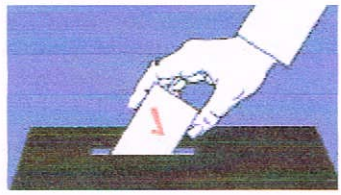
AN MIT ENTERPRISE TECHNOLOGY REVIEW

Campaigning for Computerized Voting

Despite staunch opposition from the computer science community, ATM-style electronic voting may offer the best hope for escaping the mess inflicted by paper-based balloting systems.



By Simson Garfinkel
The Net Effect
September 3, 2003

Over the last two decades, geeks have rarely passed on an opportunity to replace a perfectly good mechanical device with a computerized system. Got one of those old-fashioned cash registers? Replace it with a PC and a touch screen. Got a hotel with perfectly good door locks and metal keys? Rip them out and replace them with computerized locks and swipe-cards. Wherever you look, pinball is out, video games are in.

But there is a rising chorus of geeks—a chorus led by some very high-profile computer science professors and researchers—who say that one machine should never be computerized: the voting machine. These computer professionals say that accurately counted free elections are the bedrock of democracy. Voting, they claim, is too important to be done on a computer. The irony is delicious—it's sort of like group of doctors arguing for the return of leeches because the President of the United States is too important to be treated by modern medicine.

Specifically, the computer scientists are opposed to that new generation of

voting machines that resemble automatic teller machines. These systems are called "direct recording electronic" (or DRE) voting machines because people vote on the touch screen and the votes are recorded directly on the computer's hard drive, without any paper being harmed in the process.

There are a lot of reasons to like these DRE machines. Because the voting is done on a large touch screen, they can use big fonts that are easier for the elderly to read. The machine can be programmed to reject attempted votes that are patently wrong, like voting both "yes" and "no" on a referendum question. The machines can be equipped with speech synthesizers, allowing people who are blind or illiterate to vote on a truly secret ballot for the first time in their lives. They can even confirm the voter's choices on a second screen—which means that there would be no more elderly Jewish voters in Palm Beach accidentally casting their ballots for Pat Buchanan.

Nevertheless, most computer professionals are opposed to the DRE machines. One reason is that there is fundamentally no way to audit them: If 600 people vote at a DRE on Election Day and the machine says that 310 voted for the Democratic candidate, who is to say that the number 310 is true? Perhaps only 280 voted Democratic, but the machine was programmed to randomly flip 5 percent of the Republican votes to Democrat before recording them on the computer's hard drive. To make this sort of programmatic tampering harder to detect, perhaps the program was devised so that the flipping would only happen on the first Tuesday in November. On other days—presumably the days when election officials tested the voting machine—no vote flipping would take place. To make it even harder to detect, perhaps the flipping occurs only when the machine discerns that the vote is close; this would avoid the embarrassment of having polls predict one outcome, and having the machines tally another.

This sort of election-stealing logic would be easy to code into the voting machine's operating system. The logic could be written by a lone programmer—perhaps an activist hacker with a grudge—without the knowledge of the voting machine company. The logic could be so well hidden that not even a careful review of the machine's source code would find it. This isn't as far-fetched as it might sound: Unauthorized features called "Easter eggs" are routinely hidden in commercial software, even software shipped by Microsoft.

I keep writing "*most* computer professionals" because I recently met one who isn't opposed to DREs: In fact, he's positively enthusiastic about them. And this man isn't just anybody; he's Ted Selker, an award-winning inventor with many patents, formerly with IBM Research, currently a professor at the MIT Media Lab, and member of several panels and commissions that looked at the issue of voting following the debacle of the 2000 presidential election.

I met Selker a few days after he had attended a meeting of computer scientists and election officials in Colorado. He was livid. He had just spent two days listening to the experts of the field talk about all of the failings with DREs and how these systems could be used to steal an election.

"What these people don't realize," he told me, "is that automated tabulating machines were invented for a reason"—that is, because paper is a fundamentally bad way of making and keeping accurate records. Paper is bulky and heavy. It can be hard to read something recorded on paper, no matter whether the marks were made by hand with pen-and-ink or by a computerized printer. Paper rips and gets jammed in machines. Paper dust gets everywhere. Eliminating paper, Selker explained to me, has the potential for dramatically improving elections.

"But what about all of the ways that you can hack the voting machines?" I asked him.

Selker laughed. Politicians, he told me, have been hacking elections in America for more than 200 years. The geeks are focusing on the abilities of hackers to steal elections by reprogramming DREs because electronic attacks are what these folks understand. But if your goal is truly better elections, he says, the DREs can do more good than harm.

One of the most effective ways to affect an election's outcome is to take your opponent's supporters off the election roles. That's what happened in Florida three years ago: thousands of Democrats, many of them minorities, showed up at voting places and discovered that they were no longer registered. Why? Because it's illegal for convicted felons to vote unless that right is specifically restored. Florida had recently purged the voting roles against a computerized database of convicted felons; tens of thousands of people were removed, some apparently in error. Other techniques for stealing an election, Selker told me, are stationing tow trucks outside the polls to intimidate voters; setting up police roadblocks (as was done in Florida in 2000); intentionally designing confusing ballots; putting people on the ballot with the same name as your opponent; and getting votes the old fashioned way—by buying them. "And don't get me started on absentee ballots," he said.

Selker has been studying the electoral process for years, and he has come to a disturbing conclusion: The more he looks, the more problems he finds. A few years ago, for instance, he stationed himself at a Chicago polling place on election day. He discovered that the election workers had not been adequately informed as to how ballots should be properly marked for an important question; the ballots that were filled out incorrectly had to be disqualified. Those were paper ballots, Selker was quick to point out. Hacking aside, election officials are supposed to be able to audit the programming of a voting machine. What they can't do is make sure that every election-day volunteer is giving out correct instructions for filling in a paper ballot.

What about the value of a paper trail? I asked Selker. Just having a vote on paper is no guarantee that it will be correctly counted, he explained. He cited an example (again from Chicago) of an election commissioner who bragged about counting votes for a Republican candidate and then writing them down as votes for the Democrat.

All of this suddenly matters a great deal. Over the next year, counties all over the United States will be throwing out their old mechanical voting machines and buying new voting systems. The money for this project—roughly $3.9 billion—is coming from the U.S. Congress through the Help America Vote Act. The two big contenders are the DRE machines and a paper-based system that counts votes with optical scanners.

Ironically, many of the proposals that have been made to "improve" the security of DRE systems actually make it easier for politicians to sabotage an election via other means. For example, any technique that gives a voter a printed receipt is susceptible to a vote-selling scam: Just turn in the receipt, and collect your $20. Even receipts that would be visually inspected by the voter and dropped into a sealed box—a proposal made by Stanford professor David Dill—are vulnerable to a vote-selling technique known as "chain voting."

Before talking with Selker, I was squarely in the anti-DRE camp. After listening to him, I realize that there is another side to the story that is being systematically underreported by the technology press. Did he convince me? Well, let's say that I'm no longer convinced of the inherent correctness of the anti-DRE position.

So you can imagine how surprised I was by the next thing that Selker told me. "Of course," he said, "this country is going about election machines entirely the wrong way."

The current DRE machines, says Selker, are monstrosities. They cost ten times more than they should. Their designs are secret and their code is proprietary. And even worse, what precious few facts that have been revealed in public are deeply troubling.

A few months ago, the source code for a voting machine manufactured by Diebold was inadvertently left on a Web site. A group of researchers at Johns Hopkins downloaded the code and analyzed it. They found many software errors and poor design methodology. One of the most glaring problems had to do with encryption: although the computer used the DES algorithm to encrypt the votes, the encryption key was hard-coded into the program and unchangeable. A key that can't be changed offers little more security than using no encryption at all.

Instead of having US taxpayers spend more money on proprietary voting machines of questionable quality, Selker says that we should follow in the footsteps of Brazil, which deployed DREs in the 1990s and is currently working on the second generation of these machines.

Brazil's machines were designed in a transparent, public process by two of the country's leading research institutions. The national government then accepted bids from different companies who competed to build machines according to the open design. Everything was above-board—extremely important for a nation that has a history of election fraud.

These voting machines are simple, compact, functional, and have done a great job to bringing fair elections to the entire country. For example, each system operates on either wall current or on a set of self-contained batteries, allowing it to accept votes more than 12 hours deep in the Amazon jungle without having to be plugged in. The touch screens display not only the candidates' names but also their photographs—an important detail in a country where so many voters are illiterate. What's more, instead of costing thousands of dollars, each machine costs just hundreds.

The Brazilian machines are not perfect: they've been criticized because, like other DREs, they fundamentally cannot be audited after the fact. But security is a series of tradeoffs: the first electronic election in Brazil gave voters a printed receipt that the voters had to drop into a box after verifying it; this receipt was reportedly used for chain voting scams and the practice was discontinued in the next election.

Selker is convinced that DREs are the way of the future; many notable computer scientists continue to believe otherwise. "Election technology has not advanced to the point where it can provide us with electronic systems that are reliable enough to trust with our democracy," writes Stanford's Dill on his Web site, VerifiedVoting.org.

My feeling is that elections are in a mess throughout this country: voting machines are a problem, but so are the voter registration system, election-day intimidation, and the whole districting process. The problem with optical scan (the main technological competitor to DRE) is that unless the ballots are actually scanned when they are turned in by the voters, there is no way to prevent people from throwing away their votes by making minor clerical errors on the ballots.

Selker's argument is simple: paper is bad, and whatever problems are inherent in today's DREs can be overcome by an open design and review process. Nobody else seems to be making this case. The U.S. DRE vendors want to sell high-priced proprietary voting machines. Meanwhile the academics want to stick with paper and all its problems.

> Join the discussion

Technology Review columnist Simson Garfinkel is the author of 12 books on computing, including *Database Nation*. More by this author >>

TR RELATED ARTICLES

- Sponges Grow Sturdy Optical Fiber
- Gold Speck Highlights Molecules
- Tool Sketches Quantum Circuits
- The Great (Driverless) Car Race

RECOMMENDED LINKS

- Help America Vote Act
- The Caltech-MIT Voting Technology Project
- Technology Review profile of Ted Selker
- Article describing "chain voting" in Illinois Issues (March 2000)
- VerifiedVoting.org
- Brazil's new voting machines

About Us | Contact Us | Privacy | Terms of Use | Advertise | Subscribe | Newsfeed

MIT