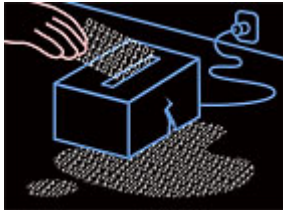


TECHNOLOGY ADVICE YOU CAN TRUST

PC WORLD



voting machines most pressing questions about ballot box security.

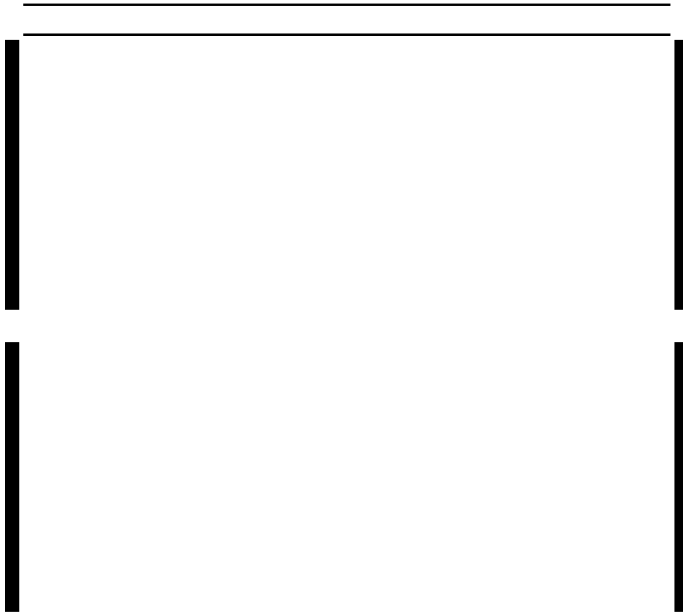
Paul Boutin

From the June 2004 issue of PC World magazine
Posted Wednesday, April 28, 2004

With the presidential election less than six months away, election officials are other paper-related problems that plagued the 2000 contest. New touch-screen machines have already been deployed in 27 states.

But as the California primary proved in March, such e-voting systems have

Diego from opening on time. Orange County poll workers unfamiliar with the system gave voters ballots for the wrong districts, invalidating 7000 votes. As a result, the state's election committee leaders asked California's secretary of state to decertify paperless touch-screen machines so that they can't be used in November's general election.



Ready or not, new touch-screen voting machines will be in thousands of voting booths this fall. The federal Help America Vote Act of 2002 supplied nearly \$4 billion in funding to replace punch-card and lever machines, but mandated that states receiving the funds must replace those machines by this November.

The aging machines' error rates--aggravated by their inability to clearly log the voter's intent (Florida's notorious "hanging chad" problem)--are so high that in 2000 the number of votes

separating Bush and Gore was less than the margin of error in the count. But according to MIT professor Ted Selker, cochair of the Caltech-MIT Voting Technology Project, touch-screen replacements aren't faring better than paper-based systems.

Many voters are wondering if they should be worried about the coming election. Unfortunately, the answer is yes, though not for the reasons you might think. Most experts agree that it's highly unlikely a hacker could walk into a polling place and throw an election. But the electronic nature of the new voting machines, combined with their lack of a physical audit trail for each vote, leaves a hole that crooks with inside access could exploit.

We've taken a look at the technology behind voting machines to show you how they work and to answer your questions about the specialized computers you may encounter in the booth this fall.

The Technology

How does e-voting work?

See "[E-Voting Step-By-Step](#)" for a detailed walk-through of voting with Election Systems & Software's IVotronic system. Most e-voting machines use similar procedures, with variations in the secure media used to activate the machines and the procedures for retrieving votes. All e-voting machines include backup batteries, so they can run for a few hours during a power outage. Votes stay in nonvolatile RAM, so they aren't lost if the batteries die. See "[E-Voting Machine Spec Check](#)" for information on the guts of different machines.

Advertisement

machines.

Do these machines connect to the Net?

No. The booth machines operate independently, or connect only to a local election judge's workstation. They lack the hardware to connect to the Net.

To report results, most systems collect votes onto one voting machine or PC at the polling place. That machine then dials in to a PC at election headquarters and transfers that precinct's tallies over an encrypted modem-to-modem connection. Later, poll workers deliver the memory cards along with a printout of the results.

The PCs used to collect and transmit results aren't supposed to be connected to the Internet while tallying results.

What about my privacy? Is my vote being tied to my name?

No. Anonymity is an important design factor in e-voting systems to prevent bribery or intimidation. Unfortunately, guaranteeing anonymity also makes it harder to track election fraud and errors.

What's so great about e-voting?

Most important, touch-screen systems can reduce several common mistakes voters make in the booth. They provide immediate feedback on your vote, helping to ensure that you don't vote for too many candidates in a race, forget to vote on an issue, or enter an unintended vote because you misread the interface.

E-voting terminals can be more convenient than paper systems as well. When equipped with headphones and a Braille keypad, touch-screen machines let sight-impaired voters cast their votes without needing to share their choices with a human aide. Officials don't need to supply paper ballots in different languages--voters select the language as a menu option. Results can be transmitted to election headquarters in seconds, and recounts are a snap since each vote is unambiguously stored in memory.

The people who run elections love the machines, says Hugh Gallagher, an independent consultant to state and local election committees nationwide. "If you got a couple of these registrars over a cup of coffee, they'd tell you it is a pain [to deal with paper ballots]," he says. "People put boxes of ballots on top of their car at the end of the day and drive off. You end up out on the freeway with the local sheriff, picking up ballots off the road."

Voters like them too, as e-voting skeptic Avi Rubin, a Johns Hopkins professor who coauthored a scathing review of the machines' potential security holes last year, discovered when he volunteered as an election judge at a Maryland district in March. Rubin reported his experience online (see "[My Experience as an Election Judge in Baltimore County](#)") and was struck by the popular

[an Election Judge in Baltimore County](#)") and was struck by the popular enthusiasm for the same Diebold machines that his report had blasted. "With very few exceptions, the voters really loved the machines," he wrote. "The most common comment was, 'That was so easy.'"

The Problems

What about e-voting machines makes people so nervous?

To many experts like Rubin, the machines' biggest vulnerability is simple: There's no way for a voter to know what the machine records when they cast their vote and no voter-verified physical record available for recounts. If the software goes awry or is tricked into flipping votes, no one will be able to tell as long as the total ballot count stays the same.

What types of problems have occurred?

The November 2003 election in Fairfax County, Virginia, was a showcase for e-voting bugs. When polls closed at 7 p.m., many of the county's 223 precincts tried to transmit their results to the election center at once, tying up the line for hours. Many precinct judges gave up and drove their tallies to headquarters. A software problem delayed some results for 21 hours. Voters claimed that some of the booth machines crashed and had deleted some votes before their eyes. Election officials repaired ten broken machines off-site, with vote data inside, then returned them to service--a violation of state law.

Wasn't the software on these machines certified before the election?

Yes. But according to Harvard research fellow Rebecca Mercuri, a computer scientist who has worked elections for two decades, the certification tests look for logic errors and vote-counting mistakes, not security holes. Much of the testing is automated, and layers beneath the voting applications--compilers, OSs, firmware on the machines' chips--are not examined. Technically, she says, "The certification process is a joke." What's more, voting machine vendors have distributed uncertified code upgrades to their machines after the certification process was complete, but before an election.

Is e-voting more or less error-prone than other methods of voting?

The Caltech-MIT Voting Technology Project was established in December 2000 to study voting machine reliability and generate guidelines for future voting systems. The project's 2001 report--still considered the definitive study of machine accuracy--found that in elections from 1988 to 2000, touch-screen (also called DRE, for direct record electronic) machines fared worse than paper ballots in many cases (see the [project's report here](#)). But generally, their margin of "residual votes"--those thrown out because of error--was within the range of other voting technologies. In presidential elections, for example, punch-card machines had the highest percentage of residual votes, at 2.5 percent. Touch-screen voting machines were slightly better, at 2.3



at 2.5 percent. Touch-screen voting machines were slightly better, at 2.3 percent, and optically scanned paper ballots worked best, at 1.5 percent.

Why such mediocre results from a supposedly better technology?

Voting Project cochair Ted Selker (pictured in photo) says, "[DREs are] not doing as well as they should because people aren't familiar with them yet. The people who create the ballots don't have enough experience."

The wizard-based PC software election officials use to design ballots can't guarantee good design. For example, in one midwestern precinct, a button allowed voters to vote a straight Democratic or Republican Party ticket. But many voters touched the already-checked buttons for their candidates on subsequent screens, which removed their votes instead of confirming them. Other ballots placed a "next screen" button near a button to cast the ballot and exit, which could have caused voters to prematurely end their voting.

Where does e-voting break down?

Closed source code: According to Rubin, "The biggest potential [for election fraud] is when the original code is being written." Mercuri, Rubin, and Selker agree: Since the public can't inspect the code these machines run, a programmer who's been bribed or threatened, or a manufacturer willing to rig an election, would have the best chance to hack the vote. And while open-sourcing the code of e-voting machines (as the Australian Capital Territory did in its 2001 e-voting pilot program) would help fix security holes and put people's minds at ease, it's not a panacea (see "[Is Open Source the Answer?](#)").

Poorly implemented security: Independent consulting firm RABA Technologies audited the Diebold machines used in Rubin's Maryland precinct during a simulated vote. They found ample holes for hackers who could get time alone with the machines. One tester was able to pick the physical locks securing the PCMCIA flash memory card that stores the votes in about 10 seconds and gained access to a keyboard port. By attaching a standard keyboard to the voting machine, RABA's team was able to invoke supervisory functions that let them overwrite election results without leaving a trace.

But pulling off any of those hacks without some type of inside access to the voting machines would be extremely difficult. Rubin, whose 2003 report made the machines sound like Swiss cheese, told *PC World* that his experience at the polls changed his mind: "I'm becoming more and more convinced that the risks of a voter walking in off the street and throwing the whole election are pretty small."

PCs in the mix: Most touch-screen systems run proprietary operating systems in the booths, though Diebold's machines run on Windows CE. But nearly all systems collect votes on PCs at election headquarters. The PC in the system RABA evaluated hadn't gotten the latest Microsoft security upgrades

system RABA evaluated hadn't gotten the latest Microsoft security upgrades, which left it vulnerable to the Blaster worm and other viruses should it be connected to the Net.

The Paper Fix

Will paper receipts fix these problems?

Yes and no. The biggest danger of touch-screen machines is that if votes are lost or changed, no voter-verified audit trail is available for a recount, and the evidence of tampering could also be erased. To close that hole, California and several other states have mandated that touch-screen machines produce a printed receipt at the end of each voter's session. That printout will be secured behind a transparent screen, so the voter can't take it or alter it. If the voter accepts the vote as printed, it gets dumped into a secure container for storage. Or the voter can reject the printout and start over.

The Caltech-MIT project has stated there may be a way to design a reliable paperless audit system that's more reliable than a printout, but none exists yet.

Will voting machines have a printed receipt by this November?

Most won't. New equipment must be certified by the Federal Election Commission or by state officials before it can be sold. Most counties and states won't have paper-trail touch screens until 2005 or 2006, though Nevada expects to have them for a third of its voters this fall.

Why don't we forget touch screens and use optically scanned paper ballots?

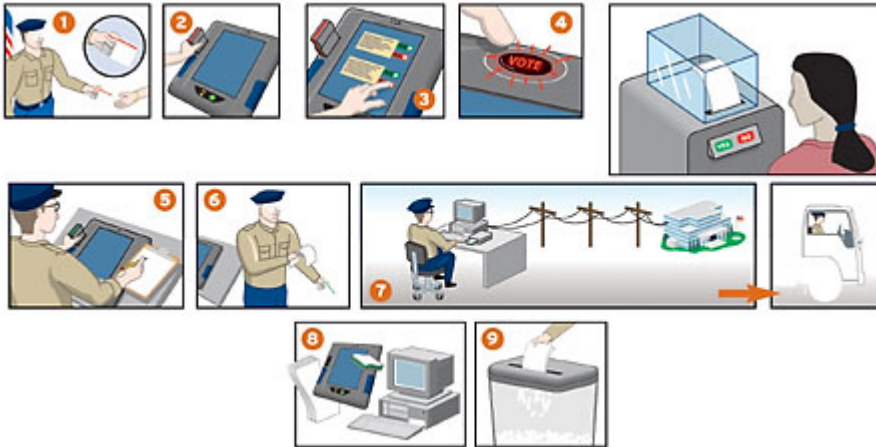
True, ballots optically scanned at precinct headquarters have the lowest margin of error, and they already create a paper trail. But those ballots can still be misread, and they don't meet the accessibility requirements of the Americans with Disabilities Act without add-on equipment.

What's going to happen in November?

Expect problems with the new machines--mostly because they're new and people aren't used to them yet. Mike Alvarez, Caltech's cochair of the Voting Technology Project, says that "any jurisdictions that have made substantial changes to their voting systems are the places where the most problems are likely to occur." But that applies to adding paper-trail technology, too.

It's a safe bet that, whoever wins, supporters for a losing candidate will claim the paperless machines miscounted votes en masse. Expect to see challenges and lawsuits. Even if the machines work flawlessly, it'll be hard to prove that to a skeptical public that views a paper printout as the only credible form of audit trail.

How it Works: E-Voting Step-by-Step Using the ES&S IVotronic



1. A poll worker hands you a Personal Electronic Ballot that contains a chip storing the ballot you need. Machines by other companies put the ballot on a smart card.

2. You take the PEB to a voting booth and slide it into a slot in an IVotronic machine, activating it for voting.

3. The IVotronic steps you through the electronic ballot, letting you make your choices in each race and review your votes.

4. You press the big red Vote button, storing your votes in triplicate in the IVotronic's internal NVRAM (Non-Volatile Random Access Memory) banks.

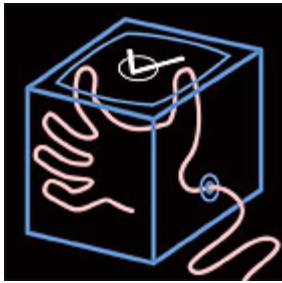
Many states will require a voter-verified paper trail in future elections. You'll look at a printout of your vote behind a glass or plastic barrier; then you'll press a button to accept it, or reject it and start over.

5. Every hour or so, election judges manually add the totals from each machine to make sure the number of votes matches the number of voters who have come in.

6. At the close of polls, election judges print out final tallies from each machine and load them into a master PEB unit.

7. Election judges post a printout of the local results, transmit them to a special PC at election headquarters over an encrypted telephone line, and later deliver the master PEB and printouts in person.

8. In case of a recount or dispute, your vote is stored in several places: in triplicate on the voting machine, on the printout from the voting machine, on the master PEB, and on computers at your local precinct and at election headquarters.



headquarters.

9. All records are destroyed according to state or local law after a specified number of days. Destruction is the final security check--it prevents the vote from being tampered with while it's in

Security Holes: How to Hack an E-lection

Experts who have studied electronic voting say there are several ways determined criminals could hack the vote.

Inside Job: Employees at a voting machine maker insert vote-rigging code into a software release before shipping it. When the election starts, votes flip from one candidate to a rival. It's the most paranoid of scenarios, but also the most likely to succeed.

Wiretap: A hacker intercepts the encrypted calls from each precinct into the election center PC and phones in his own results to headquarters. Winners are announced, and then officials discover the local smart card tallies don't match. Panic!

The Paper Caper: E-voting proponents claim that voter-verified printouts will prevent ballot box skulduggery. Oh yeah? Hackers could rig the system to flip a small percentage of votes and allow the machine to print out the switched vote. In their haste to leave, many voters either won't notice or won't bother to revote.

On the Inside: E-Voting Machine Spec Check

Most (85 percent) of the e-voting machines that will be used this November are built by one of three companies: Diebold Election Systems, Election Systems & Software, and Sequoia Voting Systems. Here's what the machines are made of.

Diebold Accuvote-TS

- 400-MHz Intel PXA-255 CPU
- Windows CE
- 64MB of flash memory
- Removable 32MB-128MB PCMCIA smart card for vote storage
- 9-by-12-inch touch screen



ES&S IVotronic

- 25-MHz Intel 386EX CPU
- Proprietary OS
- Three 2MB NVRAM audit log and image storage caches
- Removable NVRAM or 16MB-196MB CompactFlash for vote storage
-

Sequoia Voting Systems

- National Semiconductor Geode CPU (300-MHz Pentium equivalent)
- 32MB (or greater) CompactFlash
- Removable 128MB (or greater) PCMCIA card for vote storage
- 9-by-12-inch touch screen

Is Open Source the Answer?

If voters don't trust paperless machines to do what they're supposed to,

officials for the Australian Capital Territory (the southeastern region of the country that includes Canberra) designed a Linux-based voting machine, posted the code for public review, and then hired local vendor Software Improvements to build the machines, which were tested at 10 percent of polling places in ACT's 2001 regional election.

The diskless machines run on 386 or higher PC hardware and connect to a

Eric Raymond, president of the Open Source Initiative, says open-sourcing

that "there is no foolproof protection against bugs and hacks." For example, insiders could still replace the code loaded onto the machines.

Does the open-source approach work? Deputy Electoral Commissioner Alison

source, but "those voters and political participants that do know about open source have commented very favorably about this aspect." More important, techies aren't shouting that the machines are an unknown risk. As a result, Aussie voters haven't demanded a paper audit trail for the machines.

Related Topics: [Consumer-Related Legal Issues](#)