

Election Science

In the advent of the Iraq war, we had to worry about inspection science. Now, as a national election approaches in the United States, we should give a thought or two to election science. Among the rich possibilities for research here, two questions emerge that need serious attention: How do we guarantee the accountability of the voting system? And what does information technology have to offer?

We voters should be interested in the answers, because we want to preserve our faith in the system and its fairness. The two fundamental requirements are traceability (we'd like to know that our vote counted as delivered) and privacy (we don't want our vote known by others). The system for counting votes ought to deliver both objectives without requiring us to rely on trust. In this important domain of vote-recording methods, we are now looking at a new technology that is being quickly adopted: electronic touch-screen voting machines, manufactured by a few corporations and delivered to a number of states for hefty prices. Maryland, for example, just shelled out \$55 million for machines known as the Diebold AccuVote-TS Voting System. Enthusiasm for electronic vote-counting on the part of state election commissions is understandable; few, naturally, want a debacle of the kind that turfed the 2000 Florida presidential vote into the Supreme Court.

Computer science and cryptography experts can get passionate about the science issues here. The consensus view, with which a few will disagree, is that for traceability, electronic machines should provide for a voter-verifiable audit trail in which a computerized system prints a paper ballot that is read and verified by the voter. Such paper confirmation can be given to the voter privately, as well as be retained by officials for later verification. Most of the machines aren't equipped for this (including the ones in that Maryland purchased, though Nevada has fared better with a vendor whose e-machines are fitted with voter-verifiable receipt printers). Although some machines can print vote totals and transactional information at the close of an election, these are not considered voter-verifiable.

For the moment, never mind who's right about the need for paper. Most of the machines out there don't allow for such an auditable paper trail, so let's ponder the following hypothetical scenario. It's the morning after Election Day, and it's still a tight race in the battleground state of Ohio. It looks as if the incumbent president will win the national election if he takes Ohio, but his lead there is only 2000 votes. A team of Democratic lawyers is already challenging the count from several downstate jurisdictions in which voters are claiming that the vote recorded from their precincts shows large majorities for Bush—in sharp disagreement with exit polls. Unfortunately, Diebold machines that do not provide voter-verifiable receipts are in use in this particular district, and public controversy is already high in the state (owing to an actual pre-election statement by Diebold's chief executive officer, a prominent Bush fundraiser, that he would “deliver” the state of Ohio to the president). Thus, the aftermath of a savagely partisan U.S. election turns into a field day for conspiracy theorists, and trust in government takes another hit.

Is this just another exercise in political paranoia? Something of the sort could happen in Maryland. At the 2004 IEEE Symposium on Security and Privacy, the Johns Hopkins University Information Security Institute reported an analysis of the Diebold computer software source code. They found it “far below even the most minimal security standards applicable in other contexts” and identified flaws that would allow the system to be hacked for the purpose of changing votes. They also showed that this could be accomplished at the “retail” level, by outsiders attacking a single machine or precinct, or on the “wholesale” level, by insiders bent on larger-scale manipulation. Since then, Diebold and Maryland have taken some steps to improve the system to prevent security vulnerabilities.

So, you're ready to vote. Remember that not all electronic voting machines will print out a receipt for you to verify your transactions. You press all the right buttons and leave, hoping that your votes have registered. Your state election commission may have asked you to take it on faith that your vote will be counted correctly, perhaps because of “upgrades” that have solved those computer code problems or some other glitch. As you leave the polling place, how comfortable are you?

Donald Kennedy
Editor-in-Chief