Florida's voting systems were in the news again last month. A 10 September primary election marked the state's first large-scale roll-out of tens of thousands of sleek new touch-screen voting machines, the cornerstone of Florida's plan to resolve the problems of the 2000 U.S. presidential election by replacing many of their punch-card and other older machines.

The confusing butterfly ballots and hanging chads of two years ago are indeed gone. But in their place voters found touch-screen devices that didn't work properly or, in some cases, at all. A few machines in Miami-Dade County reset themselves while voters were trying to vote. Precincts in Palm Beach County reported problems activating some of the electronic cards used to authenticate the voters. Even mark-sense ballots designed to be read by optical scanners proved troublesome. In Union County many votes had to be hand-counted because the optical scanning system reported all votes as being cast for just one party's candidate.

Will the November general elections in Florida be less chaotic? To judge from these primaries—and from Palm Beach County's municipal elections in March, which had a number of electronic voting problems as well—probably not. Using the new machines, it is still possible to inadvertently cast a ballot for a candidate that the voter never intended to select. Will the results be more reliable? There will simply be no way to ever know, because the new equipment does not make an independent recount possible.

Around the globe, election officials are examining technologies to address a wide range of such voting issues. The problems observed in the November 2000 election accelerated existing trends to get rid of lever machines, punch-cards, and hand-counted paper ballots and replace them with mark-sense balloting, Internet, and automatic teller machine (ATM) kiosk-style computer-based systems [see table, p. 48]. An estimated US $2–$4 billion will be spent in the United States and Canada to update voting systems during the next decade.

It seems plausible to imagine that computerized methods for ballot casting and tabulation could alert the voter to mistakes—for example, by flagging overvoting, when more candidates are chosen than is allowed, and by reducing undervoting, when some selections are skipped. New vote-tallying systems, which count the marks made on ballots, should be faster, more accurate, and cost-effective, and better able to prevent certain types of tampering (such as ballot-box stuffing) than older products.

And voting online might enable citizens to vote even if they are unable to get to the polls. Yet making these methods work right turns out to be considerably more difficult than originally thought. As it turns out, many of the voting products currently for sale provide less accountability, poorer reliability, and greater opportunity for widespread fraud than those already in use. These problems result from an underlying fundamental conflict in the construction of electronic voting (e-voting) systems: the simultaneous need for privacy and auditability, which is the ability, when necessary, to recount the votes cast. Privacy is critical to a fair election, necessary to prevent voter coercion, intimidation, and ballot-selling. But maintaining the voter's privacy precludes the use by computer-based products of standard audit and control practices: logging transactions and identifying them from end to end. In other words, the privacy constraint directly conflicts with the ability to audit the ballot data.

For the system to work, there must be a way to backtrack vote totals from actual ballots that come from (and must be independently verified by) legitimate voters voting no more than once. In turn, the ballot must in no way identify or be traced back to the voter after it is cast. These constraints, many experts say, cannot be mutually satisfied by any fully automated system.

Such problems plague all electronic voting products, whether kiosk systems, where voters go to a polling station, or Internet-based, where voters can submit a ballot from their homes, offices, or any site connected to the global network. Unlike

New electronic voting systems pose risks as well as solutions

A Better Ballot Box?

BY REBECCA MERCURI
Bryn Mawr College
automated teller machines at banks, where videocameras are used to deter theft, receipts are issued, cash provides a physical audit mechanism, and insurance covers losses, the privacy requirement means that analogous checks and balances cannot be employed to protect ballots in e-voting systems.

Internet voting is further flawed because authentication of the voter must be performed by the same system that records the ballots, and this compounds the auditability and privacy problems.

Just verifying a person's right to vote is difficult. Civil rights groups have objected, for example, to the use of bio-identification through fingerprints and retinal scans, fearing that the data will be used for criminal investigations or other purposes. Alternative log-in mechanisms, like personal identification numbers or smart cards, are not viable since they can be easily transferred, sold, or faked. To quote cryptographer Bruce Schneier, founder of Counterpane Internet Security Inc. (Cupertino, Calif.): “A secure Internet voting system is theoretically possible, but it would be the first secure networked application ever created in the history of computers.”

Electronic voting offers fewer problems when used for such things as shareholders’ meetings, public policy initiatives, award nominations, opinion surveys, and school, club, and association elections. These systems will have different requirements for security and auditability, depending upon their use. Web-based shareholder balloting has grown in popularity despite fears of computer security experts. Peter Neu- mann, principal scientist of SRI International’s Computer Science Laboratory (Menlo Park, Calif.), is one expert who for years has warned that “the Internet is not safe for elections, due to its vast potential for disruption by viruses, denial-of-service flooding, spoofing, and other commonplace malicious interventions.” Such a problem occurred in April 2002, when the financially troubled media conglomerate, Vivendi Universal (Paris), fell victim to a hacking attack that caused the ballots of some large shareholders to be counted as abstentions. Fortunately, since shareholder balloting is not anonymous (votes must be identified with their owners during tabulation), this particular breach was detectable.

To Ensure an Accurate Ballot
The Mercuri Method allows voters to check that their votes will be recorded accurately by requiring that electronic voting machines be modified to generate paper ballots. Such a system does not exist, but could be created by machine manufacturers.

In the proposed system, a voter, Zelda, votes on a touch-screen machine.

The system records Zelda’s vote electronically, but the definitive record is a paper ballot, which the system prints and displays behind a glass or plastic panel.

Zelda reviews the printed ballot. If it does not represent her choices, she calls an election official who voids the ballot. She votes again, and once she approves the ballot, it drops into a ballot box for later tallying. Ballots may be optically scanned or hand-counted.
Despite manufacturers’ statements to the contrary, it is beyond the scope of present computer science and engineering principles to design a fully electronic, self-auditing voting system that sufficiently guarantees that all ballots are recorded and tallied in accordance with the voters’ intentions. Even so, existing systems are often viewed as an improvement by some communities, such as those in Florida or Brazil (in 2000, the first to use fully computerized balloting nationwide) that have suffered from earlier election scandals or difficulties. But reliance on this type of so-called fail-safe system design is risky, as Counterpane’s Bruce Schneier has noted: “Computerized voting machines, whether they have keyboard and screen or a touch-screen ATM-like interface, could easily make things worse. You have to trust the computer to record the votes properly, tabulate the votes properly, and keep accurate records.”

In truth, no manner of self-reporting by the voting system is sufficient to ensure that intentional tampering, equipment malfunction, or erroneous programming has not affected the election results. Neither is any examination of the system, before, during, or after the election, no matter how thorough, sufficient to assert that such problems did not exist. This is due, in part, to the inherently insoluble task of making certain that computer-based products do not contain unknown additional features.

**On the Road Toward Electronic Balloting**

Twenty years ago, three-fourths of all U.S. counties voted by paper ballot or mechanical lever machines. In 2000, fewer than a third of them used such methods. Optically scanned, mark-sense ballots had the largest share (40.2 percent of counties), with direct-recording electronic devices (8.9 percent) moving up. Punch card machines still maintained a hold (19.2 percent) but will drop off sharply.
Trade secrecy, usability, privacy, security, and other inherent computer issues result in a dangerous "trust us" mentality on the part of manufacturers

Even more risky is the fact that at least one machine’s firmware, that of the Sequoia Edge, can be reprogrammed through a port on the voting machine kiosk. Although this port is “secured” during the voting session by a flimsy, numbered, plastic tab, it is exposed after the election, providing essentially no protection against reprogramming.

E-voting products from other companies have also proved problematic. The systems involved in the 10 September voting snafus in Miami-Dade and Broward counties were from Election Systems & Software Inc. (Omaha, Neb.). Problems included machines that took three times longer than expected to boot up, that reset themselves spontaneously, and, in one precinct, that apparently failed to record about 1800 votes.

Recently, an evaluation performed by the University of Maryland on a system being considered by four Maryland counties—the AccuVote-TS touch-screen system from Diebold Election Systems Inc. (Canton, Ohio)—produced evidence of a digital divide. Individuals familiar with computers found the system easier to use than those with less computer experience. The study also revealed reliability problems during the system’s first use in an April school board election when smart cards for authenticating voters had been produced to incorrect specifications, delaying voting at some sites. Nevertheless, last May, Diebold won a $54 million contract from the state of Georgia, which plans to use the systems in all 159 counties.

Trust, but verify

The combination of the lack of standards, legislative loopholes, trade secrecy, usability problems, privacy, security, and other inherent computer issues results in a dangerous “trust us” mentality. Transparency in the process is essential, not only to provide auditability, but also to enhance voter confidence.
This can be provided, quite simply, through the use of a voter-verified physical audit trail for use in recounts.

A method of voting described by this author over a decade ago, referred to as the Mercuri Method, requires that the voting system print a paper ballot containing the selections made on the computer [see illustration, p. 47]. This ballot is then examined for correctness by the voter through a glass or screen, and deposited mechanically into a ballot box, eliminating the chance of accidental removal from the premises. If, for some reason, the paper does not match the intended choices on the computer, a poll worker can be shown the problem, the ballot can be voided, and another opportunity to vote provided.

At the end of the election, electronic tallies produced by the machine can be used to provide preliminary results, but official certification of the election must come from the paper records. Since the ballots are prepared by computer in machine- and human-readable format, they can be optically scanned for a tally, or hand-tabulated for a recount. After the election, yet other entities (such as the League of Women Voters or a news organization like Reuters) can verify the ballots using their own scanning equipment, if the format is produced in a generic way.

This type of system is cost-effective. No longer must blank ballots be prepared in advance, as with mark-sense or other paper-based voting systems. Incidentally, mark-sense products—preprinted ballots with circles or ovals that a voter fills in with a pencil or pen—do provide a physical record that is available for recount. They have the lowest undervote rate of all the computerized tabulation systems, according to a number of studies, including one by the Caltech/MIT Voting Technology Project [see “On the Road Toward Electronic Voting” p. 48].

One evolving system, still only at a trial stage, from Populex Systems (West Dundee, Ill.), is similar to the Mercuri Method. As company founder Sanford Morgenstein puts it, “The count is not something that’s kept in a computer, but one that is tangible, that you can look at.” Nonetheless, it differs in an important respect: voters use a touch screen to generate a printed ballot that contains only a bar code to indicate the votes. Thus, the system is open to vote tampering, according to Doug Jones, a computer science professor at the University of Iowa who examines evoting technologies, since many voters won’t check that the bar code matches their choice.

According to Jones, an election could be rigged by altering at random, say, one ballot in 100, enough to swing many close elections. “If only 1 voter in 100 bothers to check, that means that only 1 in 10,000 will find an error,” Jones says. And whod’s to know that the bar-code reader hasn’t been programmed to misread ballots? Hence, the Mercuri Method requires a human-readable plain text printout.

Besides its utility in recounts, the fact that the voter sees the final ballot on the screen as well as on paper has been shown to help voters catch their own mistakes. Visually impaired or illiterate voters can be allowed to use voice-feedback scanners to read the paper ballot, so they would not be disenfranchised by this process.

The Mercuri Method recount concept has been incorporated into recent voting legislation reforms (including some in Florida, California, and Maryland) that require the voting systems to produce paper audit trails. Brazil will use the method for 3 percent of its voting systems in an upcoming election.

Although some vendors, such as Avante Systems (Princeton, N.J.), have started to incorporate voter-verifiability into their products, the largest companies have oddly interpreted these laws to mean that audit trail printing can be done from the internally recorded ballots after the election. Their claim is that cryptography and redundancy will be used to secure the data. But these techniques are insufficient to ensure end-to-end correctness, since voters cannot verify that the ballots produced are indeed the ones they cast. Furthermore, data can be corrupted (intentionally or accidentally) early in the process, resulting in stored information that seems correct, but may not be.

Cryptography can, though, be effectively used along with a voter-verifiable ballot to prevent ballot-box stuffing, and to make certain that the paper tallies match the electronic results. David Chaum, a Palo Alto, Calif., cryptologist who, 20 years ago, invented electronic cash, has a technique that provides the best of all possible worlds: a computer-generated, voter-verifiable physical ballot that also gives the voter a receipt that can be used to determine that his or her vote was tabulated correctly, without revealing its contents.

One drawback of Chaum’s method is that to demonstrate that the votes are tallied correctly requires a lot of math. As a result, it is difficult to explain to election officials, poll workers, and voters how it establishes the correctness of the balloting and tabulation process. But it gives a glimpse of the type of voter-verifiable systems that may be used for future elections.

An observer of voting technology once remarked: “If you think technology can solve our voting problems, then you don’t understand the problems and you don’t understand the technology.” Computerization alone cannot improve elections. Those designing and those buying election systems must be aware of their inherent limitations, mindful of the sometimes conflicting needs for privacy, auditability, and security in the election process, and willing to seek out-of-the-(ballot)-box solutions.