MSNBC.com

Newsweek

Black Box Voting Blues

Electronic ballot technology makes things easy. But some computer-security experts warn of the possibility of stolen elections

By Steven Levy
Newsweek

Nov. 3 issue - After the traumas of butterfly ballots and hanging chad, election officials are embracing a brave new ballot: sleek, touch-screen terminals known as direct recording electronic voting systems (DRE). States are starting to replace their Rube Goldbergesque technology with digital devices like the Diebold Accu-Vote voting terminal. Georgia uses Diebolds exclusively, and other states have spent millions on such machines, funded in part by the 2002 federal Help America Vote Act. Many more terminals are on the way.

Unforunately, the machines have “a fatal disadvantage,” says Rep. Rush Holt of New Jersey, who’s sponsoring legislation on the issue. “They’re unverifiable. When a voter votes, he or she has no way of knowing whether the vote is recorded.” After you punch the buttons to choose your candidates, you may get a final screen that reflects your choices—but there’s no way to tell that those choices are the ones that ultimately get reported in the final tally. You simply have to trust that the software inside the machine is doing its job.

It gets scarier. The best minds in the computer-security world contend that the voting terminals can’t be trusted. Listen, for example, to Avi Rubin, a computer-security expert and professor at Johns Hopkins University who was slipped a copy of Diebold’s source code earlier this year. After he and his students examined it, he concluded that the protections against fraud and tampering were strictly amateur hour. “Anyone in my basic security classes would have done better,” he says. The cryptography was weak and poorly implemented, and the smart-card system that supposedly increased security actually created new vulnerabilities. Rubin’s paper concluded that the Diebold system was “far below even the most minimal security standards.” Naturally, Diebold disagrees with Rubin. “We’re very confident of accuracy and security in our system,” says director of Diebold Election Systems Mark Radke.

After Rubin’s paper appeared, Maryland officials—who were about to drop $57 million on Diebold devices—commissioned an outside firm to look at the problem. The resulting report confirmed many of Rubin’s findings and found that the machines did not meet the state’s security standards. However, the study also said that in practice some problems were mitigated, and others could be fixed, an attitude Rubin considers overly optimistic. “You’d have to start with a fresh design to make the devices secure,” he says.

In the past few months, the computer- security community has been increasingly vocal on the problems of DRE terminals. “I think the risk [of a stolen election] is extremely high,” says David Dill, a Stanford computer scientist. The devices are certified, scientists say, but the process focuses more on making sure that the machines don’t break down than on testing computer code for Trojan horses and susceptibility to tampering. While there’s no evidence that the political establishment actually wants vulnerable machines, the Internet is buzz-ing with conspiracy theories centering on these “black box” voting devices. (The biggest buzz focuses on the 2002 Georgia gubernatorial election, won by a Republican underdog whose win confounded pollsters.) Suspicions run even higher when people learn that some of those in charge of voting technology are themselves partisan. Walden O’Dell, the CEO of Diebold, is a major fund-raiser for the Bush re-election campaign who recently wrote to contributors that he was “committed to helping Ohio deliver its electoral votes for the president next year.” (He later clarified that he wasn’t talking about rigging the machines. Whew.)

To remedy the problem, technologists and allies are rallying around a scheme called verifiable voting. This supplements electronic voting systems with a print-out that affirms the voter’s choices. The printout goes immediately into a secure lockbox. If there’s a need for a recount, the paper ballots are tallied. It’s not a perfect system, but it could keep the machines honest. If Representative Holt’s proposed Voter Confidence Act is passed, verification will be the law of the land by the 2004 election, but prospects are dim, as the committee chairman, Bob Ney of Ohio, is against it.

Critics of verifiable voting do have a point when they note that the printouts are susceptible to some of the same kinds of tricks once played with paper ballots. But there’s a promise of more elegant solutions for electronic voting that are private, verifiable and virtually tamperproof. Mathematician David Chaum has been working on an ingenious scheme based on encrypted receipts. But whatever we wind up using, it’s time for politicians to start listening to the geeks. They start from the premise that democracy deserves no less than the best election technology possible, so that the vote of every citizen will count. Can anyone possibly argue with that?

URL: http://msnbc.msn.com/id/3339650/