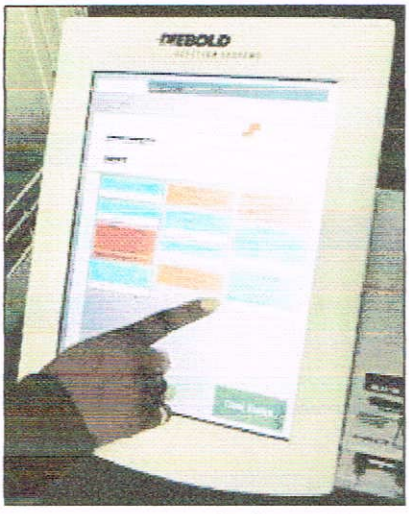
Science



Jim Ruymen / Reuters

Sparks fly in e-voting debate

Researchers face off over security issues

An electronic voting machine is demonstrated at the Registrars-Recorder/County Clerk's headquarters in Norwalk, Calif. The machines have stirred up a controversy over computer security.

By Alan Boyle
Science editor
MSNBC
Updated: 7:58 p.m. ET Feb. 16, 2004

SEATTLE - Researchers argued the pros and cons of electronic voting this weekend with the fervor of candidates on the campaign trail — but agreed on at least one point: This year's presidential balloting has the potential to suffer more glitches than the infamous 2000 election.

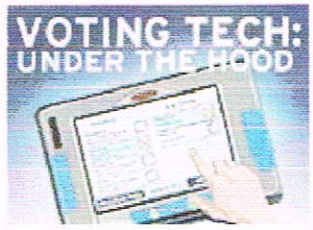
The e-voting debate has been simmering ever since the flaws in Florida's punch-card voting system brought the term "hanging chad" into the American political vocabulary. Hundreds of millions of dollars have been spent since then to upgrade voting systems, with much of that going to paperless e-voting systems. A study released last week by Election Data Services indicates that 50 million voters, 28 percent of the projected voting population, will use such e-voting systems in 2004 — more than double the number in 2000.

Alan Boyle
Science editor

- Click for profile
- E-mail the author

INTERACTIVE

Meanwhile, computer security experts and activists have been sounding the alarm about the vulnerability of e-voting systems, warning that hackers could perpetrate wholesale fraud. The annual meeting of the American Association for the Advancement of Science, which concluded Monday in Seattle, provided a rare opportunity for the top supporters and critics of e-voting to state their case in a scientific forum.



E-voting indictment

The case against e-voting was laid out by Stanford University's David Dill and SRI International's Peter Neumann, computer scientists who have documented security gaps and glitches in the systems and posted their results online at VerifiedVoting.org and SRI's Computer Science Laboratory.

Their view is that the current generation of software running the e-voting terminals cannot be made secure against tampering -- either by insiders or computer-savvy outsiders — and that such tampering could well go undetected.

"If you think I sound negative here, you don't understand how difficult it is to build secure computer systems," Neumann said at a Sunday symposium. "In some sense, the electronic voting problem is the paradigmatic 'hard problem.'"

For now, they say, the only solution is to go to a system that uses electronic terminals or other means to mark on paper ballots. These ballots, rather than the electronic tally, would be the votes that actually counted — and would provide a verifiable paper trail if there were any question about the result.

"I would immediately stop using these (e-voting) machines and use paper systems until they can be trusted," Dill told journalists at a Saturday briefing. Florida election officials may have looked silly in 2000 as they scrutinized individual punch cards for hanging chads, but at least they had something to review.

"I think we can learn a lot of wrong lessons from 2000. ... What I'm most worried about is having an election where no one can be sure the totals are anywhere close" to the actual votes cast, Dill said.

E-voting defense

The specialists on the other side of the debate acknowledged that today's e-voting systems have problems — but argued that today's paper-based systems had even more serious problems.

"I'm very frightened about paper," said Ted Selker, a computer

MORE ON E-VOTING

- Will high-tech save or sink future elections?
- E-voting flaws risk ballot fraud
- Pentagon launches e-voting effort
- E-voting firm reports computer break-in
- Should Pentagon end experiment?
- Maryland e-voting system criticized
- Pentagon cancels Net voting test
- Your views on e-voting
- More views on Internet voting

scientist at the Massachusetts Institute of Technology who specializes in user interfaces. Selker was one of the researchers in charge of the Caltech-MIT Voter Technology Project, which analyzed the shortcomings of ballot systems in the wake of the 2000 elections.

The project concluded that up to 6 million votes were lost in the 2000 election, including up to 2 million due to poor ballot designs such as Florida's infamous "butterfly ballot," up to 3 million due to outdated registration rolls and up to 1 million due to polling place operations that made voting too inconvenient.

Selker said the outlook was no better for this November's elections: "There's no systematic improvement in polling place practices and education. ... There's no improvement in ballot design."

He said the debate over e-voting was taking attention away from the voter registration "mess" and potential abuses associated with absentee voting. "I happen to believe that there are more problems with absentee balloting than all these other things put together," Selker said.

In an effort to turn the tables on the issue of ballot security, Selker noted that paper ballots could be lost, changed, misread or added to. During his visits to Chicago polling places, he noted frequent instances of lax security.

"In the 60 precincts I went to, only four of the ballot boxes were locked," he said.

To address the concerns raised by e-voting's critics, many election officials were rushing to add printers to their electronic systems — and Selker worried that such hybrid systems have not been adequately tested. Under the strain of a real-world election, the printers could jam up, or produce smudged printouts, or overload the system with multi-page ballot printouts.

Selker also proposed a scenario for a "paper-hacking" attack, in which an insider programs the election software to make some of the markings on just some of the printouts subtly unreadable by a counting machine. If the insider is backing Candidate X over Candidate Y, such an operation could hold down the vote in precincts where Candidate Y was favored.

The tone of the debate, particularly during Saturday's briefing, was civil but sharp, punctuated by the occasional "That's not true!" or "Let me finish!"

Both sides agreed that trustworthiness was an important factor for voting systems, and that the current systems were not worthy of trust. "Just as you don't trust computers, Peter, I don't trust people," Selker told Neumann on Sunday.

Looking ahead

Could ballot machines be made more trustworthy? Both sides say it's not acceptable to give voters a paper ATM-style receipt that could be taken out of the polling place, because that would open the door to coercion and vote-buying on a massive scale.

Selker noted that in Brazil, electronic voting has actually earned more trust than previous voting methods, in large part because multiple players were involved in designing and implementing the system. He said he was currently working on a project called Secure Architecture for Voting Electronically, or SAVE, that would build redundancy into the e-voting process to make it less less vulnerable to tampering. (A PDF file describes the SAVE approach.)

Some researchers and companies are working on cryptographic systems that would give voters a secret code they could check against a database. Such a code could let the voter verify that their vote has been counted correctly, while stopping short of proving to someone else that the vote had been cast in a particular way.

"It would be very good if there would be cryptographic checksums on these things," Neumann acknowledged. But he still had his doubts that any system could be made sufficiently secure against computer attacks.

Andy Neff, chief scientist for VoteHere, described his company's efforts to come up with a paperless vote-verification system that uses cryptography. VoteHere — which is based in Bellevue, Wash., and recently reported a computer hack attack — has told activists that it will make the source code for its verification software public.

On Sunday, Neff told MSNBC.com the public release was probably "a matter of weeks away, not months away." Neff and VoteHere's executive vice president, Kevin Brown, said the company was giving the code its final polish and working out the procedure for the release.

"We want to be sure we're dressed right for the prom," Neff said.

MORE FROM SCIENCE

Next →