ScienceNews
MAGAZINE OF THE SOCIETY FOR SCIENCE & THE PUBLIC
http://www.sciencenews.org/view/feature/id/7911

Ballot Roulette

Computer scientists and mathematicians look for better ways to vote

By Peter Weiss
November 4th, 2006; Vol.170 #19 (p. 298)

ENLARGE

As voters and election officials grapple with new technologies, such as these touch-screen voting machines in Cook County, Ill., scientists are uncovering evidence of flaws in some of the latest gadgetry and seeking ways to improve voting systems.
Getty Images

Two months ago, in primaries for governor and congressional and state legislative seats in Maryland, many trips to the polls became painful experiences. At hundreds of precincts in Montgomery County, for instance, new touch-screen voting machines sat useless for lack of plastic authorization cards needed to operate them. In many polling places, electronic poll books with lists of eligible voters froze or mistakenly claimed that new arrivals had already cast their ballots.

Maryland governor Robert L. Ehrlich Jr. has called for a return to paper ballots and is urging voters statewide to cast paper absentee ballots for next week's general election to avoid the computerized machines in polling places.

In Illinois in March, hundreds of precincts in Cook County reported difficulties with their electronic-voting systems. Snafus with electronic systems have also plagued contests this year in Iowa and Arkansas, not to mention the 2004 election, in which problems with electronic machines occurred in Ohio, North Carolina, Florida, and other states.

The technologies that underlie the U.S. voting system have undergone a huge change in the past 6 years. According to the Washington, D.C.–based Election Data Services, a company that

tracks voting-machine trends, the percentage of citizens using computerized-voting machines has climbed from roughly 12 percent in 2000 to an expected 38 percent in this Tuesday's election.

Although the machines have gotten a bad rap, human foibles contributed to the recent problems, and the electronic systems are in some ways an improvement over older technology. But whether they are the best option remains to be seen, and the search for the most practical and secure voting technology goes on.

"Five to 10 years ago, computer scientists weren't paying attention" to the technology used in voting, notes computer scientist David A. Wagner of the University of California, Berkeley.

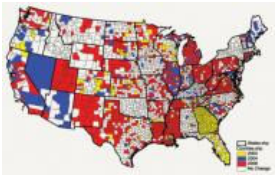
However, newly aware of the stakes, risks, and intellectual challenges associated with voting equipment, computer scientists and mathematicians specializing in encryption are now avidly taking part in the search for dependable and inviolable voting technology. These researchers are investigating existing systems, devising ways to improve them, and inventing entirely new approaches.

"In the long term, the goal is to ... make a voting system that's more reliable and secure than what we have now or have ever had. I think that's a very feasible goal," says computer-security specialist Edward W. Felten of Princeton University.

Open sesame

The technological transformation now under way in polling places has its roots back in 2000. That's when the close and pivotal presidential vote in Florida focused national attention on voting-system flaws. Those flaws included technological ones, such as confusing ballot layouts and balky punch-card ballots (remember "butterfly ballots" and "hanging chads") that made many voters' intentions uncertain.

Identifying



ENLARGE

FLECKS OF FLUX. Change in voting technology has swept the United States since 2000, albeit unevenly. Counties shown in yellow switched to new voting equipment in 2002, blue in 2004, and red in 2006. Counties in white have not changed.
Election Data Services

the 2000 election debacle as partly a technology failure, Congress in 2002 passed the Help America Vote Act (HAVA), which pledged $3.9 billion to the states for modern voting equipment, voter education,

and other election reforms. Under HAVA, many electoral districts across the country have purchased electronic-voting machines to replace punch-card equipment and mechanical voting machines. The electronic machines typically either scan a paper ballot that was marked by hand or record voters' selections made by means of buttons, a dial, or a touch screen.

The latter class of devices, known as direct-recording-electronic (DRE) machines, is the newer of the two electronic approaches and the one that's attracted the most criticism for reliability problems. But operational breakdowns aren't the only cause for concern. Several analyses dating back to 2003 have identified security vulnerabilities in DREs that could allow an attacker to secretly alter vote tallies or disrupt polling. Because the machines weren't designed to produce a paper record of votes, many voting activists have fretted that a recount after a security breach would be impossible. In the past 3 years, however, more than 20 states have adopted rules requiring that DREs print a record of each person's vote.

Except for their voting software and a few other modifications, DREs differ little from everyday personal computers. Researchers familiar with the vulnerabilities of ordinary computers say they've found insecure aspects of touch-screen voting machines made by Diebold Election Systems of Allen, Texas. The company's DREs will be the most widely used electronic machines in this Tuesday's contests. Investigators have uncovered evidence, for instance, of inadequate protections of vote tallies and other data, opportunities for tampering with authorization cards or other features of the system, and easy-to-defeat physical barriers, such as locks and cladding that covers critical hardware.

A 2003 security analysis of DREs made by the top four vendors —Diebold, Election Systems and Software, Hart InterCivic, and Sequoia Voting Systems—found security flaws in all the machines reviewed. Compuware Corp. of Detroit conducted that study for Ohio.

In one of the most recent studies of Diebold machines, a team of Princeton University computer security experts installed a computer program that boosts the tally of one candidate at the expense of his or her opponents. The researchers introduced the vote-stealing software into a machine in their lab by means of a memory card that polling officials routinely insert and remove during their duties. Because poll workers using the Diebold machines monitor only the total number of people voting—which the tampering doesn't alter—the monkey business could go undetected, Felten says.

In the same study, Felten, Ariel J. Feldman, and J. Alex Halderman, all of Princeton, made a computer virus that can reside on the memory card, install itself along with the vote-stealing software in whatever machine the card is inserted into, and then later infect any new, uninfected memory card that gets plugged in. "Because cards

are transferred between machines during vote counting and administrative activities, the infected population will grow over time," the team reports in a preprint, made available on the Internet (http://itpolicy.princeton.edu/voting/).

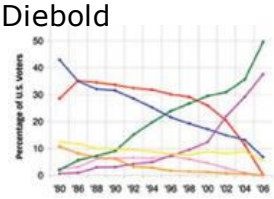
While the possibility of a voting machine virus had been hypothesized by other researchers, the new study shows that the threat is real, comments computer scientist Douglas W. Jones of the University of Iowa in Iowa City. "It's a demonstration that needed doing," he adds.

The Princeton findings—and those of previous analyses of Diebold machines—may have implications for other brands of DREs, Felten says. "Similar products designed against similar engineering problems tend to fail in similar ways," he says.

Fortunately, there's no firm evidence so far that hackers or other miscreants have exploited the vulnerabilities that computer scientists have identified.

Representatives of Diebold, one of the vendors most under fire for security weaknesses, contend that the company has tightened security of its machines in response to earlier findings. However, director of marketing Mark Radke dismisses the new Princeton report as "unrealistic and inaccurate." Additional protections given the machines by election districts, but downplayed in the report—such as physically sealing card slots and election officials' keeping an eye on machines—would prevent the kind of tampering described in the study, he contends.

Diebold



ENLARGE

OUT WITH THE OLD. Voting by punch cards (red line) and levers (blue line) has dropped sharply in recent years. In the meantime, the use of optical scanners (green line) and computerized devices (magenta line) such as touch screens has soared.
Election Data Services

also points to a 2005 academic study indicating that DREs, compared with older methods, substantially reduce numbers of spoiled ballots that can't be counted (http://vote.caltech.edu/media/documents /wps/vtp_wp25.pdf).

Brainstorms

While some researchers probe for flaws in specific voting machines, others are tinkering with ways to make electronic voting work better.

At a voting-technology meeting in Vancouver, British Columbia in August, a research team including Wagner suggested a way to reduce the complexity of the programs used in touch-screen devices. These simpler computer-based voting systems would be more reliable and easier to scrutinize for tampering than those used today, Wagner says.

In conventional DREs, the computer tailors the ballot on its screen to each voter according to, say, that person's party affiliation in a primary or to special needs such as a foreign language.

In the new proposal, Wagner and his colleagues suggest a different procedure in which election officials mock up in advance all the possible ballot screens, including where a voter's finger will need to touch to register a choice. On Election Day, the computerized voting machine simply displays the screens and records voters' responses.

"The trick is, we do all the heavy lifting before the election," Wagner says.

The team's prototype user interface required a mere 293 lines of programming instructions. By contrast, the Diebold AccuVote TS machine contains some 14,000 lines of user-interface code, although that software includes an audio interface for visually impaired voters and other functions not present in the prototype, acknowledge Wagner, Ka-Ping Yee, and Marti Hearst, all of the University of California, Berkeley, and Steven M. Bellovin of Columbia University.

Thinking outside the box of the electronic-voting machine itself, another team at the Vancouver meeting proposed a simple way to boost security of an election district's central computers.

Election administrators typically upload tallies from those computers to the Web for the public to see, notes Iowa's Jones. That practice may open them to attack from computer hackers prowling cyberspace. "If [attackers] infiltrated your system and put in software that can be switched on and off somehow, [incoming] messages as simple as 1 bit are a threat," Jones notes.

With just $20 worth of electronic parts, Jones and Tom C. Bowersox, an Iowa computer science undergraduate, created a device that halts any such incoming messages, allowing data to flow only from the secure election computers to the outside.

Their invention is a takeoff on a one-way valve called a data diode, which typically keeps data from flowing out of a secure computing system.

"Security [of computer systems] is complicated, and usually you wait until you get burned," says Jones. "I don't want to get burned on democracy."

From the crypt

Taking another, very different, approach to modern election problems, a small cadre of scientists has been researching novel balloting schemes that rely primarily on clever math. In the past couple of years, several teams have devised ways to combine the high-level formulas of cryptography with paper ballots.

Unlike voting systems in use today, these schemes would give voters a way to check that their votes were recorded as marked. They would also provide observers—such as political parties and voting-advocacy groups—a means to test the accuracy of the vote tallying as it takes place, all without violating voter privacy, says computer scientist Ben Adida of Harvard University.

He and Ronald L. Rivest of the Massachusetts Institute of Technology (MIT) recently devised one such cryptographic voting approach, called Scratch & Vote. Adida presented the new scheme at an Oct. 30 conference called "Workshop on Privacy in the Electronic Society."

Scratch & Vote and some new cryptographic approaches like it use a perforated ballot with voting boxes on one half and candidates' names—printed in varying order from ballot to ballot—on the other. After marking a ballot, each voter detaches and shreds the portion with the printed candidate names. The voter then feeds the marked portion, which includes an encrypted version of the names and their order, through an optical scanner to record the vote in the election system. That portion, which the voter keeps as a paper receipt, doesn't reveal the voter's choices but does provide an indelible record of the voter's ballot.

A major issue for cryptographic schemes is that the encrypted information must truly represent the order of selections on a given ballot, Adida notes. That's where the scratch part of his and Rivest's scheme comes in. Each ballot has a scratch foil like that of a lottery ticket, which voters can scrape away to verify that the codes are correct.

After voting, citizens can also look on the election district's Web site and confirm that their ballots were scanned. Moreover, because all the encrypted votes are posted on the Web with no violation of their secrecy, outsiders have a way to independently perform tallies on the encrypted data, Adida explains.

Because the cryptographic systems are so transparent, they "achieve a class of verification that's really far superior to current systems," he says.

Another new cryptographic scheme, called Punchscan, uses scannable ballots with two separable layers that are marked by voters with ink daubers like those used in bingo games. Unlike Scratch & Vote, a Punchscan election would allow voters to keep either layer of the ballot while destroying the other. But neither half on its own includes enough information to reveal a voter's choices.

Punchscan's inventors, who include independent cryptography consultant David Chaum, have created an interactive tutorial on the Web about the method (http://punchscan.org/learnmore.php).

Computer scientists Stefan Popoveniuc and Ben Hosp, both of George Washington University in Washington, D.C., also posted a preprint of a scientific paper explaining the system on Sept. 3 on the same Web site.

Although most cryptographic schemes have remained within the small community of cryptography specialists, a Bellevue, Wash.–based company called VoteHere has developed a commercial device that connects to conventional voting machines such as DREs and prints encrypted vote receipts.

Still, cryptography remains out of the mainstream of voting technologies. That may change, however, given a recent push by cryptographers to redesign their systems and bring them to public attention.

If the effort succeeds, it would be in keeping with a broader trend since 2000 toward a sounder scientific foundation for voting technology.

Today, the California Institute of Technology and MIT run a joint institute devoted to voting technology. Other universities participate in ACCURATE, a research collaboration on the topic. For the past 2 years, the National Institute of Standards and Technology has been developing voting-technology guidelines and is now preparing a program to certify testing laboratories for voting equipment.

Although most voters may never decide how to vote by a process anyone might describe as scientific, the means by which votes are cast and counted may be heading in that direction.

SUGGESTED READING :

For information about the Caltech/NMIT Voting Technology Project, go to .Klarreich, E. 2002. Election selection. Science News 162(Nov. 2):280-282. Available at .Peterson, I. 1993. Making votes count. Science News 144(Oct. 30):282-283.The ACCURATE Center has a Web site at .For the Election Data Services Web site, go to .For further information about the Punchscan system, go to .

CITATIONS & REFERENCES :

Ben AdidaHarvard UniversityDivision of Engineering and Applied SciencesCRCSCambridge, MA 02138Steven M. Bellovin454 Computer Science BuildingDepartment of Computer ScienceColumbia University1214 Amsterdam AvenueMailstop Code 0401New York, NY 10027-7003Tom C. BowersoxDepartment of Computer ScienceUniversity of IowaIowa City, IA 52242Ariel J. FeldmanDepartment of Computer SciencePrinceton University35 Olden StreetPrinceton, NJ 08544Edward W. FeltenDepartment of Computer SciencePrinceton University35 Olden StreetPrinceton, NJ 08544J. Alex

HaldermanDepartment of Computer SciencePrinceton University35 Olden StreetPrinceton, NJ 08544Marti HearstSchool of Information102 South HallUniversity of California, BerkeleyBerkeley, CA 94720-4600Douglas W. JonesDepartment of Computer ScienceUniversity of IowaIowa City, IA 52242Mark RadkeDiebold Election Systems1253 Allen Station ParkwayAllen, TX 75002Ronald L. RivestCSAIL, MIT32 Vassar StreetCambridge, MA 02139VoteHerePacific Plaza155 108th Avenue, NESuite 650Bellevue, WA 98004David WagnerEECS Computer Science DivisionUniversity of California, BerkeleyBerkeley, CA 94720-1776Ka-Ping YeeUniversity of California, BerkeleyElectrical Engineering and Computer Sciences387 Soda HallBerkeley, CA 94720-1776