Making Votes Count

How to steal an election — the modern way

By IVARS PETERSON

"It's not the voting that's democracy; it's the counting." — Tom Stoppard, dramatist

For decades, the voters of Bucks County, Pennsylvania, have registered their choices by pulling levers on bulky mechanical voting machines. Many of these machines are now so old that their manufacturers are no longer in business, and the county government has to scrounge discarded equipment from other jurisdictions to maintain a supply of spare parts.

In 1989, the county commissioners decided to buy new voting equipment — a decision that the voters would have to approve in a referendum. Such a vote would merely authorize the spending of a certain sum of money for this purpose; it would not specify the type of equipment to be purchased.

But it was clear from the beginning that the county government intended to obtain one of the several different types of computer-based voting systems on the market. Vendors of such systems typically promise lower election costs, greater speed in tallying votes, and improved accuracy.

When Rebecca T. Mercuri, then an elected Democratic party official in the county, heard about the decision to hold a referendum on this matter, an alarm went off in her mind. From her extensive knowledge of computers and her wide experience in verifying and validating software, she was familiar with the kinds of problems involving reliability, accuracy, and security that can readily afflict computer systems.

"I don't think we really want these [computerized voting systems]," Mercuri thought at the time. She started a campaign to dissuade county officials from going ahead with their plans. She assiduously collected whatever information existed about various computer-based products for registering and tallying votes, particularly their vulnerabilities.

This effort brought her into contact with Computer Professionals for Social Responsibility (CPSR), a group based in Palo Alto, Calif., and Washington, D.C., which has been documenting the risks of computerized vote counting. She also obtained the help of Mae Churchill, who heads an organization known as Election Watch, in Pacific Palisades, Calif.

"They were running around the country doing what I was trying to do singlehanded — to alert people to the hidden dangers of these computerized systems," Mercuri says.

What Mercuri learned appalled her. "We have this trust that these machines will collect and tabulate our votes properly," Mercuri declares. "That's utter bunk."

As more and more counties and cities turn to electronic elections of one kind or another, "we are starting to see situations that look very fishy," she contends. "Elections are not being administered properly."

For example, serious problems, possibly involving fraud, have surfaced in a mayoral contest held last March in St. Petersburg, Fla. Questions have also been raised about the accuracy of vote tallies in the special election held earlier this year in the first congressional district of Wisconsin, where as many as 5 percent of the voters may have failed to get their punch-card votes counted.

Indeed, so many errors in the use of computer-based voting systems have come to light in recent years that the security and auditability of such systems formed a topic of discussion by a panel of experts at the Computers, Freedom and Privacy conference held last March in Burlingame, Calif. The subject was also featured at the 16th National Computer Security Conference, convened last month in Baltimore by the National Institute of Standards and Technology (NIST), located in Gaithersburg, Md.

"We wanted to explore methods that could lead to increased security and improved auditability of these systems," says Mercuri, who organized and chaired both panel discussions. Mercuri herself is now a research fellow at the University of Pennsylvania in Philadelphia.

To varying degrees, errors and fraud have always been part of elections in the United States. "Don't rely on any election statistics before 1920," warns Gary L. Greenhalgh, former director of the Federal Election Commission's National Clearinghouse on Election Administration. He is now national sales director for the Microvote Corp., based in Indianapolis.

"They're estimates at best, because the fraud was massive," Greenhalgh used to tell students in the courses he taught. "That's just the way it was."

Indeed, paper ballots could be readily torn, lost, mishandled, replaced, miscounted, or destroyed. Voter lists and voting machines could be manipulated in a variety of ways. The integrity of an election depended greatly on the trustworthiness and diligence of the county or local officials running the show.

Voting with the aid of computers began in the late 1960s, says voting-equipment expert Roy G. Saltman of NIST. At that time, rapid population growth in such places as Los Angeles had officials looking for a relatively inexpensive alternative to the large, costly mechanical voting machines then in use.

One answer was punch cards. Voters could indicate their choices by using a stylus to punch out scored rectangles on a card. Assuming that its attached punch-card reader sensed the voters' choices correctly, a central computer would then count the votes.

Later, vendors of election equipment introduced mark-sense ballots, in which marks made on a ballot are detected optically, then fed into a computer — either at each precinct or at a central facility — for tallying. More recently, several jurisdictions have adopted electronic systems that register votes directly rather than on paper ballots.

"From the very start, there were concerns about the integrity of the process of computerized voting," Saltman says. The primary issues have been — and continue to be — the accuracy with which voters' choices are recorded and the correctness of the computer software that generates results.

In particular, "electronic voting systems are a source of worry because they perform their work in microcircuitry not readily accessible to examination, and they often leave no tangible record of what they have done," says Michael I. Shamos, an attorney in Pittsburgh who evaluates computer-based voting systems for Pennsylvania and Texas.

A voter may well ask, "Is my vote being recorded correctly? Does the system know who I am and therefore how I voted? How do I know they programmed it correctly? Could some hacker manipulate the votes?"

Nonetheless, given the evident vulnerabilities of paper ballots and mechanical voting machines, electronic systems — properly implemented — are far safer than any prior method of voting, Shamos argues. "I do not claim that electronic voting is free of troubles but instead urge that its advantages far outweigh its risks," he says.

The problem is that there are no real guarantees that a computerized voting system is functioning properly and that the voting and tallying procedures have adequate security. "At this time, there is no set of generally accepted procedures to assure system integrity because there are no mandatory security standards governing the operation of computerized vote tallying, even in federal elections," Saltman notes.

This situation is exacerbated by state and local election officials, whose primary concern is keeping election costs down and who put a premium on speed and convenience. As a result, "the vendors don't particularly care about computer security because the marketplace doesn't care," Greenhalgh insists. State and local election agencies rarely ask about security and auditability when they purchase electronic vote-tabulation systems.

Tampering with the kinds of systems now deployed can be remarkably easy, Mercuri maintains. From intentionally damaging the equipment to bypassing the vote-tallying program in order to modify results, an individual or group intent on subverting an election has a variety of options.

At the same time, many election officials are content to let the vendors of election equipment run their elections for them. "The election official passes on [his or her] responsibility to the vendor, who is accountable to no one," says Eva Waskell, who heads CPSR's election project. "We have private elections in this country."

And that leaves lots of room for trouble.

A hotly contested municipal election held on March 23 in St. Petersburg, Fla., demonstrates the kinds of shenanigans that can go on when politics and computers mix. The day after the election, a local watchdog group, the Florida Business Council, began receiving reports of voting irregularities and other suspicious practices.

"There were indications to us that it involved not just ballot stuffing but also computer tampering," says Bill Scanlan, a member of the Florida Business Council.

When the group began investigating the charges, it discovered that the local election supervisor had authorized the use of two different computer programs to tally the votes registered on punch cards, with each program handling half the ballots. A third program — which had not been certified by the state for use in elections — merged the two sets of results.

The council also found that in the final tally, one precinct with no registered voters had suddenly acquired 7,331 voters, of whom 1,429 had cast ballots. The controversial incumbent mayor had won the race by just 1,425 votes.

The charges were serious enough to initiate a court-authorized investigation, and various individuals were called to testify under oath. However, although the investigation uncovered instances in which a programmer had temporarily suspended the vote counting to make some sort of adjustment to the computer's operating system software, no one ever got to analyze the computer programs themselves. Their vendors argued that the line-by-line contents of these programs are proprietary — as precious a trade secret as the formula for Coca-Cola.

It proved extremely difficult to demonstrate that deliberate fraud rather than administrative incompetence was at the heart of the problems. "There are many, many stories of accidental errors creeping into voting processes," comments computer security expert Peter G. Neumann of SRI International in Menlo Park, Calif. "In many cases, it's easy to masquerade a potential misuse as an accident. In essence, the two are indistinguishable in many cases."

But Scanlan and his colleagues remain suspicious. They have heard from other Florida counties where a similarly suspect process involving the merging of two separate counts has occurred. "The more we investigate, the more questions are raised," Scanlan says.

Over the years, computer scientists and other researchers have proposed a variety of high-tech solutions — some of them, for example, involving a form of cryptography — to security problems in computer systems in general. But these solutions invariably prove flawed in some fundamental way, Neumann says.

"Technological solutions are extremely insidious," he notes. "They give you the impression that you have a solution, whereas that solution is still completely subvertible."

In the case of election software, the trade-off between anonymity and accountability — required to keep individual ballots secret while ensuring that only legitimate voters cast ballots — makes the problem even harder to solve. "I personally do not believe that any vote-tabulation system, particularly one that involves computers, can be designed to be impervious to attack," Mercuri says. "Security and auditability are really largely a matter of degree."

She adds, "The problem is that the degree of security for these systems has not been mandated [at the federal level], leaving local municipalities and states to devise their own standards, which vary."

This situation leaves the administration of elections in the hands of about 10,000 separate authorities, who run elections in jurisdictions as large as New York City and as small as villages in New England with just a handful of voters.

In 1990, the Federal Election Commission established voluntary guidelines for the manufacture, procurement, and evaluation of vote-tallying equipment. But critics charge that these rules are incomplete and have not been widely adopted.

Things could be much better. "All parties — vendors, certifying authorities, purchasers, concerned citizens, everyone — must work together to continually improve and monitor the entire election process," Mercuri says.

But few in government seem interested. "There is currently no technical staff with computer and communications expertise assigned within the federal government to advise the Congress on the effect of these technologies on the integrity of the election process," Saltman remarks.

Bucks County still hasn't obtained new, electronic voting machines. "I've been successful in keeping this off the ballot," Mercuri says. "In fact, it was recently reported that, again due to some efforts on my part, they aren't even going to consider getting them for another three years."

"I think they're just waiting for me to move," she jokes.

But the caution displayed in Bucks County runs counter to the general trend. Installation of computer-based systems continues at a rapid pace. Earlier this year, New York City awarded a $60 million contract for the purchase of 7,000 machines for directly recording votes — even though critics contend that the particular brand of machine purchased has not yet been adequately tested. In Europe, countries such as Norway and Belgium are already on their way to all-electronic elections.

"It takes trustworthy systems and trustworthy people to avoid tampering; it takes even more to avoid accidents from user operation or misuse," Neumann says. "Our trusting of people and of systems that are not trustworthy is an open invitation to disaster."

Ironically, such a disaster may occur not in a national election, but in the numerous local contests that often have low voter turnout yet decide positions having considerable authority over contracts, law enforcement, and taxes. "It's in these small elections for critical offices, wherever the elections are not well administered for whatever reason, that the temptation to steal an election may be strongest," Greenhalgh says.

But "whether it's an administrative error or stealing an election, you get the same result," he adds. "People lose confidence in the process." □