Bruce Schneier

What's Wrong With Electronic Voting Machines?

By Bruce Schneier
OpenDemocracy
November 9, 2004

In the aftermath of the American presidential election on 2 November 2004, electronic voting machines are again in the news. Computerised machines lost votes, subtracted votes, and doubled some votes too. And because many of these machines have no paper audit trails, a large number of votes will never be counted.

While it is unlikely that deliberate voting-machine fraud changed the result of this presidential election, the internet is buzzing with rumours and allegations in a number of different jurisdictions and races. It is still too early to tell if any of these problems affected any individual state's election, but the next few weeks will reveal whether any of the information crystallises into something significant.

The US has been here before. After the 2000 election, voting-machine problems made international headlines. The government appropriated money to fix the problems nationwide. Unfortunately, electronic voting machines -- although presented as the solution -- have largely made the problem worse. This doesn't mean that these machines should be abandoned, but they need to be designed to increase both their accuracy, and peoples' trust in their accuracy.

This is difficult, but not impossible.

Before I discuss electronic voting machines, I need to explain why voting is so difficult. In my view, a voting system has four required characteristics:

1. Accuracy. The goal of any voting system is to establish the intent of each individual voter, and translate those intents into a final tally. To the extent that a voting system fails to do this, it is undesirable. This characteristic also includes security: It should be impossible to change someone else's vote, stuff ballots, destroy votes, or otherwise affect the accuracy of the final tally.
2. Anonymity. Secret ballots are fundamental to democracy, and voting systems must be designed to facilitate voter anonymity.
3. Scalability. Voting systems need to be able to handle very large elections. Nearly 120 million people voted in the US presidential election. About 372 million people voted in India's May 2004 national elections, and over 115 million in Brazil's October 2004 local elections. The complexity of an election is another issue. Unlike in many countries where the national election is a single vote for a person or a party, a United States voter is faced with dozens of individual election decisions: national, local, and everything in between.
4. Speed. Voting systems should produce results quickly. This is particularly important in the United States, where people expect to learn the results of the day's election before bedtime.

Through the centuries, different technologies have done their best. Stones and potshards dropped in Greek vases gave way to paper ballots dropped in sealed boxes. Mechanical voting booths, punch-cards, and then optical scan machines replaced hand-counted ballots. New computerised voting machines promise even more efficiency, and internet voting even more convenience.

But in the rush to improve speed and scalability, accuracy has been sacrificed. And to reiterate: accuracy is not how well the ballots are counted by, say, a punch-card reader. It's not how the tabulating machine deals with hanging chads, pregnant chads, or anything like that. Accuracy is how well the process translates voter intent into appropriately counted votes.

Trust a computer to be inaccurate

Technology gets in the way of accuracy by adding steps. Each additional step means more potential errors, simply because no technology is perfect. Consider an optical-scan voting system. The voter fills in ovals on a piece of paper, which is fed into an optical-scan reader. The reader senses the filled-in ovals and tabulates the votes. This system has several steps: voter to ballot, to ovals, to optical reader, to vote tabulator, to centralised total.

At each step, errors can occur. If the ballot is confusing, some voters will fill in the wrong ovals. If a voter doesn't fill them in properly, or if the reader is malfunctioning, then the sensor won't sense the ovals properly. Mistakes in tabulation -- either in the machine or when machine totals get aggregated into larger totals -- also cause errors.

A manual system of tallying the ballots by hand, and then doing it again to double-check, is more accurate simply because there are fewer steps.

The error rates in modern systems can be significant. Some voting technologies have a 5% error rate, which means one in twenty people who vote using the system don't have their votes counted. A system like this operates under the assumption that most of the time the errors don't matter. If you consider that the errors are uniformly distributed -- in other words, that they affect each candidate with equal probability -- then they won't affect the final outcome except in very close races.

So we're willing to sacrifice accuracy to get a voting system that will handle large and complicated elections more quickly.

In close races, errors can affect the outcome, and that's the point of a recount. A recount is an alternate system of tabulating votes: one that is slower (because it's manual), simpler (because it just focuses on one race), and therefore more accurate.

Note that this is only true if everyone votes using the same machines. If parts of a town that tend to support candidate A use a voting system with a higher error rate than the voting system used in parts of town that tend to support candidate B, then the results will be skewed against candidate A.

With this background, the problem with computerised voting machines becomes clear. Actually, "computerised voting machines" is a bad choice of words. Many of today's mechanical voting technologies involve computers too. Computers tabulate both punch-card and optical-scan machines.

The current debate centres on all-computer voting systems, primarily touch-screen systems, called Direct Record Electronic (DRE) machines (the voting system used in India's May 2004 election -- a computer with a series of buttons -- is subject to the same issues).

In these systems the voter is presented with a list of choices on a screen, perhaps multiple screens if there are multiple elections, and he indicates his choice by touching the screen. As Daniel Tokaji points out, these machines are easy to use, produce final tallies immediately after the polls close, and can handle very complicated elections. They can also display instructions in different languages and allow for the blind or otherwise handicapped to vote without assistance.

They're also more error-prone. The very same software that makes touch-screen voting systems so friendly also makes them inaccurate in the worst possible way.

'Bugs' or errors in software are commonplace, as any computer user knows. Computer programs regularly malfunction, sometimes in surprising and subtle ways. This is true for all software, including the software in computerised voting machines.

For example:

In Fairfax County, Virginia in 2003, a programming error in the electronic-voting machines caused them to mysteriously subtract 100 votes from one candidate's totals.

In a 2003 election in Boone County, Iowa the electronic vote-counting equipment showed that more than 140,000 votes had been cast in the municipal elections, even though only half of the county's 50,000 residents were eligible to vote.

In San Bernardino County, California in 2001, a programming error caused the computer to look for votes in the wrong portion of the ballot in 33 local elections, which meant that no votes registered on those ballots for that election. A recount was done by hand.

In Volusia County, Florida in 2000, an electronic voting machine gave Al Gore a final vote count of negative 16,022 votes.

There are literally hundreds of similar stories.

What's important about these problems is not that they resulted in a less accurate tally, but that the errors were not uniformly distributed; they affected one candidate more than the other. This is evidence that you can't assume errors will cancel each other out; you have to assume that any error will skew the results significantly and affect the result of the election.

And then there's security

Another issue is that software can be 'hacked'. That is, someone can deliberately introduce an error that modifies the result in favour of his preferred candidate.

This has nothing to do with whether the voting machines are hooked up to the internet on election day, as Daniel Tokaji seems to believe. The threat is that the computer code could be modified while it is being developed and tested, either by one of the programmers or a hacker who gains access to the voting-machine company's network. It's much easier to surreptitiously modify a software system than a hardware system, and it's much easier to make these modifications undetectable.

Malicious changes or errors in the software can have far-reaching effects. A problem with a manual machine just affects that machine. A software problem, whether accidental or intentional, can affect many thousands of machines and skew the results of an entire election.

Some have argued in favour of touch-screen voting systems, citing the millions of dollars that are handled every day by ATMs and other computerised financial systems. That argument ignores another vital characteristic of voting systems: anonymity.

Computerised financial systems get most of their security from audit. If a problem is suspected, auditors can go back through the records of the system and figure out what happened. And if the problem turns out to be real, the transaction can be unwound and fixed. Because elections are anonymous, that kind of security just isn't possible.

None of this means that we should abandon touch-screen voting; the benefits of DRE machines are too great to throw away. But it does mean that we need to recognise the limitations, and design systems that can be accurate despite them.

Computer security experts are unanimous on what to do (some voting experts disagree, but it is the computer security experts who need to be listened to; the problems here are with the computer, not with the fact that the computer is being used in a voting application). They have two recommendations, echoed by Siva Vaidhyanathan:

1. DRE machines must have a voter-verifiable paper audit trails (sometimes called a voter-verified paper ballot). This is a paper ballot printed out by the voting machine, which the voter is allowed to look at and verify. He doesn't take it home with him. Either he looks at it on the machine behind a glass screen, or he takes the paper and puts it into a ballot box. The point of this is twofold: it allows the voter to confirm that his vote was recorded in the manner he intended, and it provides the mechanism for a recount if there are problems with the machine.
2. Software used on DRE machines must be open to public scrutiny. This also has two functions: it allows any interested party to examine the software and find bugs, which can then be corrected, a public analysis that improves security; and it increases public confidence in the voting process - if the software is public, no one can insinuate that the voting system has unfairness built into the code (companies that make these machines regularly argue that they need to keep their software secret for security reasons. Don't believe them. In this instance, secrecy has nothing to do with security).

Computerised systems with these characteristics won't be perfect -- no piece of software is -- but they'll be much better than what we have now. We need to treat voting software like we treat any other high-reliability system.

The auditing that is conducted on slot machine software in the US is significantly more meticulous than that applied to voting software. The development process for mission-critical airplane software makes voting software look like a slapdash affair. If we care about the integrity of our elections, this has to change.

Proponents of DREs often point to successful elections as "proof" that the systems work. That completely misses the point. The fear is that errors in the software -- either accidental or deliberately introduced -- can undetectably alter the final tallies. An election without any detected problems is no more a proof that the system is reliable and secure, than a night that no one broke into your house is proof that your locks work. Maybe no one tried to break in, or maybe someone tried and succeeded -- and you don't know it.

Even if we get the technology right, we still won't be finished. If the goal of a voting system is to accurately translate voter intent into a final tally, the voting machine itself is only one part of the overall system. In the 2004 US election, problems with voter registration, untrained poll workers, ballot design, and procedures for handling problems, resulted in far more votes being left uncounted than problems with technology.

If we're going to spend money on new voting technology, it makes sense to spend it on technology that makes the problem easier instead of harder.

earlier essay: Getting Out the Vote
later essay: Profile: "hinky"
categories: Elections
back to Essays and Op Eds