Election Security and the Need for a Voter-Verified Audit Trail

by David Jefferson

Electronic voting machines—touch-screen computers known as DREs (direct recording electronic)—are, in principle, a major advance in voting technology. They offer huge advantages in election administration; in the level of service offered to non-English speaking voters, the disabled and the illiterate; and, in principle, they should offer greater accuracy as well. Unfortunately, as presently designed, they have a profound security flaw that leaves them wide open to software error, manipulation and fraud on a potentially unprecedented scale. It is vital that this catastrophic flaw be corrected before DREs become the standard voting equipment in the United States. Fortunately, it can be corrected easily by adding one important safeguard to every voting machine: the ability to produce a voter-verified audit trail.

> "It is vital that this catastrophic flaw be corrected before DREs become the standard voting equipment in the United States."

In a DRE there is an enormous amount of software—hundreds of thousands of lines—that operates between the voter's touch on the screen and the capture of that vote on the machine's memory cartridge. It is extremely easy for either a software bug or fraudulent code to cause the voting machine to display the correct votes on the screen for the voter to see but to record different votes in memory. A single programmer acting alone, anywhere along the production process for DRE software, can make this happen. Voting system vendors deny it publicly, but they, and all other software producers, understand this very well and try to prevent it. Unfortunately, it is not readily preventable; even giant Microsoft produces code that is riddled with bugs and security flaws and has been plagued by its own programmers deliberately hiding undocumented "features"—known as "Easter eggs"—in their products. In point of fact, there is no guarantee that DRE software does not already have erroneous or malicious logic that can incorrectly record votes.

Since all voting machines produced by the same vendor run essentially identical code, any fraudulent logic in one will be replicated in all machines of the same kind. Thus, any problem would simultaneously affect hundreds of counties, and tens of millions of votes, nationwide. If undetected (a likely case), the problem could continue for many election cycles, having an effect on election outcomes on a national scale.

Wouldn't such a problem be detected during qualification, certification, or logic and accuracy testing of voting machines before they are used in an election? For most ordinary bugs introduced by a programmer's mistake, the answer is yes. But if malicious logic is deliberately introduced by a programmer and carefully concealed, it can easily be hidden so well that no reasonable amount of testing of the code, even by experts, would find any problem! People who are not experts in software and computer security, and that includes most election officials, frequently find this conclusion completely counterintuitive. But any security expert will tell you that it is very easy to write hidden logic that behaves properly when being tested and only does its dirty work when used in a real election.

Aren't there elaborate internal cross checks, redundancies and procedural safeguards that will detect problems like this? In a word, no. All such measures assume that votes are recorded correctly in the first place. But if the DRE deliberately or erroneously records them incorrectly, then all subsequent cross checks and procedures are useless.

So what can be done about this danger? We need a fundamental design modification to DREs: a voter-verified audit trail. The idea is simple. A voting machine, in addition to recording votes electronically, should also print the votes on paper (or other indelible medium), during voting, for the voter to inspect. The paper ballots would be used as backup to the electronic copies in case of a recount, a challenge or any problem with counting the electronic ballots.

How does this solve the problem of malicious or buggy DRE software? The key observation is that, unlike the electronic ballot, once the paper ballot is inspected by the voter, it cannot be changed by software at all! No bug or malicious code, however obscure or clever, can prevent the accurate capture of votes! This one simple, elegant modification cuts to the heart of virtually all security vulnerabilities introduced by electronic voting, which is why essentially the entire computer security community in the United States agrees on the necessity for it. Before we spend billions of dollars nationwide converting our election systems to DRE, it is essential that we guarantee that they are invulnerable to errors or potential fraud in voting machine software. Rarely in the world of software security is there a simple solution to such a wide range of problems, but we are lucky in this case. Voter-verified audit trails should be a requirement for all DRE machines in the U.S. ET

Dr. David Jefferson is a senior computer scientist at Lawrence Livermore National Lab and long-time election security researcher and expert.

A solution in search of a problem

by Jim Dickson

Voter-verified paper ballots are not only unnecessary, they constitute a major threat to the modernization of the nation's obsolete voting system. Cal Tech and MIT report that in 2000 roughly two million Americans went to the polls, voted and left believing that their ballots were going to be counted. These voters had their votes taken away because of the high rates of error inherent in punch-card, lever and optical-scan machines. Touch-screen systems are proven to have the lowest error rate. Electronic voting on touch-screen machines has been in use for 40 years. Not one election in four decades has been spoiled by the use of direct recording electronic (DRE) machines. In the same time period, scores of elections have been damaged by the use of paper voting.

Every election system is imperfect; every method of voting is subject to malicious attack or inadvertent damage. The question is: what is the probability of such an accidental or malicious deed? Elections are layered with human safeguards, procedural protections, as well as modern hardware and software systems. If we trust our work, finances and safety to computers every day, we should be able to do the same with our elections.

> "If we trust our work, finances and safety to computers every day, we should be able to do the same with our elections."

Running an election is like flying an airplane. There are computers on board with back-up systems, but there is also a captain and co-pilot. On-board computers, like the computers used for elections, are not accessible to just anyone. Before a city or county can buy a machine, it must go through vigorous testing and certification, first at the federal level and then at the state level. The machine manufacturers do not design the ballot or program the machine; both are the responsibility of the local city or county officials. Once the machines are programmed for a specific election, they are stored in secure facilities with tamper-evident locks and seals and are only distributed to the polling places the day before the election. On Election Day, each machine is opened and initialized in the presence of poll workers and judges (in most states, four individuals in each polling place). Each machine is checked to confirm that there are no votes registered on it. The machines and the programs that run them, including the tabulating software, are not accessible from the Internet. If a rogue programmer wanted to steal an election, he would have to gain access to hundreds of thousands of machines one at a time.

DREs are the only voting systems that offer millions of disabled Americans the ability to cast a secret, independent and verifiable vote by reading the ballot via earphones for the voter. I am blind, and I have never cast a secret ballot. According to the census there are 11.5 million Americans who, because of blindness or hand-arm disabilities, have had to use third-party assistance. After the 2000 election many Americans, for the first time, asked themselves, "was my ballot marked properly?" Those of us with disabilities ask ourselves this question every time we vote. Audio ballots are also important to citizens who speak minority languages. Like my grandparents, millions of immigrants become citizens. They often leave their countries of origin without acquiring reading proficiency in their native languages. Millions of other American citizens have limited reading ability, and they will be able to listen to the ballot and vote without embarrassment or insecurity. There are four manufacturers whose DRE machines are accessible to the disabled: Diebold, Sequoia Pacific, Hart Intercivic and Elections Systems and Software. None of these offer a voter-verified paper ballot. As a matter of fact, there is no voter-verifiable paper ballot machine on the market that has been certified at the national level. A touch-screen system that offers an accessible voter-verified ballot has never been used in an actual election.

Introducing a new voting technology to market takes years. After a new system is designed, it must be tested: Will the machines run flawlessly for 12 hours? Are they easy to set up and operate? After these types of questions have been satisfactorily answered, the machines are given real-world trials in a number of elections with small turn-outs, such as school board or county commissioner elections. Once the machines are proven to work flawlessly, they can be used in a primary election with the general election to follow. Often a county or a city will first deploy the new system in only part of its jurisdiction. The public and poll workers must be taught, in advance of Election Day, how to use the new equipment. Years of running elections and testing new voting systems have taught us that new systems must be introduced slowly, deliberately and incrementally. There has never been a new voting technology brought to market in less than four years. If we go to paper, then the two million Americans who thought they had voted but did not get their vote counted in 2000 will not have their vote counted in 2004, 2006 or even 2008. ET

Jim Dickson is Vice President for Governmental Affairs of the American Association of People with Disabilities (AAPD). He leads the AAPD Disability Vote Project, a broad coalition of 36 national disability-related organizations.