

Election Auditing Is an End-to-End Procedure

Ted Selker

After the 2004 U.S. presidential election, allegations of voting machine irregularities appeared on blog sites and in the press. However, numerous pieces of evidence suggest that electronic voting machines outperformed all other methods used in November's election (1, 2). Data indicate that the residual vote rate (i.e., the number of uncounted votes resulting from an unintentional or intentional nonvote for the presidential race) dropped from 1.91% in 2000 to 1.07% in 2004, with the most dramatic improvements occurring in states that invested heavily in new election technology, as well as improved training and procedures (3). Nevertheless, we may never be able to remove lingering doubts because—in spite of the enormous sums of money, energy, and brainpower that have been expended to improve the election process since 2000 and in spite of the significant strides forward that have been made—we have been sloppy in our procedures and in our record-keeping.

These concerns have fueled movements to pass legislation in many states that would require a paper record of every vote (4). However, I believe the Voter-Verifiable Paper Audit Trail (VVPAT), designed to do this for direct record electronic (DRE) voting machines adds complexity to the tasks that voters, poll workers, and officials perform—increasing confusion and even possibilities for error (5). While observing Nevada's September deployment of machines, I witnessed poll workers place paper-trail printers in unsecured spots; open the printers without supervision (they should be handled like ballot boxes); and even, in a muddled attempt to reload the paper in a jammed printer, cut out portions of the paper-trail record. Nevada's Secretary of State reported that these state-of-the-art units added \$500 to the cost of each DRE (6). Problems observed during earlier tests of Avante's paper-trail system in Sacramento, CA, and Wilton, CT, were even worse (75). I have witnessed similar mishandling of ballots and equipment when the optical scan sys-

tem was used. Such mistakes illustrate that machines work only as well as the people who operate them. Any audit trail system is only valuable to the extent that voters, poll workers, and officials successfully operate it.

People tend to be suspicious of new machines whose inner workings are mysterious (8, 9). Such fears intensify when we rely on unfamiliar technology to determine results of a heated and close election. The public's inherent distrust of voting technology has been reinforced by lost votes in

2000 and continued confusion. Those forging future elections must not only make a system that works, but also prove to Americans that it does so. Voter verification should be only one part of supervising a complex process (10, 11).

To maximize security during the design phase, the architecture of voting technology can be broken into modules that are designed by separate teams, so that no one person would have knowledge of the entire program (12). However, sophisticated code design cannot replace thorough testing.

Proving program correctness is theoretically unsolvable (13, 14). Testing large circuits or programs is accomplished by testing them in pieces for all possible input scenarios (15). New methodologies for improving code quality, such as extreme programming in which small teams work intensively on component modules, institutionalize good practices of incremental testing (16). In addition, this technique inherently reduces the ability of any one person to have access to the entire code.

Systems must be tested as a whole for all possible input. In the case of voting machines, so-called logic and accuracy

tests are designed to do this. Code programming must be examined as comprehensively as possible to confirm that "malware" has not been fraudulently imbedded.

Maryland and California are among states that have instituted a policy of "parallel monitoring" (17), in which a random selection of voting machines is taken out of service on Election Day and test-voted at the same time as the actual polling machines. This method can provide assurance that the test machines are identical to those being used and makes it impossible for a malevolent coder to distinguish between the two groups in advance.

If parallel testing or certification audits show problems, we might rerun an election, as recently happened in the Ukraine. Even better would be to avoid such a costly necessity by demonstrating before

an election that voting machine do not have malware and then securing them. Brittan J. Williams at Election Center has successfully caught problems with advance testing of equipment in Georgia, which showed the most dramatic improvement of its residual vote rate of any state in 2004 (18). Current Federal Election Commission (FEC) guidelines require voting

machines to include internal clocks, which can be forwarded and then tested for software designed to attack on Election Day. One problem with this approach is that the clocks can be programmed to behave differently during an election that at other times; the Nedap Powervote currently used in the Netherlands does not rely on an internal clock (19).

The ability of voters and poll workers to operate voting technology successfully must be as thoughtfully conceived and extensively tested as its security. In 2000, more than 1.3 million votes were lost because of ballot design problems such as the infamous butterfly layout (20). The biggest improvements in error rates in 2004 occurred in states, such as Georgia, that invested heavily in training and voter education, as well as in machines (3). In spite of widespread expectations that the massive increase in unfamiliar voting systems would result in millions of troubleshooting calls, the Election Incident Reporting System recorded under 3000 complaints relating to voting machines nationwide (21). These results are encouraging; nevertheless, forensic data and experi-

The author is codirector of the CalTech/MIT Voting Technology Project and is at Massachusetts Institute of Technology, Cambridge, MA 02139, USA. E-mail: selker@media.mit.edu

ments with current equipment estimate that a significant number of voters accidentally make selections other than what they intend to (19, 22). Therefore, system developers must seek new ways to simplify the voting process.

Improving voter accuracy is an achievable goal. For example, a new electronic ballot design, known as the Low Error Voting Interface (LEVI) has been shown in tests to reduce errors by half (23). Among its innovative features, a contemporaneous review sidebar at the edge of the page displays status for each race, which visibly changes as the voter successfully enters a selection. The concept of voter verification offers a similar opportunity to let voters review and correct their work.

An ideal system would improve voting accuracy even as it creates a back-up record for auditing purposes. Moreover, a true verification audit trail should confirm that a vote has been received into the final counting lot, not just into the local precinct machine. By means of special architectures with redundancy and cryptographic controls to guard against manipulation or unwarranted control, the precinct machine could instantaneously transfer a voter's selections to the central counting office, which would return a report confirming receipt (12). Voters might also be able to reconfirm, by computer, that their ballots are part of the final count. To avoid the possibility of reports being used to collect purchased-vote fees, ballot selections would not be displayed.

David Chaum and VoteHere promote work with cryptographic records that could allow voters to keep a receipt, which, without printing the actual completed ballot, could later be reassembled to prove that it had not been altered (24). Another verification method, Voter-Verified Audio Audit Transcript Trail (VVAATT), uses a voting machine's existing audio output, earphones, and an inexpensive tape recorder, which is locked in a box, to create an audit transcript (25). The machine speaks the name of each candidate that a voter selects, and the recorder tapes the entire sequence for each ballot. A primary advantage is that audio prompts help voters recognize unintended selections as they proceed, so that they can immediately correct mistakes (26). In addition, if a recount is necessary, the taped transcript can be tallied by hand or by machine.

When a voter realizes that the vote cast is not what was intended, there is a natural human reaction to blame the machine rather than to accept responsibility for pressing the wrong button (26). A policy

of videotaping voters from behind could be used to allow voters to check any claim of machine malfunction. To preserve secrecy, the videotape should overwrite itself. VoteGuard is a screen capture verification system that does not require a camera (27).

Regardless of the method, polling-place setup and procedure constitute two of the weakest links in our ability to audit elections. I have witnessed poll workers take ballots out of ballot boxes without supervision; erase and change records; give voters incorrect ballots (electronic and physical); send voters to nonfunctioning booths; misinstruct voters on how to use the voting machine; check over completed ballots; hang over people voting in booths; and transport records and voting materials to the counting place without a corroborating witness (5).

Principles for assuring that voting materials are handled in secure ways are commonly overlooked or ignored. Fortunately, these problems should be the easiest to fix. However, such changes require thoughtful collaboration between technology developers and election officials.

There must also be adequate training for poll workers to ingrain good habits, such as always working in pairs to corroborate how ballots and equipment have been handled. Mutual oversight has always been crucial to securing any election process.

Simple changes like banning the use of pencils that can be easily erased for polling-place recordkeeping may do as much to improve election auditing as advanced voting technology. To secure an election properly, we must look for all of the possible points of failure, check for problems at each of them, and document what has been done at every step. Throughout the process, a team of publicly accountable bipartisan and nonpartisan observers should be required to check over and sign off on every phase—from the development and testing of machines to the counting of votes and storage of records. Let us revisit the entire process before we pass expensive and counterproductive legislation.

References and Notes

1. D. Kimball, "Summary tables on voting technology and residual vote rates"; available at www.umsi.edu/~kimball/rtables.pdf
2. C. Stewart III, Addendum to voting machines and the underestimate of the Bush vote, December 2004; available at http://vote.caltech.edu/media/documents/Addendum_Voting_Machines_Bush_Vote.pdf
3. C. Stewart III, Residual vote in the 2004 election, February 2005; available at http://vote.caltech.edu/media/documents/vtp_wp21v2.3.pdf

4. [This or some other reference] R. Kibrik, www.verifiedvoting.org/article.php?list=type&type=13
5. T. Selker, *User Experience* 4, 1 (Spring 2005).
6. [Author, add ref. here].
7. C. B. McCormack, Presentation to the U.S. Election Assistance Committee (EAC), Hearing on Use, Security, and Reliability of Electronic Voting Machines, 5 May 2004; available at www.electiontech.org/downloads/EACtestimony505.pdf
8. A. H. Teich, *Technology and the Future* (Wadsworth, Belmont, CA, 2003).
9. R. Mehuri, *IEEE Spectrum* 39, 10 (November 2002).
10. E. Fischer, "Election reform and electronic voting systems (DREs): Analysis of security issues; CRS report for Congress" (RL32139, Congressional Research Services, Library of Congress, Washington, DC, 4 November 2003).
11. R. G. Saltman, "Accuracy, integrity, and security in computerized vote-tallying" (Spec. Publ. 500-158, U.S. National Bureau of Standards, Washington, DC, 1989).
12. S. D. Liburd, thesis, Massachusetts Institute of Technology (2004).
13. K. Thompson, *Commun. ACM* 27 (XX), 8 (1984).
14. P. Popov, L. Strigini, *IEEE Trans. Software Eng.* 29, 4 (2003).
15. B. Berard et al., *Systems and Software Verification: Model-Checking Techniques and Tools* (Springer-Verlag, New York, 2001).
16. S. Ambler, R. Jeffries, *Agile Modeling: Effective Practices for eXtreme Programming and the Unified Process* (Wiley, New York, 2002).
17. California Parallel Monitoring Program, "Report of findings for November 2, 2004" (Secretary of State of California, Sacramento, 2004); available at www.ss.ca.gov/elections/november2004_pmp_report.pdf
18. B.J. Williams, M. S. King, *Commun. ACM* 47 (10), 39 (October 2004); available at http://theory.lcs.mit.edu/~rivest/voting/reports/cacm/2004-10_CACM_p39_Williams_King_-_Implementing_Voting_Systems_-_The_Georgia_Method.pdf
19. R. Sinnott et al., in "First report—December 2004" (Irish Commission on Electronic Voting, Dublin, 2004) Appendix 2C, pp. 153–191; available at www.cev.ie/html/report/first_report/pdf/Appendix%202C.pdf
20. R. M. Alvarez et al., "Voting: What was, what will be, (Caltech/MIT Voting Technology Project (VTP), California Institute of Technology, Pasadena, CA, and MIT, Cambridge, MA, July 2001); <http://www.vote.caltech.edu/reports/2001report>.
21. Election Incident Reporting System, 2004 reported machine problems, 2005; available at https://voteprotect.org/index.php?display=EIRMapNation&tab=ALL&cat=02&start_time=&end_time=&end_date=&search=
22. S. M. Sled, "Vertical proximity effects in recall" (VTP Working Pap. 6r, Caltech and MIT, October 2004); available at www.vote.caltech.edu/Reports/vtp_WP6r.pdf.
23. T. Selker, Presentation at Caltech/MIT Voting Technology Project Symposium, Cambridge, MA, 2 October 2004; available at www.vote.caltech.edu/events/2004/voting-tech
24. Voting technology: Innovations for today and tomorrow, Caltech/MIT Voting Technology Project Symposium, Cambridge, MA, 1 and 2 October 2004; available at <http://www.vote.caltech.edu/events/2004/voting-tech>
25. T. Selker, *Sci. Am.* 291, 4 (MONTH 2004).
26. S. Cohen, T. Selker, "An active approach to verification (VTP Working Pap. 28, Caltech and MIT, May 2005), available at http://vote.caltech.edu/media/documents/wps/vtp_wp28.pdf
27. See <http://www.vote-guard.com/10.1126/science.1109901>

Additional resources

IEEE Voting Equipment Standards Project
1583 <http://grouper.ieee.org/groups/scc38/1583/>

[Figure:] A paper-trail printer being opened
without supervision during the 7 September
2004 election.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65