks and balances are possible, we need to examine the entire voting process, not just the technology—even though, let's face it, the technology is woefully flawed at this point.

An election has essentially three phases: registration, voting, and tallying. The risks of human manipulation of the system are highest in the first two phases, and the risks of digital manipulation are highest in the last two.

Registration phase

"Vote early and often" is a cynical phrase that witnesses the long history of manipulation in the registration phase. We've all heard the stories of dead people being registered to vote, eligible voters being purged from the rolls, and so forth.

Digital voting machines have nothing to do with this, of course. Federal registration standards could improve the process, along with stronger identification requirements and database technology to verify voter eligibility.

Unfortunately, improvements in this area will also erode privacy. An interesting conundrum: Do we want a more secure election or privacy?

Voting phase

The human risks in the voting phase are fairly well known. It's easy to lose votes. For example, one way to prevent people from reaching the polls is to make them wait in line for hours. Corrupt election officials have been known to lose ballots and ballot boxes, and organizations can create votes relatively easily by manipulating absentee ballots in a get-out-the-vote drive.

These methods give perpetrators the advantage of plausible deniability. Corrupt election officials can deny knowing that so many people were going to turn out or they can claim that they've never seen that ballot box before.

Unfortunately, it is difficult to institute checks and balances to prevent this sort of manipulation.

Digital manipulation. The risks of digital manipulation are well documented, but election officials can easily detect under- and overcounts by tracking how many voters used each machine and comparing that number to the total number of votes recorded on it.

In Maryland, voters place their ballots in a bag or box located next to the voting machine. At the end of the day, the election official counts the cards and compares the number to the machine's tally. Any difference indicates a likely problem. This is how several under- and overcounts were identified in the recent election.

The problem is what to do when a problem is detected? The bits stored on the machine are the only record. No independent method exists for auditing or recounting the results. This is unlike just about every other electronic transaction you make today. If you use an ATM machine or a credit card, you get a paper receipt.

Using paper receipts with voting isn't

Published by the IEEE Computer Society

as straightforward as in these commercial transactions, and this may not be the best solution to the problem. But we certainly must have some method of completing an audit or recount to verify the equipment's trustworthiness.

Accountability. It becomes easier to change a vote count with digital voting machines, which makes accountability even more important to controlling this risk. The lack of a robust recount method makes recovering from this form of attack impossible.

Some political scientists claim that we could use statistical means such as comparing historical and exit-poll data to the actual results to detect a vote-changing attack. But even if a statistician finds a problem, how is that valuable when it isn't possible to audit machine performance?

Furthermore, since there are no standard policies for handling election equipment after the polls close, the perpetrators of such fraud could "clean" the machines in the time between the analysis and subsequent audit. I am sure that some jurisdictions have excellent policies; I'm equally sure that many have absolutely no policy.

Tallying phase

The only real risk in the tallying phase is digital. The risk here primarily involves changing votes because adding or subtracting votes would result in different numbers from those reported by subordinate jurisdictions. Changed votes, however, could escape detection.

HELP FOR THE PROCESS

But enough about the problems. What are some possible solutions?

I'm only going to address the problems directly solvable digitally. Those related to human foibles are best left to political scientists and lawyers.

Certification

The first and most important step is to develop and institute detailed technical standards for the development, testing, and certification of voting machine hardware and software. Currently, there are no standards by which to measure the assurance or reliability of the software that vendors develop.

Nor are there open and public methods for testing it. Instead, laboratories test the software in secret, under contract to the vendor. This creates a serious conflict of interest.

Currently, there are no open and public methods for testing the voting machine software and hardware that vendors develop.

Further, even though federal law requires vendors to use only certified software in an election, several cases are documented in which vendors have installed uncertified software or patches during an election. In some cases, the jurisdiction had no idea it was using uncertified software.

Trust

The second step is to institute methods of assuring jurisdictions that the software configuration on a particular voting machine is certified and unmodified from its certified version.

Here's where trusted computing can play what I hope all can agree is a positive role. Equipping each digital voting machine with a Trusted Platform Module would allow poll watchers or election judges to measure the software by taking cryptographic hashes of each component as it is loaded and chaining it into single or multiple hashes.

These hashes will uniquely fingerprint the machine's software configuration. Each machine can then "attest" its configuration to a central server monitored by a poll watcher or election judge. Anyone monitoring the attestation server can easily detect any changes in the software and take the machine offline for further analysis.

Audit trail

The third and final step is some sort of voter-verifiable audit trail.

To many people, this means a paper solution. But paper introduces new problems that require more thought.

I don't know exactly what the solution should be. However, I do know we need this capability so that recounts aren't simply a matter of the computer adding the same bits over again. Every important process should have an independent audit capability. An election is no different.

These three steps will not eliminate election mischief by any means. Abuses of the election processes have occurred since the first vote was cast in this world, and they will continue to occur until the last vote is cast. We can, however, take some very simple steps to dramatically mitigate the potential abuses associated with using digital technology in our election process. ■

William A. Arbaugh is an assistant professor in the Department of Computer Science and the Institute for Advanced Computer Studies at the University of Maryland at College Park. Contact him at waa@cs.umd.edu.