washingtonpost.com

New Voting Systems Assailed

Computer Experts Cite Fraud Potential

By Dan Keating
Washington Post Staff Writer
Friday, March 28, 2003; Page A12

As election officials rush to spend billions to update the country's voting machines with electronic systems, computer scientists are mounting a challenge to the new devices, saying they are less reliable and less secure from fraud than the equipment they are replacing.

Prompted by the demands of state and federal election reforms, officials in Maryland, Georgia, Florida and Texas installed the high-tech voting systems last fall. Officials in those states, and other proponents of electronic voting, said the computer scientists' concerns are far-fetched.

"These systems, because of the level of testing they go through, are the most reliable systems available," said Michael Barnes, who oversaw Georgia's statewide upgrade. "People were happy with how they operated."

In Maryland, "the system performed flawlessly in the two statewide elections last year," said Joseph Torre, the official overseeing the purchase of the state's new systems. "The public has a lot of confidence in it, and they love it."

But the scientists' campaign, which began in California's Silicon Valley in January, has gathered signatures from more than 300 experts, and the pressure has induced the industry to begin changing course.

Electronic terminals eliminate hanging chads, pencil erasure marks and the chance that a voter might accidentally select too many candidates. Under the new systems, voters touch the screen or turn a dial to make their choices and see a confirmation of those choices before casting their votes, which are tallied right in the terminal. Recounts are just a matter of retrieving the data from the computer again. The only record of the vote is what is stored there.

Critics of such systems say that they are vulnerable to tampering, to human error and to computer malfunctions -- and that they lack the most obvious protection, a separate, paper receipt that a voter can confirm after voting and that can be recounted if problems are suspected.

Officials who have worked with touch-screen systems say these concerns are unfounded and, in certain cases, somewhat paranoid.

David Dill, the Stanford University professor of computer science who launched the petition drive, said, "What people have learned repeatedly, the hard way, is that the prudent practice -- if you want to escape with your data intact -- is what other people would perceive as paranoia."

Other computer scientists, including Rebecca Mercuri of Bryn Mawr College, say that problems are so likely that they are virtually guaranteed to occur -- and already have.

Lost and Found

Mercuri, who has studied voting security for more than a decade, points to a November 2000 election in South Brunswick, N.J., in which touch-screen equipment manufactured by Sequoia Voting Systems was used.

In a race in which voters could pick two candidates from a pair of Republicans and a pair of Democrats, one machine recorded a vote pattern that was out of sync with the pattern recorded elsewhere -- no votes whatsoever for one Republican and one Democrat. Sequoia said at the time that no votes were lost -- they were just never registered. Local officials said it didn't matter whether the fault was the voters' or the machine's, the expected votes were gone.

In October, election officials in Raleigh, N.C., discovered that early voters had to try several times to record their votes on iVotronic touch screens from Election Systems and Software. Told of the problems, officials compared the number of voters to the number of votes counted and realized that 294 votes had apparently been lost.

When Georgia debuted 22,000 Diebold touch screens last fall, some people touched one candidate's name on the screen and saw another candidate's name appear as their choice. Voters who were paying attention had a chance to correct the error before finalizing their vote, but those who weren't did not.

Chris Rigall, spokesman for the secretary of state's office, said that the machines were quickly replaced, but that there was no way of knowing how many votes were incorrectly counted.

In September in Florida, Miami-Dade and Broward counties had a different kind of vote loss with ES&S touch-screen equipment: At the end of the day, precincts that reported hundreds of voters also listed virtually no votes counted. In that case, technicians were able to retrieve the votes from the machines.

"If the only way you know that it's working incorrectly is when there's four votes instead of 1,200 votes, then how do you know that if it's 1,100 votes instead of 1,200 votes? You'll never know," said Mercuri.

Because humans are imperfect and computers are complicated, said Ben Bederson, a professor of computer science at the University of Maryland, mistakes will always be made. With no backup to test, the scientists say, mistakes will go undetected.

"I'm not concerned about elections that are a mess," Dill said. "I'm concerned about elections that appear to go smoothly, and no one knows that it was all messed up inside the machine."

"We're not paranoid," said Mercuri. "They're avoiding computational realities. That's the computer science part of it. We can't avoid it any more than physical scientists can avoid gravity."

The Miami-Dade and Georgia terminals were reprogrammed right up until the eve of the fall elections. The last-minute patches don't go through sufficient review, Mercuri said, and any computer that can be reprogrammed simply by inserting an update cartridge cannot be considered secure or reliable.

Dill said hackers constantly defeat sophisticated protections for electronic transactions, bank records, credit reports and software. "Someone sufficiently unscrupulous, with an investment of $50,000, could put together a team of people who could very easily subvert all of the security mechanisms that we've heard about on these [voting] machines," he said.

People who have sold or administered electronic voting systems, however, say the scenarios of fraud or widespread, election-changing error were not of the real world.

'We'd Detect It'

Howard Cramer, vice president for sales at Sequoia, one of the nation's largest suppliers of electronic voting systems, noted that his company has been supplying the systems for a decade and a half. "Our existing approach is verifiably accurate, 100 percent," he said. "Some of the things they're saying are flat-out wrong. Some are conceivable, but outside the likelihood of possibility."

The designer of Georgia's security system, for example, said nobody could insert a secret program to steal an election when the machines are created, because no one even knows at that time who the candidates will be, and the only people with access to the machines at the last minute are local officials.

"They're talking about what they could do if they had access to the [computer program] code, if we had no procedures in place and no physical security in place," said Brit Williams, a computer scientist at Kennesaw State University. "I'm not arguing with that. But they're not going to get access to that code. Even if they did, we'd detect it."

He also said that Georgia's patch was checked before it was installed and did not affect the tallying of votes. And no one, he said, could reprogram Georgia's terminals by inserting a cartridge.

"On our machine, the port is in a locked compartment. The only person in the precinct who has a key to that locked compartment is the precinct manager. [Critics are] looking at it from a purely computer science point of view, saying the system is vulnerable, and it would be vulnerable if we let anyone walk up and stick a card into it, but that doesn't happen."

After Dill launched his campaign, officials in the Silicon Valley county of Santa Clara delayed a purchase of 5,000 touch-screen voting machines. Despite insisting that their systems are reliable and secure, the nation's leading vendors all immediately agreed to provide paper receipts, and the California secretary of state announced a task force to review the security concerns. A month ago, Santa Clara went ahead with its $20 million purchase, insisting that receipts be provided once the state approves the new equipment.

Georgia and Maryland officials said that providing paper receipts may create more problems than it solves -- that paper would have to be transported and monitored with security, and printers could jam. Cramer of Sequoia said paper is unnecessary, costly and may pose a problem for blind voters.

But if customers want receipts, he said, his company will supply them. And Williams said receipts may have a place in the system. "The advantage of a hard piece of paper -- one that a voter would hold in his hand and say, 'That is who I voted for' -- that is psychological, and there certainly is value to that. We need public confidence in our elections," he said.

Similarly, the official overseeing Maryland's program would accept paper if it were available.

"I've been doing voting systems for 15 years," Torre said. "I don't care if they give voters a piece of paper or not. If they come out with a receipt, that's fine. Maybe with the momentum out of California, we'll have receipts before too long."