

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield et al.,	:	
	:	
Petitioners	:	
	:	
v.	:	
	:	No. 442 M.D. 2006
Pedro Cortes,	:	
Secretary of the Commonwealth,	:	
	:	
Respondent	:	

CERTIFICATION OF DOUGLAS W. JONES, Ph.D

QUALIFICATIONS AND SUMMARY OF OPINIONS

1. It is my opinion that none of the six DRE Voting systems, (Danaher ELECTronic 1242, Diebold (now Premier) TSx, ES&S iVotronic, Hart Intercivic eSlate, Sequoia Edge II and Sequoia AVC Advantage) certified by the Pennsylvania's Secretary of the Commonwealth, Pedro Cortes, 1) provides for a permanent physical record of every vote cast; 2) permits a statistical recount of a random sample of ballots using manual, mechanical or electronic devices of a type different than those used for the specific election and 3) is secure enough against a tampering threat that could alter the outcome of an election.
2. These opinions are based upon my training and professional experience as a professor of computer science specializing in computer security; my review of a large body of current scholarly work on the subject of electronic voting system security and of technical specifications and publications of DRE system manufacturers; other information gathered over the years at conferences, seminars and workshops on electronic voting systems and my examination of DRE machines for several states. To the extent that I have been unable to examine a particular vendor's electronic voting system with the exact version number certified for use in Pennsylvania, defects identified in prior versions discussed here are, based on my longstanding study of these systems, structural and persistent.
3. I am an Associate Professor at the University of Iowa, Department of Computer Science, where I have taught since 1980. I received my Ph.D. and MS degrees in Computer Science from the University of Illinois at Urbana Champaign, in 1980 and 1976, respectively, and a BS degree in Physics from Carnegie-Mellon University in 1973.
4. My expertise in voting technology includes the following:
5. I served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems from 1994 to 2004, and chaired the board for 3 terms. This board examines all voting systems offered for sale in the state of Iowa to determine if they meet the requirements of Iowa law.
6. I was invited to testify before the United States Commission on Civil Rights on evaluating

voting technology for their January 11, 2001 hearings in Tallahassee Florida. I was invited to testify before the House Science Committee on problems with voting systems and the applicable standards for their May 22, 2001 hearings. I was invited to testify at an April 17, 2002 hearing of the Federal Election Commission. At that hearing, I recommended changes to the draft voting system standards that were subsequently adopted as the 2002 FEC Voluntary Voting System Standards.

7. I wrote Chapter 1 of *Secure Electronic Voting*, edited by Dimitris Gritzalis and published by Kluwer Academic Publishers in 2002.
8. In the summer of 2004, I consulted with Miami-Dade County to assess problems with their ES&S iVotronic touch-screen electronic voting system and to assess their pre-election testing of their touch screen and optical scan voting systems. As part of this consultation, I was able to examine the iVotronic and a substantial amount of accompanying documentation.
9. My paper, *Auditing Elections*, was published in October, 2004 in the *Communications of the Association for Computing Machinery*.
10. I am one of the ten principal investigators in A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections (ACCURATE), a multi-institutional center awarded a 5-year research grant by the National Science Foundation starting in October 2005.
11. I have served as an electronic voting expert for election observation and assessment missions run by the Office for Democratic Institutions and Human Rights of the Organization for Security and Cooperation in Europe in Kazakhstan (November 2005, August 2007) and Holland (November 2006).
12. In December 2005, I was invited by the Arizona Senate Government Accountability and Reform Committee to investigate the Optech 4C absentee vote tabulation system being used in Maricopa County.
13. I served as an expert witness in the case of *Conroy v. Dennis* in Colorado in 2005, where I was asked to assess the voting system assessment process conducted by the State of Colorado. In this context, I was allowed to examine all documents submitted to Colorado by Diebold, ES&S, Hart and Sequoia in their most recent rounds of voting system certifications in that state.

Documents Reviewed

14. I have been asked to examine several recent reports produced for California and Ohio in order to assess those reports and their implications for the use of direct recording electronic (DRE) voting systems in Pennsylvania. For this review, I have examined the following documents:
15. From the California Top to bottom Review of voting systems (TTBR), performed by teams convened by the University of California, I have examined the Source Code, Red Team and Documentation reviews of the Hart, Sequoia and Diebold (since renamed Premier) voting systems. These documents are available from the California Secretary of State web site, http://www.sos.ca.gov/elections/elections_vsr.htm
16. From the Ohio Evaluation & Validation of Election-Related Equipment, Standards & Testing (EVEREST) reports, I have examined the Evaluation and Validation of Election-Related Equipment, Standards and Testing report produced by researchers from Penn State, the University of Pennsylvania and WebWise Security on the ES&S, Premier and Hart voting systems. I also examined the reports on red-team testing conducted by Microsolved Inc. on these same systems as part of the EVEREST project. All EVEREST documents are available from the Ohio Secretary of State web site,

17. I have also reviewed the definitions of the terms Electronic Voting Systems and Ballot in the Pennsylvania Election Code 25 P.S. § 3031.1 Definitions, some of the requirements for Electronic Voting Systems set forth in 25 P.S. § 3031.7, the requirements for statistical sample set forth in 25 P. S. § 3031.17, and the provisions for a recount or recanvass of the vote set forth in 25 P.S. § 3154 (e).

Preferatory remarks on voting system security

18. Secure voting is extremely difficult, whether done using manual, mechanical or electronic means. While the algorithms involved are trivial, requiring nothing more than a sum, for each candidate or ballot position, of the number of votes, the distributed nature of the computation and the number of participants pose immense problems. Elections involve an appreciable fraction of the entire national population as participants, and the history of election fraud includes examples that were perpetrated by every class of participant, from voter to polling place election judge to election administrator to voting system maintenance technician.
19. All of today's voting systems are software based, with the exception of hand-counted paper ballots and mechanical lever voting systems. The correctness of this software is central to the trustworthiness of our election results, and because the current system of software certification is seriously flawed, the move to computerized election technology has simply replaced known evils with poorly understood systems without necessarily addressing the underlying problems. This is essentially the same thing we did a century ago when most of the nation began its move from paper ballots to mechanical lever voting systems.
20. Our current system of voting system certification illustrates a major failure in voting system transparency. Although the Federal Election Assistance Commission is slowly changing things, voting system testing under the FEC/NASED voting system standards (1990 and 2002) has been an entirely closed process. The testing authorities have not been obligated to disclose any report of their testing to the public other than a simple pass-fail judgment, while hundreds of pages of test results are sent back to the vendors.
21. There is an overwhelming public interest in the integrity of our election machinery, and this interest extends to all questions about the competence and thoroughness of the testing to which our voting systems are subjected. As things stand, the voting system vendors have been allowed to hide behind a myth of thorough and painstaking testing, telling not only the public but also state and county authorities that these tests prove the security of their systems when they do no such thing. The California TTBR and Ohio EVEREST reports conclusively destroy this myth, demonstrating that this process has allowed seriously defective voting systems to remain in the marketplace for over a decade.
22. The central problem with voting system certification is that no individual or small group of individuals can or should be trusted. The potential gains from a corrupt election are immense, and over the course of history, this has driven many individuals and corrupt organizations to undertake great efforts to gain control over the machinery of elections. Therefore, a credible system of software certification for voting systems must rely on open disclosure of all software that can possibly have an impact on the outcome of the election. We do not have such open disclosure now, because the voting system vendors treat their software as proprietary trade secrets.

Some legal issues

23. In assessing the use of DRE voting systems for use in Pennsylvania, Pennsylvania law raises

some significant puzzles. 25 P.S. § 3031.1 Definitions requires that electronic voting systems maintain “a permanent physical record of each vote cast”. In my opinion, flash memory or equivalent technologies should not be construed to be permanent physical records.

24. Flash memory or equivalent technologies such as battery-backed random-access memory (RAM), electrically erasable programmable read only memory (EEPROM), erasable programmable read-only memory (EPROM), and magnetic disk drives are all examples of non-volatile memory. That is, while their contents does not spontaneously change (within the design lifetime of the memory), all of them permit erasure, alteration, and reuse. Thus, in my opinion, non-volatility is not the same as permanence.
25. All of the DRE voting machines from ES&S, Hart, Sequoia and Premier and Danaher use some form of flash memory or equivalent non-volatile memory. There is considerable variation in detail, but all allow their memory to be cleared and reused from one election to the next.
26. The statistical sample required in 25 P. S. § 3031.17 involves a recount of a random sample of the ballots cast in an election. The word ballot, as defined in 25 P.S. § 3031.1, is defined in a manner that permits a statistical sample only in the context of ballot cards and paper ballots. In contrast, in the context of electronic voting systems, the word ballot is defined as “the apparatus by which the voter registers his vote electronically”. Thus, the DRE voting machine itself is defined as the ballot.
27. The statistical sample is also required to be done “using manual, mechanical or electronic devices of a type different than those used for the specific election.” In the case of a DRE voting machine, the machine is only capable of producing a facsimile of the ballot images it has recorded in its internal memory prior to a count of the votes on that facsimile. I use the term ballot image here to refer to the record maintained by the voting mechanism of the selections made by a single voter; this usage comes from the 1990 FEC Voting System Standards. The problem here is that this facsimile was necessarily produced by the same DRE voting machine as was used to produce the first count, and it is certainly not produced by something of “a type different” from that used in the original election.
28. Based on my knowledge of the way DRE electronic voting machines record data to their memory devices, in my opinion, recounting ballot images produced by the same software that recorded and tabulated votes in a specific election is not a recount using a device of a type different than those used in the specific election.

Problems with workmanship

29. Pennsylvania law, 25 P.S. § 3031.7, requires that electronic voting systems be “(11) ... constructed in a neat and workmanlike manner ...” The California TTBR and the Ohio EVEREST source code reviews confirm that none of the machines examined meet this requirement in regard to their software, including what is frequently mischaracterized as firmware. It is not practical to enumerate all of the problems encountered in these studies, but the following examples should suffice to illustrate the pervasiveness of problems with workmanship:
30. The California TTBR Source Code Review of the The Diebold Voting System notes many problems that can best be described as defects in workmanship. It noted that Diebold's programs usually omit input validation (Section 4.2.1) and made only irregular use of defensive programming (Section 4.2.2). These are a systematic source of security vulnerabilities across the entire product line. In the TSx, this shows up, for example, in the comment that there are “multiple buffer overflows in .ins file handling [that] allow arbitrary code execution on startup

(Issue 5.2.3). Similarly “A buffer overflow in the handling of IP addresses might be exploitable by voters” (Issue 5.2.17). Finally “AV-TSX startup code contains blatant errors” (Issue 5.2.24); the latter defect led to the comment that “this bug sheds light on the vendor’s software engineering practices ... The probability that an experienced C++ programmer would make such a mistake or overlook it during even a cursory review of the code is exceptionally low. This suggests to us that after this code was written it was not reviewed by any other engineers at Diebold.”

31. The Ohio EVEREST Evaluation and Validation of Election-Related Equipment, Standards and Testing notes, for the ES&S iVotronic, a similar range of defects in workmanship, typically involving failure to properly validate inputs and apply other defensive programming methods. For example “the iVotronic does not verify that allocated memory buffers are sufficiently large to store variable length strings ... during the poll opening process” (Section 7.2.5). Similarly “The logic that reads image files from the Compact Flash card has an exploitable stack-based buffer overflow” (Section 7.2.6).
32. The Ohio EVEREST Evaluation and Validation of Election-Related Equipment, Standards and Testing notes, for the Hart system in general, that “there are a multitude of exploitable errors caused by poor coding practices; buffer overflows, printf attacks, integer overruns, unchecked or inconsistently checked and propagated error conditions” (Section 9.1.12).
33. The California TTBR Source Code Review of the Sequoia Voting System also notes many problems that can be described as defects in workmanship. Again, a common problem is a lack of input validation and defensive programming. For example “due to poor input validation of endorsements, it is possible to [cause] ... the Edge to enter an infinite loop while generating reports” (Section 4.4.10). Similarly, “memory allocation may cause integer overflows. Several memory allocation routines used in the Edge show fragile programming practices that are prone to introduce vulnerabilities” (Section 4.4.16). Another example of poor workmanship is that “the Edge contains several instances of dead code” (Section 4.4.20). Dead code is software that is never used, the presence of dead code is evidence of sloppy development practices and poor quality control.

Problems with design

34. Pennsylvania law, 25 P.S. § 3031.7, requires that electronic voting systems be “(11) ... suitably designed for the purpose used ...” The California TTBR and the Ohio EVEREST source code reviews confirm that none of the machines examined meet this requirement in regard to their software, including what is frequently mischaracterized as firmware. It is not practical to enumerate all of the problems encountered in these studies, but the following examples should suffice to illustrate the pervasiveness of significant design flaws:
35. The California TTBR Source Code Review of the The Diebold Voting System notes many problems that can best be described as design flaws. “The AV-TSX automatically installs bootloader and operating system updates from the memory card without verifying the authenticity of the updates” (Issues 5.2.1 and 5.2.2). Similarly, “an attacker with temporary physical access to the inside of the machine’s case could ... compute the System Key from the serial number then use it to decrypt the other keys” (Issue 5.2.5). Or “the smart card authentication protocol can be broken” (Issue 5.2.7) and “Security key cards can be forged and used to change system keys” (Issue 5.2.8).
36. The Ohio EVEREST Evaluation and Validation of Election-Related Equipment, Standards and Testing notes, for the ES&S iVotronic, pervasive design flaws. “The firmware and configuration of the ES&S precinct hardware can be easily tampered with in the field. Virtually

every piece of critical data at a precinct – including precinct vote tallies, equipment configuration and equipment firmware – can be compromised through exposed interfaces, without knowledge of passwords and without the use of any specialized proprietary hardware” and “(Chapter 4). Much of the security of the iVotronic rests on a device called the PEB. “In spite of the proprietary nature of the “official” PEB, ... [it was] relatively simple to emulate a PEB to an iVotronic or to read or alter the contents of a PEB using only inexpensive and commercially available IrDA-based computing devices (such as Palm Pilot PDAs and various mobile telephones)” (Section 6.1.1).

37. The California TTBR Source Code Review of the Hart InterCivic Voting system reveals similarly serious flaws. The Hart eSlate operates only when connected to a device called the JBC. “There is no cryptographic protection for messages on the eSlate-JBC network and therefore there is no authentication, message integrity, or confidentiality” (Section 6.2.3 Issue 5). Voters enter a numeric access code into the eSlate to begin a voting session. “These codes are predictable: anyone who sees a single voter code can compute the sequence of all subsequent voter codes” (Issue 7). Hart provides a mechanism to verify that the firmware of a voting device is the official version, but “the firmware image is provided by the running program, a malicious image [program] can simply provide data that fools the check” (Issue 11). The The Ohio EVEREST Evaluation and Validation of Election-Related Equipment, Standards and Testing notes that the Hart system retains the order in which votes were cast (Section 9.1.8), allowing anyone with access to the MBB (results cartridge, a PCMCIA card) to violate the voter's right to a secret ballot.
38. The California TTBR Source Code Review of the Sequoia Voting System also notes pervasive design flaws. “In the Sequoia system, much of the data that determines the outcome of an election ... reside on removable media that may pass through several sets of hands. ... Unfortunately, the software mechanisms that safeguard these critical election components are largely ineffective or absent from the Sequoia system It is a relatively simple matter to place counterfeit precinct results on Edge Results Cartridges” (Section 3.1). “The keys used to protect the 'firmware update' process are statically defined in the code” (Section 4.4.2). Similarly “The keys intended to be used for Consolidation Cartridge signatures and Results Cartridge signatures are hardcoded” (Section 4.4.4). The use of hardcoded keys or statically defined keys in Diebold software was the subject of national attention in 2003. There is no excuse for any vendor continuing to make this mistake 4 years later. In addition “a person who gains access to the votes stored on a Results Cartridge can determine the original order in which votes were cast” (Section 4.4.8), potentially allowing anyone with access to this cartridge to violate the voter's right to a secret ballot.
39. Where defects in workmanship may be easily corrected, defects in design are much harder to correct. I discovered Diebold's use of hardcoded keys in 1997 at a meeting of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, and at that meeting, I scolded Diebold's representative, Bob Urosevich, for this amateurish mistake. This problem remained in the Diebold system 5 years later, when Khono, Stubblefield, Rubin and Wallach reported it in their paper Analysis of an Electronic Voting System (released as Johns Hopkins University Information Security Institute Technical Report TR2003-19, July 23, 2003, published in the Proceedings of the IEEE Symposium on Security and Privacy, May 2004). Only after that report came out did Diebold make any effort to eliminate these hard-coded keys, and as pointed out above, the mechanism they used to update these keys, the key card, remains ineffectively secured. I would expect the design flaws discussed above to be similarly difficult to correct.

40. These defects are not merely of theoretical interest. The red-teams convened as part of the California TTBR and the Ohio EVEREST efforts were able to exploit the flaws found in every voting system they tested in a way that could be used to corrupt an election.

The Difficult Problem of Software Version Verification

41. To have confidence in an electronic voting system, it is necessary to verify that only specific, tested and certified software is used in any part of the voting system, whether in the voting booth, at the tabulating center or elsewhere. It is necessary but not sufficient because, as the reports discussed above disclose, the certification process itself is seriously flawed. The problem is, how can an observer assure himself or herself that the software that is actually in use is indeed the very same software that has been approved for use?
42. For the computer I am using to write these comments, I can begin to answer this question by clicking on the "About this Mac" option on my screen, which helpfully informs me that I am running Mac OS X Version 10.4.11. This message tells me, with real certainty, that I am not running an authentic version of, say, Mac OS Version 10.3.4, because we can define authentic versions of the operating systems as those versions that honestly report their identity. Unfortunately, the self-reported identity of a piece of software does nothing to assure an observer that this software is honest! Any software, including voting system software, could easily be programmed to report any false version number when queried.
43. In the case of my computer system, I trust the self-report of the system only because I personally installed the original version of the operating system on this machine, using media provided by the vendor, and because I trust the vendor's software update product to make secure connections to their web server to install operating system upgrades. Thus, a central element of my own personal trust here is that I personally had physical control of this computer system since it originally came out of the box.
44. The use of "software fingerprints" computed by some cryptographically secure hash function, as some security specialists have recommended, does nothing to change this fact. So long as the observer is limited to inspecting the self-declaration of identity of the system, there is no way for the observer to know whether that identity is declared honestly or not. The self-declaration that a piece of software has some particular MD5 hash can definitively tell you that the system is not the correct system, if the announced hash value is not the correct one, but it cannot tell you that the system is correct, since dishonest software could easily report a dishonest number.
45. Only if the observer can directly examine the memory of the computer and compare it with a reference memory image can the observer really know that what is in the computer and what is authorized to be there are the same. If we allow this comparison, however, we compromise the author's right to retain this software as a trade secret. In addition, if we are not very careful, the same memory access that allows inspection can also allow modification, thus elevating the election observer to the status of a security threat.
46. It may be possible to protect proprietary software from disclosure to observers if we allow the observer to run their own software on the voting system, where their software has read-only access to the system memory and a very narrow channel through which the software can announce the cryptographically secure hash code it has computed. This requires that the observer trust the processor on the system to accurately run the hash-checking software, it requires that the firewalls protecting the system from the observer's software be secure against

attacks by the observer's software, and it requires careful design of the choked-down channel by which the observer's software can report the hash code without disclosing the proprietary software itself.

47. It is important to emphasize that, to my knowledge, no such verification system is used in any voting system currently sold or used in the United States. The State of Nevada, however, uses a system of similar sophistication to verify that the software used in electronic gaming equipment is indeed the software that they have certified.
48. As discussed above, Hart provides a mechanism that attempts to verify that the firmware of a voting device is the official version, but this mechanism relies on the firmware being tested to provide an accurate copy of itself. As a result, Hart's scheme is still based on self attestation.

Memory Cartridges and Chain of Custody

49. All modern electronic voting systems pose problems that follow directly from the miniaturization of the technology. Where the automatically recorded record of precinct vote totals from a lever machine was recorded on a sheet of paper described as a "bedsheet" because it was so large, the automatic totals produced by a typical precinct-count direct recording electronic (DRE) or optical scan voting system are recorded on media such as compact flash cards or PCMCIA cards. The largest electronic media in common use today include devices such as the Election Systems & Software (ES&S) PEB--used in the iVotronic DRE, one of the voting machines challenged by plaintiffs--which is about 1×3×6 inches in size, or the similar sized memory pack found in the Optech III Eagle precinct-count ballot scanner.
50. If we confine ourselves to precinct-count optical scan or hand count paper ballot systems, note how easy it is for an observer to determine that the ballot box dumped out for hand counting is the same ballot box that was used by voters. Similarly, note how easy it is for an observer to determine that the bedsheet removed from the back of an automatic recording lever voting machine is the same one that the election judges sign and witness for delivery to the county building. In each case, it is easy because the object being observed is large and difficult to conceal.
51. In contrast, when a memory device the size of a large postage stamp or a pack of cigarettes is involved, as is the case with current DRE voting systems, it is vulnerable to sleight-of-hand manipulations. As a result, unlike conventional ballot boxes, it is almost impossible for an observer to see that the memory card inserted in the envelope for transport to the county building is indeed the one that was pulled from the machine only seconds earlier.

Defensive Measures

52. It has long been argued by election administrators and voting system vendors that "checks and balances in elections equipment and procedures prevent alleged fraud scenarios" (the title of Diebold's July 30, 2003 rebuttal to the public release of reports of security flaws in their voting system).
53. I have observed election procedures both in the United States and overseas, and I have personally seen many polling place election officials fail to follow the procedures required by their jurisdictions.
54. I have never personally seen such violations in a context where I believed that there was any malicious intent. I have seen violations that could be attributed to carelessness, but even these are rare. The vast majority of election officials I have dealt with, at all levels, have been both honest and conscientious.

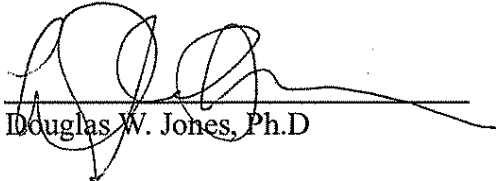
55. The fundamental problem with our reliance on procedural defenses is the sheer complexity of our voting systems. Conducting an honest election is difficult, and this difficulty is magnified by every additional procedural requirement we place on election workers. Procedures that are easy to follow, in isolation, become easily forgotten in the context of a busy polling place after a long election day. The only procedures we can safely rely on are those that are obvious, easy to remember, and easy to do.
56. The sets of procedural defenses required to mitigate the weaknesses that have now been documented for all of the leading DRE voting systems do not meet this criterion.
57. In some cases, as with the vulnerabilities of the ES&S iVotronic PEB interface, there are no feasible procedural defenses. The only procedure that could prevent a voter from attacking an iVotronic through the PEB interface involve violation of the voter's right to privacy in the voting booth.
58. It is dangerous to rely on procedural defenses where the primary threat is from corrupt insiders. Throughout American history, it is fair to say that corrupt political machines have been the perpetrators of most of the election fraud. The historical record of such frauds is very well documented, from the era of Tammany Hall when such fraud first came to public attention, all the way up to the recent past. Therefore, the fact that the vast majority of election officials are honest cannot be taken to imply that all of them are honest.
59. The vulnerabilities of the current breed of DRE voting systems is such that a single dishonest election official with brief access to a single voting system component can cause serious problems. For the Diebold/Premier, ES&S, Hart and Sequoia machines, anyone with access to the results cartridge is in a position to either corrupt a single machine, inject a virus into the entire voting system or violate voters rights to a secret ballot.

Conclusion

60. The only effective defense against the weaknesses discovered by the California TTBR and the Ohio EVEREST studies is the defense mandated by Pennsylvania law, 25 P. S. § 3031.17, a recount of a random sample of the ballots cast in an election. This defense works only if the word ballot is interpreted narrowly as the permanent physical record of the vote cast, where the voter is able to directly inspect and authorize the counting of that record. Paper ballots satisfy this requirement. In my opinion, none of the records maintained by DRE voting machines can be trusted for this purpose.
61. To my knowledge, there has been no in-depth study of the Danaher Controls ELECTronic 1242 system. This is a very old machine (it was formerly the Shouptronic 1242) designed using 1980's vintage technology. I have no reason to believe that it is any more secure than more recent DRE designs.

I hereby certify that the foregoing statements are true and correct. I understand that the statements made in this certification are subject to the penalties of 18 Pa. C.S.A. § 4904 relating to unsworn falsification to authorities.

Date: Jan 23 2008


Douglas W. Jones, Ph.D