ELECTRONIC VOTING MACHINES PROMISE TO MAKE

FIXING

ELECTIONS MORE ACCURATE THAN EVER BEFORE, BUT

THE

ONLY IF CERTAIN PROBLEMS—WITH THE MACHINES

VOTE

AND THE WIDER ELECTORAL PROCESS—ARE RECTIFIED

By Ted Selker

COURTESY OF SEQUOIA VOTING SYSTEMS

Voting may seem like a simple activity—cast ballots, then count them. Complexity arises, however, because voters must be registered and votes must be recorded in secrecy, transferred securely and counted accurately. We vote rarely, so the procedure never becomes a well-practiced routine. One race between two candidates is easy. Half a dozen races, each between several candidates, and ballot measures besides—that's harder. This complex process is so vital to our democracy that problems with it are as noteworthy as engineering faults in a nuclear power plant.

Votes can be lost at every stage of the process. The infamous 2000 U.S. presidential election dramatized some very basic, yet systemic, flaws concerning who got to vote and how the votes were counted. An estimated four million to six million ballots were not counted or were prevented from being cast at all—well over 2 percent of the 150 million registered voters. This is a shockingly large number considering that the decision of which candidate would assume the most powerful office in the world came to rest on 537 ballots in Florida.

VOTING MACHINE—here, Sequoia Voting Systems's AVC Edge—is fairly typical of direct record electronic (DRE) voting machines on the market. Voters enter their votes via a touch-screen interface.

COURTESY OF SEQUOIA VOTING SYSTEMS

Three simple problems were to blame for these losses. The first, which made up the largest contribution, was from registration database errors that prevented 1.5 million to three million votes; this problem was exemplified by 80,000 names taken off the Florida lists because of a poorly designed computer algorithm. Second, a further 1.5 million to two million votes were uncountable because of equipment glitches, mostly bad ballot design. For example, the butterfly ballot of Palm Beach County confused many into voting for an unintended candidate and also contributed to another appalling outcome: 19,235 people, or 4 percent of voters, selected more than one presidential candidate. Equipment problems such as clogged punch holes resulted in an additional 682 dimpled ballots that were not counted there. Finally, according to the U.S. Census Bureau, about one million registered voters reported that polling-place difficulties such as long lines prevented them from casting a vote.

Thus, registration and polling-place troubles accounted for about two thirds of the documentable lost votes in 2000. The remaining one third were technology-related, most notably ballot design and mechanical failures. In the aftermath of the 2000 election, officials across the country, at both the federal and local levels, have scrambled to abandon old approaches, such as lever machines and punch cards, in favor of newer methods. Many are turning to electronic voting machines. Although these machines offer many advantages, we must make sure that these

new systems simplify the election process, reduce errors and eliminate fraud.

Some countries have introduced electronic systems with great success. Brazil started testing electronic voting machines in the mid-1990s and since 2000 has been using one type of machine across its vast pool of 106 million voters. It has multiple organizations responsible for different aspects of voting equipment development as part of the safeguards. It also introduced the machines in carefully controlled stages—with 40,000 voters in 1996 (7 percent of whom failed to record their votes electronically) and 150,000 in 1998 (2 percent failure). Improvements based on those experiments reduced the failure rate to an estimated 0.2 percent in 2000.

Voting Technology

VOTING SYSTEMS have a long history of advancing with technology. In ancient Greece, Egypt and Rome, marks were made for candidates on pieces of discarded pottery called ostraca. Paper superseded pottery in the hand-counted paper ballot, which is still used by 1.3 percent of U.S. voters. Other modern technologies are lever machines, punch cards and mark-sense ballots (where each candidate's name is next to an empty oval or other shape that must be marked correctly to indicate the selection, and a scanner counts the votes automatically). The table on pages 94 and 95 summarizes the benefits and drawbacks of each of these methods and suggests ways to improve them. A lengthier discussion of nonelectronic systems is at www.sciam.com/ontheweb.

Electronic voting machines have been around for 135 years—Thomas Edison patented one in 1869. Elections started testing electronic voting machines in the 1970s, when displaying and recording a ballot directly into a computer file became economical. At first, many were mixed-media machines, using paper to present the selections and buttons to record the votes. Officials had to carefully align the paper with the buttons and indicator lights. Electronic voting machines that use such paper overlays are still on the market. More modern direct record electronic (DRE) voting machines present the ballot and feedback information on an electronic display, which may be combined with audio.

Such machines have many advantages: they can stop a voter from choosing too many candidates (called overvoting), and they can warn if no candidate is picked on a race (undervoting). For instance, when Georgia changed over to DREs in 2002, residuals (the total of overvotes and undervotes combined) were reduced from among the worst in the nation at 3.2 percent on the top race in 2000 to 0.9 percent in 2002. So-called ballotless voting allows the machines to eliminate tampering with physical ballots during handling or counting. (Lever machines, dating back to 1892, share many of those features.)

Yet the birthing of DRE voting equipment in the U.S. has not been easy. The voting machine industry is fragmented, with numerous companies pursuing a variety of products and without a mature body of industry-wide standards in place. Deciding what is a good voting machine is still being discussed by various advocacy organizations and groups such as the IEEE Project 1583 on voting equipment standards. Allegations of voting companies using money to influence testing and purchasing of equipment are not uncommon.

Complicating matters, local jurisdictions across the country have different rules and approaches to testing and using voting equipment. Some counties, such as Los Angeles, are sophisticated enough that they commission voting machines built to their own specifications. Many other municipalities know so little about voting that they employ voting companies to run the election and report the results.

Polling-place practices add further hazards of insecurity and potential malfunctions. I recall walking into the central election warehouse (where the voting machines are stored and the precinct vote tallies are combined) in Broward County, Florida, when it was being used for a recount in December 2002. The building's loading dock was opened to the outdoors for ventilation. The control center for tallying all the votes was a small computer room; the door to that room was ajar and no log was kept of personnel entering and leaving.

Beyond external issues, DRE machines themselves have had technological shortcomings that have slowed their adoption. Voters have found their displays confusing or challenging to use. Software bugs and difficulties in setting up DREs have also presented problems. During the 2002 Broward County recount, I was allowed to try out machines from Electronic Systems and Services (ESS), one of the country's major election machine makers. The ESS machines had an excessive undervote because the "move to next race" button was too close to the "deposit my ballot" button. An audio ballot was so poorly designed it took about 45 minutes to vote.

On machines made by the company Sequoia, people who chose a straight party vote and then tried to select that party's presidential candidate were unaware that they were *de*selecting their presidential choice. A massive 10 percent undervote was registered in one county using Sequoia machines in New Mexico.

Examining the insides of new voting machines still reveals

Overview/*Electronic Voting*

- Following the infamous 2000 presidential election, electoral officials around the country have scrambled to upgrade their voting technology with newer systems, such as direct record electronic voting machines (DREs).
- A state or county that is considering buying DREs should hire experts to test the machines thoroughly for bugs, malicious software and security holes and to assess the quality of the user interface.
- Election officials and polling-place workers should be well versed in the operation of their machines and should follow practices that do not compromise the security of the vote.
- In addition to these technology-related issues, the voter registration process and polling-place practices in general must be improved to prevent massive losses of votes.

AUDIT TRAILS

An audit trail printed on paper or recorded on tape or CD would enable an independent recount of votes made on an electronic voting machine.

VERIVOTE PRINTER UPGRADE to Sequoia Voting Systems's AVC Edge voting machine produces a paper copy of the votes made on it and displays it behind a window. Before leaving the voting booth, the voter can verify her vote by inspecting the paper record, which is retained by the machine for use in recounts

DON FOLEY (*illustration*); COURTESY OF SEQUOIA VOTING SYSTEMS (*photograph*)

many physical security faults. For example, some machines have a lifetime electronic odometer that is supposed to read every vote that the machine makes. But the odometer is connected to the rest of the machine by a cable that a corrupt poll worker could unplug to circumvent it without breaking a seal.

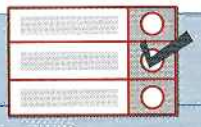
Source code for voting machines made by different companies, like most commercial software, is a trade secret. Election machine companies allow buyers to show the source code to experts under confidential terms. Unfortunately, the local election officials might not know how to find a qualified expert. And when they find one, will the voting companies be required to listen? For instance, in 1997 Iowa was considering a voting machine made by Global Election Systems, which was later bought out by Diebold. Computer scientist Douglas W. Jones of the University of Iowa pointed out security issues, and the state bought Sequoia machines instead. In February 2003 Diebold left its software on unsecured servers, and DRE critics posted Diebold's code on the Internet for everyone to see. The problems that Jones saw six years earlier had not been fixed. Any person with physical access to the machines and a moderate amount of computer knowledge could have hacked into them to produce any outcome desired.

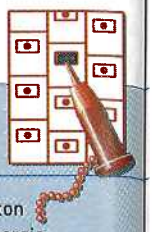
The best computer security available depends on sophisticated encryption and carefully designed protocols. Yet to know the system has not been compromised requires testing. DRE machines have not received the constant testing that they require. Security of today's voting machines is wholly dependent on election workers and the procedures that they follow.

Because virtually all tallies, no matter what voting method is used, are now stored and transmitted in some electronic form, computer fraud is possible with all voting systems. The advent of DRE machines potentially allows such tampering to go

EXISTING VOTING TECHNOLOGIES

Improving or optimizing an existing technology may be a better choice for many counties than hasty adoption of a new system—introduction of a new technology is often accompanied by an increase in errors.





TECHNOLOGY	Hand-counted paper ballots	Lever machines	Punch cards
COMMENTS	■ Used by 1.3 percent of U.S.	■ First used in 1892 in Lockport, N.Y.	■ First used in 1964 in Fulton and De Kalb counties, Georgia
ADVANTAGES	■ Simple ■ Lowest residual* rate	■ Overvotes are impossible ■ Guarantees secrecy of vote	■ Removes human errors of tallying ■ Compact machines
DISADVANTAGES	■ Recounts differ from original count by twice as much as machine-counted votes do ■ Persistent allegations of votes being altered, added, lost, and so on	■ Bulky, massive machines ■ Defective odometers common ■ Misreading of odometers ■ Voting falloff on lower races (for Senate, state office, for example)	■ Hard to punch holes correctly ■ Often punch wrong hole ■ Ballot design troubles ■ Card readers jam frequently ■ Ballot easy to spoil
WAYS TO IMPROVE	■ Count by mechanical scanner ■ Treat paper with light, heat or coating material to make vote indelible	■ Check and service before each election ■ Monitor odometers with video cameras ■ Improve labeling of groups of levers forming a race ■ Adjustable height of machines	■ Optical way to check ballot while in booth might help

unchecked from the point at which the voter attempts to cast a ballot. Schemes for altering ballots have always existed, but a computerized attack could have widespread effects were it waged on a large jurisdiction that uses one kind of software on one type of machine. Using a single system allows large jurisdictions to get organized and improve their results but must be accompanied by stringent controls.

The successful reduction of residuals across all of Georgia, mentioned earlier, is a case in point. Thorough tests on the DREs at Kenisaw State University found many problems, which were resolved before the machines were put into use. This rigorous testing and careful introduction of the machines were central to the state's success.

Electronic Fraud

HOW CAN WE FIND all the dangers created by bad software and prevent or correct them before they compromise an election? Reading source code exposes its quality and its use of security approaches and can reveal bugs. But the only completely reliable way to test software is by running it through all the possible situations that it might be faced with.

In 1983 Ken Thompson, on receipt of the Association for Computing Machinery's Turing Award (the most prestigious award in computer science), gave a lecture entitled "Reflections on Trusting Trust." In it he showed the possibility of hazards such as "Easter eggs"—pieces of code that are not visible to a reader of the program. In a voting machine, such code would do nothing until election day, when it would change how votes were recorded. Such code could be loaded into a voting machine in many ways: in the voting software itself, in the tools that assemble the software (compiler, linker and loader), or in the tools the program depends on (database, operating system scheduler, memory management and graphical-user-interface controller).

Tests must therefore be conducted to catch Easter eggs and bugs that occur only on election day. Many electronic voting machines have clocks in them that can be set forward to the day of the election to perform a test. But these clocks could be manipulated by officials to rerun an election and create bogus voting records, so a safer voting machine would not allow its clock to be set in the field. Such machines would need to be tested for Easter egg fraud on election day. In November 2003 in California a random selection of each electronic voting system was taken aside on the day of election, and careful parallel elections were conducted to show that the machines were completely accurate at recording votes. These tests demonstrated that the voting machines were working correctly.

To prepare for a fraud-free voting day requires that every effort be made to create voting machines that do not harbor malicious code. The computer science research community is constantly debating the question of how to make provably secure software. Computer security experts have devised many approaches to keep computers reliable enough for other purposes, such as financial transactions. Financial software transfers billions of dollars every day, is extensively tested and holds up well under concerted attacks. The same security techniques can be applied to voting machines. Some researchers believe that the security precautions of "open source" (making the programs available for anyone to examine) and encryption techniques can help but not completely guard against Easter eggs.

Guarding votes against being compromised has always re-

ELIZA JEWETT