The Big Gamble on Electronic Voting

By RANDALL STROSS
Published: September 24, 2006

HANGING chads made it difficult to read voter intentions in 2000. Hotel minibar keys may do the same for the elections in November.

The mechanics of voting have undergone a major change since the imbroglio that engulfed presidential balloting in 2000. Embarrassed by an election that had to be settled by the Supreme Court, Congress passed the Help America Vote Act of 2002, which provided funds to improve voting equipment.

From 2003 to 2005, some $3 billion flew out of the federal purse for equipment purchases. Nothing said “state of the art” like a paperless voting machine that electronically records and tallies votes with the tap of a touch screen. Election Data Services, a political consulting firm that specializes in redistricting, estimates that about 40 percent of registered voters will use an electronic machine in the coming elections.

One brand of machine leads in market share by a sizable margin: the AccuVote, made by Diebold Election Systems. Two weeks ago, however, Diebold suffered one of the worst kinds of public embarrassment for a company that began in 1859 by making safes and vaults.

Edward W. Felten, a professor of computer science at Princeton, and his student collaborators conducted a demonstration with an AccuVote TS and noticed that the key to the machine’s memory card slot appeared to be similar to one that a staff member had at home.

When he brought the key into the office and tried it, the door protecting the AccuVote’s memory card slot swung open obligingly. Upon examination, the key turned out to be a standard industrial part used in simple locks for office furniture, computer cases, jukeboxes — and hotel minibars.

Once the memory card slot was accessible, how difficult would it be to introduce malicious software that could manipulate vote tallies? That is one of the questions that Professor Felten and two of his students, Ariel J. Feldman and J. Alex Halderman, have been investigating. In the face of Diebold’s refusal to let scientists test the AccuVote, the Princeton team got its hands on a machine only with the help of a third party.

Even before the researchers had made the serendipitous discovery about the minibar key, they had released a devastating critique of the AccuVote’s security. For computer scientists, they supplied a technical paper; for the general public, they prepared an accompanying video. Their short answer to the question of the practicality of vote theft with the AccuVote: easily accomplished.

The researchers demonstrated the machine’s vulnerability to an attack by means of code that can be...
introduced with a memory card. The program they devised does not tamper with the voting process.
The machine records each vote as it should, and makes a backup copy, too.

Every 15 seconds or so, however, the rogue program checks the internal vote tallies, then adds and
subtracts votes, as needed, to reach programmed targets; it also makes identical changes in the backup
file. The alterations cannot be detected later because the total number of votes perfectly matches the
total number of voters. At the end of the election day, the rogue program erases itself, leaving no
trace.

On Sept. 13, when Princeton’s Center for Information Technology Policy posted its findings, Diebold
issued a press release that shrugged off the demonstration and analysis. It said Princeton’s AccuVote
machine was “two generations old” and “not used anywhere in the country.”

I spoke last week with Professor Felten, who said he could not imagine how a newer version of the
AccuVote’s software could protect itself against this kind of attack. But he also said he would
welcome the opportunity to test it. I called Diebold to see if it would lend Princeton a machine.

Mark G. Radke, director for marketing at Diebold, said that the AccuVote machines were certified by
state election officials and that no academic researcher would be permitted to test an AccuVote
supplied by the company. “This is analogous to launching a nuclear missile,” he said enigmatically,
adding that Diebold had to restrict “access to the buttons.”

I persisted. Suppose, I asked, that a test machine were placed in the custodial care of the United States
Election Assistance Commission, a government agency. Mr. Radke demurred again, saying the
company’s critics were so focused on software that they “have no appreciation of physical security”
that protects the machines from intrusion.

This same point was featured prominently in the company’s press release that criticized the Princeton
study, saying it “all but ignores physical security and election procedures.” It is a criticism that
collides with the facts on Page 5 of the Princeton study, where the authors provide step-by-step details
of how to install the malicious software in the AccuVote.

Even before the minuscule lineage of the AccuVote key had been discovered, the researchers had
learned that the lock was easily circumvented: one of them could consistently pick it in less than 10
seconds.

If skeptics cannot believe what they read about the ease of manipulating an election, they can watch
the 10-minute online video: the AccuVote lock is picked, a memory card is inserted and the malicious
software is loaded; the machine is rebooted, and within 60 seconds the machine is ready to throw the
election in favor of any specified candidate.

Computer scientists with expertise in security issues have been sounding alarms for years. David L.
Dill at Stanford and Douglas W. Jones at the University of Iowa were among the first to alert the
public to potential problems. But the possibility of vote theft by electronic means remained nothing
more than a hypothesis — until the summer of 2003, when the code for the AccuVote’s operating
system was discovered on a Diebold server that was publicly accessible.

The code quickly made its way into researchers’ hands. Suspected vulnerabilities were confirmed, and
never-considered sloppiness was added to the list of concerns. At a computer security conference,
the AccuVote’s anatomy was analyzed closely by a team: Aviel D. Rubin, a computer science
professor at Johns Hopkins; two junior associates, Tadatoshi Kohno and Adam Stubblefield; and Dan
S. Wallach, an associate professor in computer science at Rice. They described how the AccuVote
software design rendered the machine vulnerable to manipulation by smart cards. They found that the
standard protections to prevent alteration of the internal code were missing; they characterized the
system as “far below even the most minimal security standards.”

Professor Rubin has just published a nontechnical memoir, “Brave New Ballot: The Battle to
Safeguard Democracy in the Age of Electronic Voting” (Morgan Road Books), that describes how his
quiet life was upended after he and his colleagues published their paper. He recalls in his book that
Diebold’s lawyers sent each of the paper’s authors a letter threatening the possibility of legal action,
warning them to “exercise caution” in interviews with the press lest they make a statement that would
“appear designed to improperly impair and impede Diebold’s existing and future business.” Johns Hopkins rallied to his side, however, and the university’s president, William R. Brody, commended him for being on the case.

Recently, there have been signs that states are having second thoughts about trusting their AccuVote equipment. Officials in California, Florida and Pennsylvania have been outspoken about their concerns. In Maryland earlier this year, the state House of Delegates voted 137 to 0 in favor of a bill to prohibit the use of its AccuVote machines because they were not equipped to generate a paper audit trail. (The state Senate did not take up the measure and it died.)

Professor Rubin favors the use of touch screens only for “ballot marking” — capturing a voter’s intended choice — then printing out a paper ballot with only the voter’s chosen candidates that the voter can visually check. Election officials can then use the slip to tally votes with an optical scanner made by a different manufacturer.

Manual audits of the tallies in at least 1 percent of all precincts, as is now required in California, would provide a transparent method of checking for integrity. Should a full recount be necessary, the paper ballots, containing only the selected names, provide unambiguous records of original intent.


Randall Stross is an author based in Silicon Valley and a professor of business at San Jose State University. E-mail: digitaldomain@nytimes.com.