Electronic Voting Systems: the Good, the Bad, and the Stupid

Barbara Simons

As a result of the Florida 2000 election fiasco, some people concluded that paper ballots simply couldn't be counted. Instead, paperless computerized voting systems (known as direct recording electronic systems, or DREs) were touted as the solution to "the Florida problem." Replacing hanging chads with 21st century technology, proponents claimed, would result in accurate election counts and machines that were virtually impossible to rig. Furthermore, with nothing to hand-count and no drawn-out recounts to worry about, computerized voting systems were expected to enable the reporting of results shortly after the polls had closed.

Many election officials loved the idea, believing the new machines would also prove cheaper and more reliable than the old systems. That enthusiasm was reinforced by the promise of nearly $4 billion in federal funds for the purchase of DREs, courtesy of the Help America Vote Act (HAVA), passed in 2002.

The idea of computerized voting systems drew advocates from many sectors. Among the most outspoken advocates of paperless DREs is Jim Dickson, vice-president of the American Association of People with Disabilities. The League of Women Voters has also lobbied on behalf of paperless DREs (though the national office retracted its support when members revolted at the recent LWV convention).

Yet now, just two years after the passage of HAVA, voter-verifiable paper trails are being demanded by numerous public interest groups, computing professionals, and members of Congress. Where did things go wrong?

For starters, software for electronic voting machines is proprietary, the certification testing process is both secret and incomplete, and the test results are secret. (Note to system designers: this is *not* a good formula for building trust.) To cap things off, the COTS (commercial off-the-shelf) software contained in voting systems is not examined in any of the testing, simply because FEC (Federal Election Commission) guidelines don't require it.

For years, prominent computer security experts have been arguing that paperless DRE machines present major security problems, including buggy software and the risk of malicious code affecting the outcome of an election. But the warnings of experts such as Rebecca Mercuri (http://www.notablesoftware.com/evote.html) and Peter Neumann (http://www.csl.sri.com/users/neumann/neumann.html#5) went largely unheeded by election officials and the public until David Dill created a petition (http://www.verifiedvoting.org/index.asp) calling for voter-verifiable audit trails. The core idea behind the Dill petition is that voters should be able to verify that their ballots have been correctly recorded; also, it should be possible to conduct a meaningful recount. To avoid the risk that the machine prints the correct result while storing an incorrect result in computer memory, it should be possible to manually recount some number of randomly selected paper ballots as a check on the machine-generated results.

Is it true

THAT POLITICS AND TECHNOLOGY DON'T MIX?

A FEW HORROR STORIES

Because of the secrecy surrounding almost every aspect of e-voting—along with a lack of public incident reporting—independent computing technologists can provide only limited analyses of problems related to electronic voting system hardware, software, testing, security, and human factors. Nonetheless, evidence of problems is widespread. A few examples follow.

In January 2004, a special election was held in Broward County, Florida. Only one contest was included on the ballot. Yet, of the 10,844 votes cast on ES&S (Election Systems & Software) paperless touch-screen voting machines, 134 were… for no one at all. Since the winning candidate won by only 12 votes, people understandably wondered what had become of those 134 votes; there was no way of telling if some had been lost by the computer. County officials are now calling for paper ballots.

In November 2003, in Boone County, Indiana, more than 144,000 votes were cast—even though Boone County contains fewer than 19,000 registered voters, and, of those, only 5,532 actually voted. The county clerk stated the problem had been caused by a "glitch in the software." Updated results then were obtained that were consistent with the number of people who had actually voted, and the public was assured that the new electronic tally was accurate. Still, because the county used paperless MicroVote DREs, it was impossible to verify independently that the updated results were indeed correct.

When the polls opened in Hinds County, Mississippi, in November 2003, voters arrived to find that the WINvote DREs were down. Worse yet, no paper ballots were available. By mid-morning, some machines were still down. Voters complained about waiting in long lines and how they had been required to complete makeshift paper ballots—some being nothing more than scraps of paper—without adequate privacy. At 8 p.m., voters were still standing in line. One report claimed the machines had overheated. Subsequently, the Mississippi State Senate declared the results in that district invalid and scheduled a new election.

An attacker with access to the source code would have the ability to modify voting and auditing records.

SERIOUS SECURITY CONCERNS

Diebold, one of the major DRE vendors, has been at the center of a political maelstrom because of intemperate remarks made in 2003 by its CEO, Walden O'Dell. But that little PR problem pales in comparison to the security problems uncovered when Bev Harris (http://www.scoop.co.nz/mason/stories/HL0302/S00036.htm) announced in February 2003 that she had discovered Diebold voting machine software on an open FTP Web site.

Computer science professors Aviel Rubin (Johns Hopkins University) and Dan Wallach (Rice University), and their students Tadayoshi Kohno and Adam Stubblefield, subsequently analyzed some of that software and published their findings in a paper, sometimes referred to as the "Hopkins paper," presented at the May 2004 IEEE Symposium on Security and Privacy (http://avirubin.com/vote/analysis/index.html). One of the more shocking revelations made in that paper is that Diebold uses a single DES key to encrypt all of the data on a storage device. Consequently, an attacker with access to the source code would have the ability to modify voting and auditing records.

Perhaps even more surprising, Diebold had been warned in 1997 about its sloppy key management by Douglas Jones, a professor of computer science at the University of Iowa and a member of the Iowa Board of Examiners for Voting Machines and Electronic Voting Equipment (http://www.cs.uiowa.edu/~jones/voting/dieboldftp.html):

> [N]either the technical staff nor salespeople at Global Election Systems [purchased by Diebold in 2001] understood cryptographic security. They were happy to assert that they used the federally approved data encryption standard, but nobody seemed to understand key management; in fact, the lead programmer to whom my question was forwarded, by cellphone, found the phrase key management to be unfamiliar and he needed explanation. On continued questioning, it became apparent that there was only one key used, companywide, for all of their voting products. The implication was that this key was hard-coded into their source code!

Because of the security issues raised in the Hopkins paper, the State of Maryland, which had just committed to purchasing Diebold DREs, commissioned a study of Diebold machines by Science Applications International Corporation (SAIC). The SAIC report (http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf) is a very fast read, since only about one-third of it was made public. (According to Frank Schugar, project manager for SAIC, the report was redacted by Maryland, not by SAIC. The Electronic Privacy Information Center has submitted a public records request to obtain the unredacted version.) Even the limited amount of information that was released in the report, however, is quite damning. For example, the report states that the Diebold system is so complicated that even if all of the problems were fixed, there still could be security risks because of poorly trained election officials.

In November 2003, the Maryland Department of Legislative Services commissioned yet another study of Diebold machines by RABA Technologies (http://www.raba.com/press/TA_Report_AccuVote.pdf). The Trusted Agent report, released in January 2004, based on a “red team” effort to hack Diebold voting systems, revealed physical security problems such as the use of identical keys on security panels covering PCMCIA and other sockets on the machines—as well as locks that could be picked in a few seconds.

Unfortunately, when DRE vendors tout the virtues of DREs to election officials, they tend to gloss over security issues related to short- and long-term storage of the machines, as well as machine access control before and after elections.

Meanwhile, the State of Ohio, which had been considering the purchase of Diebold DREs for the entire state, hired Compuware to test hardware and software and InfoSentry to conduct a security assessment. The Compuware study uncovered yet another hardwired password, this time involving the supervisor’s card, used to start up each voting machine on Election Day as well as to terminate the voting process at the end of the day. When the card is inserted into the DRE, the election official must enter the same password or PIN that has been hardwired into the card—but not into the voting software. Consequently, anyone who is able to obtain a supervisor’s card, or who manages to create a fake card with a different password, would be able to conduct a denial-of-service attack by prematurely halting the voting machines, thereby denying some voters the opportunity to vote.

A SOFTWARE BUG THAT PREVENTS AUDITS

Concerns have also been raised about ES&S, another major player in the DRE market (altogether, DREs and optical scan voting systems manufactured by Diebold and ES&S are expected to count something between two-thirds and 80 percent of the ballots cast in the November 2004 election; see the attachments in http://www.electiondataservices.com/EDSInc_DREoverview.pdf for a detailed breakdown by machine type). That’s because a software bug had corrupted the audit log and vote image report in ES&S machines used in Miami-Dade County and many other parts of the country. (For a detailed discussion of the ES&S bug, see http://www.cs.uiowa.edu/~jones/voting/miami.pdf.)

An internal memo written in June 2003 by Orlando Suarez, division manager of the county’s enterprise technology services department, describes a discrepancy in the internal auditing mechanism of the ES&S machines that make the audit reports “unusable for the purpose that we were considering (audit an election, recount an election, and if necessary, use these reports to certify an election)."

The audit log contained results for some nonexistent machines, and it also failed to report all the results for the machines that were in operation. According to Doug Jones, there were actually two bugs. One—triggered by a low battery condition—caused corruption in the event log; the second caused the election management system to misread the machine's serial number in the face of this corruption. Although the true vote count was not affected, the problems uncovered are symptomatic of the kinds of anomalies that are not tested for under the current certification process. "As of midsummer," explained Jones, "the State of Florida has approved a fix to the two bugs that caused this problem and, in the pre-election testing conducted on August 13, the event records extracted from compact flash cards showed correct reports of low battery conditions without any corruption of serial numbers. Curiously, it was a member of the Miami-Dade [Election Reform] Coalition who found this evidence as she went over printouts of the event logs generated from the compact flash cards."

On July 27, 2004, the Miami-Dade Election Reform Coalition announced that audit data it had requested revealed that computer crashes had deleted all the election results from the September 2002 gubernatorial race in Miami-Dade, as well as from several more recent municipal elections. It appeared that no backups had been made, leading to speculation that the loss of the ballot images could be a violation of Florida law regarding the retention of ballots. (Amazingly, Miami-Dade officials chose to ignore a memo sent before the crashes occurred in which Cathy Jackson of the county's audit and management services department warned of the lack of backups and suggested that all data should be burned to CD-ROMs following each election.)

After spending a few embarrassing days trying to explain how election officials might have lost critical voting records, Miami-Dade County Elections Supervisor Constance Kaplan announced that her secretary had located a computer disk containing the missing data in the conference room next to her office. According to Jones, "The disk was a CD-R in a file folder. The county had only begun making archival CD-R copies of the data after the county audit and management department suggested that they do so that summer. Apparently, although this was being done, there was as yet no institutional memory of where these disks were being put."

CERTIFICATION FLAWS

The first FEC standard for electronic voting machines, issued in 1990, was replaced in 2002 (http://www.fec.gov/pages/vssfinal/vss.html). Still, many voting systems in use today were certified according to the 1990 standards.

Machines are tested and certified by three private companies—Ciber, Wyle, and SysTest—which are referred to as ITAs (independent testing authorities). The ITAs themselves are certified by the National Association of State Election Directors, but are not subject to any government oversight. Vendors pay for all testing.

One of the bizarre aspects of the certification process is that it distinguishes between firmware and software, with *firmware* being defined as the software that runs in the actual voting machines, while *software* is used to refer to the code used by the election management system. Wyle certifies only firmware, while Ciber certifies only software. SysTest certifies overall systems.

Rather than checking the software for security flaws and attacking the software to see if it can be compromised, the ITAs limit their tests strictly to items specifically required by the FEC standards. Particularly prominent among these are control-flow requirements, with Do-While (False) constructs and the use of intentional exceptions used as GoTos being explicitly prohibited. The 2002 FEC standards also call for "effective password management," but the phrase is not defined. We can certainly infer from the Diebold results, however, that no one is checking to see if encryption keys have been hardwired into the code. The testing also fails to check for exceptions, and there are no provisions for the inspection of COTS code.

Then there's the matter of BDFs (ballot definition files), which contain the candidates and issues information for each election. (For a detailed discussion of BDFs, see http://www.votersunite.org/info/BallotProgramming.pdf.) Clearly, these files are critical to the whole electronic voting process, yet they are never independently inspected by an ITA. Also, pre-election BDF testing is not routine in many jurisdictions.

When BDF errors do occur—leading, for example, to votes for one candidate being credited to a different candidate—they can be detected with optical scan voting systems simply because anomalous computer-reported results can be discovered through manual recounts of paper ballots. With paperless DREs, however, there is no way to perform such a recount.

ALTERNATIVE VOTING MACHINE DESIGNS

Diebold, Sequoia, ES&S, and Hart InterCivic are the major manufacturers of paperless DREs. Most DREs use touch screens as inputs, though Hart InterCivic uses a dial for candidate selection. DREs also can be equipped with earphones and various devices, typically handheld, that allow voters with vision impairments to vote independently. DREs do not allow voters to select more candidates than allowed (overvotes), and they alert voters to any omitted votes (undervotes). DREs also allow voters to review their ballots before submitting them (second-chance voting).

DREs that produce voter-verifiable paper ballots. AccuPoll and Avante produce DRE voting systems that print out ballots that voters can check to ensure that an accurate paper record of their votes exists. Avante also manufactures a model that prints optical scan ballots that sighted voters can mark, along with an "accessible" optical voting system that allows vision-impaired voters to print out optical scan ballots marked to reflect their choices.

Optical scan voting machines. Besides avoiding many of the security problems associated with paperless DREs, optical scan systems are less expensive. Typically, these systems require the voter to mark the ballot in much the same way that students taking standardized tests make computer-readable marks by using number 2 pencils to fill in ovals.

Precinct-based optical scanners require the voter to "test" the ballot by submitting it to the scanner to determine whether or not the ballot contains overvotes. This will also alert the voter should the ballot be discovered to be blank. Ideally, at the end of Election Day—after all the ballots have been initially tallied in the precinct—all the ballots, together with the results, can then be forwarded to the tabulation center. (The chance of ballot boxes or tabulation sheets being illegally manipulated is reduced if the local results are posted locally.) Note that optical scan voting systems by definition create voter-verified paper ballots.

Hybrid models. Ballot-marking systems are a cross between DREs and optical scan systems. One, made by Vogue Election Systems (VES) and currently marketed by ES&S, offers a touch screen like a DRE. The voter simply inserts a blank optical scan ballot into the machine and then proceeds as if interacting with a DRE. Once the voter has entered all of his or her choices, the machine marks the optical scan ballot accordingly, avoiding overvotes and raising alerts to undervotes in the process. This also serves to eliminate any stray pencil marks that could otherwise confuse the scanner. Attached headphones, meanwhile, provide an option that allows blind voters to vote without any assistance.

Another system, produced by Populex, includes a screen that operates with an attached stylus. The system also prints out a completed ballot once the voter has entered all of his or her choices. For human perusal, the ballot uses numbers to represent voter choices, along with corresponding bar codes for the optical scanner's benefit. Like the Vogue system, attached headphones can be provided for blind voters. For both systems headphones attached to the scanner would make it possible for vision-impaired voters, as well as the sighted, to verify their ballots, but this option is not currently available.

Cryptographic voting systems. Both VoteHere (http://www.votehere.net/) and David Chaum (http: //www.seas.gwu.edu/~poorvi/Chaum/chaum.pdf) have developed voting systems that provide an encrypted receipt that voters can use to verify that their ballots have been accurately counted. Chaum's system is not currently being manufactured, however. A problem common to both of these systems is that they offer no way to conduct a recount should it be determined that a ballot tabulation problem has occurred, although individual ballots can be corrected. Also, neither scheme is particularly easy for voters to understand.

Open source. The OVC (Open Voting Consortium, http://www.openvotingconsortium.org/) is a nonprofit group of software engineers and computer scientists working to build an open source voting system that will run on PC hardware and produce a voter-verifiable paper ballot. The group also hopes to provide a general standard for interoperable open source voting software.

PRUDENT PRECAUTIONARY MEASURES FOR DREs

Because paperless DREs provide no audit trail, it's imperative that they be extensively tested before, during, and after each election. DREs must also be securely stored *between* elections, as well as at polling sites before and during Election Day.

Similarly, all of the ballot definition files should always be scrupulously tested—with all test results (not just the BDF tests) not only made public but also archived in a central repository. In addition, there should also be a national repository of DRE problems, just as is the case with aircraft.

Finally, paper ballots should be made available at every polling location that uses DREs, both as backup in the case of failures of the DREs and to provide voters with the option of voter-verifiable paper ballots.

None of these steps can ensure that DRE software is free of malicious code and potentially damaging bugs. The best we can do is attempt to reduce the risks associated with these machines.

CONCLUSION

The issue of e-voting should have been primarily a technological issue—one that involves computer security, human factors, reliability, and efficiency. Unfortunately, within the political sphere, things are rarely quite so simple.

Election officials have had to endure a painful learning experience. Having been told that DREs were inexpensive to operate and were extensively tested and certified to ensure reliable and secure service, they've since learned that the costs associated with testing and securely storing DREs are high, the testing and certification processes are suspect, and the software is far from bug-free.

The education process continues as technologists make concerted efforts to inform both policy makers and the public about the risks associated with paperless DREs. It is critical for the continued health of democracy that we succeed.

ACKNOWLEDGMENTS

Thanks to Dan Wallach, Tracy Volz, Laura Gould, Lynn Landes, Rebecca Mercuri, and Doug Jones for their very useful comments. Q

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

BARBARA SIMONS earned her Ph.D. from U.C. Berkeley and was a computer science researcher at IBM Research, where she worked on compiler optimization, algorithm analysis, and scheduling theory. A former president of ACM, Simons co-chairs the ACM's U.S. Public Policy Committee (USACM). She served on the National Science Foundation panel on Internet Voting, the security peer review group for the Department of Defense's Internet voting project (SERVE), the President's Export Council's Subcommittee on Encryption, and the President's Council on the Year 2000 Conversion. She is a Fellow of ACM and the American Association for the Advancement of Science.