Elections: Where We Are and Where We Must Go

written comments addressed to the Election Assistance Commission
May 5, 2004
by

Douglas W. Jones

Department of Computer Science
University of Iowa
Iowa City, Iowa 52242
jones@cs.uiowa.edu

A Brief Personal Statement

I have taught Computer Science at the University of Iowa for 24 years, and am a long-time member of the Association for Computing Machinery, the American Association for the Advancement of Science and Computer Professionals for Social Responsibility. A decade ago, I volunteered to serve on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, on which I still serve; In 1999 I was elected chair of the board, a position in which I served for 3 years; my appointments to the board is by the Secretary of State, and I have served under both Republicans and Democrats.

Elections, election machinery, and the system of regulation we have for that machinery are all complex, and it took me a good five years before I felt confident to begin speaking out in public about the failings of the way we regulate voting systems in the United States. My first public criticism of our voting system standards was posted on the Internet in the Spring of 2000.

Since the election of 2000, questions about voting systems have consumes the majority of my creative efforts. I helped found the Open Voting Consortium, of which I am now Vice President and Chief Technical Officer, I serve on the advisory board of Verified Voting, and I have joined USACM, the US Public Policy Committee of the Association for Computing Machinery.

Where We Are Now

Elections are the defining institution in a democracy, and the integrity of the system of elections is essential to the integrity of any democratic nation. The integrity of the technology used for elections in the United States was brought into question by the events of Election 2000 [1,2], when widespread attention was focused on the failings of punched-card voting systems. The reforms instituted after that election, most notably the Help America Vote Act of 2002 (HAVA) [3], led to the rapid and Federally subsidized replacement of punched-card voting systems with new equipment, generally based on either optical mark-sense technology or direct-recording electronic voting systems.

While each of the 50 states are free to select their own voting systems under broad technical outlines set by civil rights law and by HAVA, Most states have opted to require conformance to a set of voluntary standards promulgated by the Federal Election Commission and the National Association of State Election Directors in 1990 and revised in 2002 (the FEC/NASED standards) [4,5]. These standards remain voluntary only in the sense that the Federal government does not require that vendors seek certification or that states demand conformance to these standards. Technically, HAVA has removed the authority for voting system standards from the FEC, moving this to the Federal Election Assistance Commission, however, until these standards activities are properly funded, we cannot expect significant changes.

I called the adequacy of the FEC/NASED standards into question in 2001 [2], and in 2003, these warnings were confirmed when one voting system vendor, Diebold Election Systems, accidentally disclosed the source code for the software used in their AccuVote TS voting system to the public [6]. This story exploded into the press with the public release of a report documenting serious security flaws in this system (the Hopkins report) [7]. While the vendor has strenuously denied the significance of these flaws [8], subsequent reports commissioned by the state of Maryland from Science Applications International Corporation (SAIC) [9] and RABA Technologies [10] and by the state of Ohio from InfoSentry [11] and Compuware [12] substantially confirm all of the major security flaws identified in the Hopkins report and identified several additional flaws. It is noteworthy that none of these studies are complete; each has missed some of the security flaws identified in the others.

All voting systems certified under the FEC/NASED standards are subject to testing by Federally certified independent testing authorities, and these tests include a source code audit, the detailed results of which are confidential. The original source code audit for the system that would later become the Diebold AccuVote TS system was available to me in my capacity as a member of the Iowa Board of Examiners for Voting Machines and Electronic Voting systems [13]; this report indicated that the software of this voting system was the best the examiners had ever seen and that they were particularly impressed by its security. In the light of the security flaws that were evident in that report [2, Jones testimony], and in light of the even more severe flaws revealed since then [7,9,10,11,12], such an evaluation calls into question both the examination process and the security of all other voting systems in the marketplace!

It is worth asking, why would a Federally certified testing laboratory declare a voting system to be secure while 5 other reviews of that same system found major flaws? The answer lies, in part, in the question being answered. The Federally certified lab asked if the system met the FEC/NASED standards, while the other reviewers simply asked if the system was secure and applied their own reasonable definitions of what it means to be secure. This calls into question the FEC/NASED standards themselves as much as it calls into question the competence of the Federally certified examiners.

There is a second problem with standards that offers a second answer to this question. When a standard poses some requirements that are broad and general, for example, that a system be secure, while providing other requirements that are specific and easily tested, for example, that single-letter identifiers be used only as loop-control variables, the enforcement and testing will naturally focus on the latter. If it cannot be quantified or measured, it is easy to ignore, and unfortunately, freedom from error or malicious content is extremely difficult to quantify or measure.

While the reports done for Maryland only cover the security of the Diebold AccuVote TS, the reports for Ohio [11,12] also cover systems made by Election Systems and Software, Hart InterCivic, and Sequoia. These 4 vendors, together, dominate the marketplace for voting systems in the United States, and the Ohio reports make it clear that, indeed, the FEC/

NASED standards process has not ensured that voting systems meet any useful security standards.

The four state-sponsored reports identify serious security problems in the administrative rules and procedures governing the use of voting systems in Ohio and Maryland. In an additional audit of voting equipment used in 17 California counties, unauthorized voting software was in use in every one of these counties [14]. We have had problems with vendors installing unauthorized systems in Iowa counties as well, and I have heard recent reports of similar problems in Florida. Taken together, these findings bring into question the assertion that "checks and balances in elections equipment and procedures"[8] are sufficient to defend the security of our current voting technology. While some of these checks and balances may exist on paper, in practice, many of them have been shown to be ineffective.

Where We Must Go

The RABA report [10] recognized that it is unrealistic to expect states that have invested millions in new voting technology to abandon it immediately, so it suggested that states pursue short-term strategies to address security problems in the current primary season, medium-term strategies for the fall general election, and long-term strategies for the future.

While I differ with some of the details the RABA report suggests, I endorse this general strategy. There is time, before the fall general election, to undertake serious reviews of state administrative rules, instituting reforms that markedly increase our confidence in election security. Canvassing procedures, auditing procedures, and physical security measures can and must be improved for the systems already in use, not only direct-recording electronic voting systems, but also optical mark-sense systems; all four state sponsored reports include numerous appropriate recommendations along these lines.

Furthermore, if we cannot strengthen the machinery of elections, we can strengthen its oversight. If election officials know they are being watched by suspicious and well informed observers, they will generally conduct their business more carefully then they might otherwise. Generally, the right of public observation of election procedures in the United States has fallen into disuse except for purposes of partisan get-out-the-vote drives. I strongly recommend that we urge people to use this right, and that we encourage the organization and education of a corps of volunteer observers to closely monitor compliance with election law and procedure and to audit, to the extent possible, the canvassing process.

In the long run, we must insist on voting systems that meet a standard of auditability comparable to the standards we apply to the financial world, where we insist that no individual or small group of people be put in a position where they can safely falsify records, and where sufficient information is saved that errors and deliberate falsification can be detected and corrected by auditors. Furthermore, we know that auditing in the financial world must be performed routinely, not just in response to allegations of fraud. Similarly, we must audit elections routinely and not just in response to allegations of irregularities.

We must insist on the same level of oversight for counting votes as we have routinely insisted on for counting dollars. Today's direct-recording electronic voting systems simply do not allow this level of oversight, even if we apply every recommendation the SAIC and Compuware reports contained for the voting system vendors [9,12]. With the technology available today, I see no way that such oversight can be provided without maintaining a voter-verified paper record of each vote cast.

Furthermore, we must recognize that all of our defenses are likely to contain holes. While there may be provably secure models for certain aspects of the election process, none of these models cover the entire process from end to end, and proofs of the implementations of such models are generally infeasible. Therefore, as in all other realms of secure computing, we must adopt a philosophy of defense in depth [15].

As an example of appropriate defense in depth, we can augment reliance on certified voting systems with requirements that these systems provide audit trails that allow voters to verify that their votes were correctly recorded by the system and to allow auditors to determine that the system correctly counted those votes. Such an audit trail is merely decorative, however, if it is not used, routinely, for auditing, and it is clear that we can also improve the system with a robust system of testing, including not only token pre-election tests, but intensive parallel testing of randomly selected machines.

References Cited

[1] *Voting Irregularities in Florida During the 2000 Presidential Election*, Report of the United States Commission on Civil Rights, June 2001.
➠ http://www.usccr.gov/pubs/vote2000/report/main.htm

[2] *Improving Voting Technology*, Hearing before the Committee on Science, House of Representatives, 107th Congress, Washington DC, May 22, 2001. USGPO Serial No. 107-20.

[3] Help America Vote Act of 2002, Public Law 107-252.

[4] *Performance and test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems*, Federal Election Commission, April 1990.

[5] *Voting System Standards*, Federal Election Commission, April 2002.
➠ http://www.fec.gov/pages/vssfinal/vss.html

[6] Eric A. Fischer, *Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues*, Congressional Research Service RL32139, Nov. 4, 2003.
➠ http://www.epic.org/privacy/voting/crsreport.pdf

[7] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin and Dan S. Wallach, *Analysis of an Electronic Voting System*, July 23, 2003.
➠ http://avirubin.com/vote.pdf

[8] *Checks and Balances in Elections Equipment and Procedures Prevent Alleged Fraud Scenarios*, Diebold Election Systems, July 30, 2003.
➠ http://www2.diebold.com/checksandbalances.pdf

[9] *Risk Assessment Report: Diebold Accuvote-TS Voting System and Processes*, as redacted by the State of Maryland, Science Applications International Corporation SAIC-6099-2003-261, Sept 2, 2003.
➠ http://www.dbm.maryland.gov/SBE

[10] *Trusted Agent Report -- Diebold AccuVote-TS Voting System*, RABA Technologies, Jan. 20, 2004.
➠ http://www.raba.com/text/press/TA_Report_AccuVote.pdf

[11] *DRE Security Assessment, Volume 1, Computerized Voting Systems, Summary of Findings and Recommendations*, InfoSENTRY, 21 November 2003.
➠ http://www.sos.state.oh.us/sos/hava/files/InfoSentry1.pdf

[12] *Direct Recording Electronic (DRE) Technical Security Assessment Report*, Compuware Corporation, 21 November 2003.
➠ http://www.sos.state.oh.us/sos/hava/files/compuware.pdf

[13] *Qualification Testing of the I-Mark Electronic Ballot Station*, Report No 45450-01, Wyle Laboratories, Huntsville Alabama, Sept. 10, 1996. This report is confidential! The only content of this report disclosed here is material that was discussed in open meetings of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems.

[14] *Minutes*, Meeting of the State of California Secretary of State Voting Systems Panel, Dec. 16, 2003.
➠ http://www.ss.ca.gov/elections/vsp_min_121603.pdf

[15] *Defense in Depth*, National Security Agency Security Recommendation Guide number 1.
➠ http://nsa2.www.conxion.com/support/download.htm