Computer Security Versus the Public's Right to Know

by

Douglas W. Jones[*]
University of Iowa
jones@cs.uiowa.edu

Notes for a panel discussion on *Electronic Voting Integrity*
Computers, Freedom and Privacy
Montreal, May 4, 2007, 11:00AM

Abstract: Computer security requires that some information be withheld from the public -- at the very least, passwords and secret keys. When a computer system is operated on behalf of the public, it is equally important that the public be able to assess the security of that system. It is extremely difficult to write rules that balance security and public oversight, and extremely easy to err on the side of security, blocking all public oversight. Examples from the domain of electronic voting clearly illustrate this. Solutions to this problem will require careful balancing in the legislative and rulemaking process.

A Story from Maryland

Maryland public records law includes a clause requiring that the "custodian of a record shall deny a request for disclosure" in the event that that record contains "information concerning the security of an information system."[1] This exclusion is part of a list that excludes personal data, personnel data, and trade secrets from disclosure under public records laws. Similar exclusions are repeated elsewhere in Maryland's code.[2]

It is my impression that these rules were adopted in order to exclude from public disclosure such things as the passwords and cryptographic keys that protect the state's information systems. They are worded broadly in a natural attempt to exclude from public disclosure anything that might be of use to an attacker intent on violating the security of the state's computer systems.

The state of Maryland commissioned SAIC to study the security of the Diebold TS voting machines used by the state of Maryland in 2003. The version of this report released to the public was redacted.[3] The redaction was explained as being necessary to preserve the security of the voting system for use in the 2004 primary elections. Only in 2005 was the above legal basis for the redaction made clear, but at least in the short term, the legal basis was redundant. It is not prudent to begin the process of acquiring a new voting system less than a year before the first expected use, and therefore, in the short term, withholding critical details of a security assessment makes some sense.

An un-redacted version of this report was leaked in late 2006.[4] This was a working draft dated 9/17/2003, recording both additions to and redactions of an earlier draft. The flaws in the Diebold TS

[*] This material is based, in part, upon work supported by the National Science Foundation under Grant No. CNS-052431 (ACCURATE). Any opinions expressed here are those of the author and are not endorsed by the National Science Foundation or by the University of Iowa.

[1] *Code of Maryland,* 07.01.07.06(3). http://www.dsd.state.md.us/comar/07/07.01.07.06.htm

[2] *Code of Maryland*, 05.01.02.04(15), 14.28.02.04(15), 22.01.02.04(C).

[3] *Risk Assessment Report, Diebold AccuVote-TS Voting System and Processes*, SAIC, Sept. 2, 2003. http://bravenewballot.org/resources/SAIC.pdf

[4] Rebecca Abrahams, Leaked 2003 report on Maryland's Diebold voting systems reveals serious security concerns were withheld from election board, governor, public. *Brad Blog*, Nov. 2, 2006. http://www.bradblog.com/?p=3719

revealed in this draft are interesting, but these could have been corrected in a year, given a willingness to make major changes in the software architecture of the system. Withholding the document beyond this time serves primarily to prevent public examination of the competence with which the state has carried out its obligation to count votes in public elections. Maryland law, unfortunately, contains no sunset provision recognizing this compelling public interest. In effect, "information concerning the security of an information system" must be withheld from the public for all time.

An Example from California

There are many other examples of problems in this area. Consider, for example, a lawsuit filed on Dec. 30, 2004 by Americans for Safe Access (to Cannabis) against Alameda County, California. The vote on Referendum R in the November 2, 2004 election election had lost by 191 votes, and Americans for Safe Access had requested a recount. The county's response was to repeat the tabulation of the electronic election records, and Americans for Safe Access sued, arguing that such a retabulation was insufficient and asking the county to release sufficient information to allow an independent audit of the election.[5]

One thing Americans for Safe Access asked for was a copy of the event logs from the voting machines – referred to as audit logs by the system vendor. The county argued "that the public release of 'variable names' in audit logs from the November 2, 2004, election would assist persons who wish to hack any future election," and that denying access to such information was "the common business practice of the computer industry with respect to preserving system security."[6] In fact, the audit logs of the Diebold voting machines in question do not contain variable names, and they do not reveal any information that could be used by an attacker to hack an election.

On April 12, 2007, in a summary judgment, the Alameda County Superior Court rejected the county's arguments. Nonetheless, these argument were successful in delaying access to records of the election for over two years. One thing that came out in this case was that the county had failed to save the event logs from these voting machines, despite federal requirements that all records of the election be retained for 22 months. It may even have been the case that the county was unaware that such logs existed prior to the lawsuit. In effect, the security argument served primarily to delay public discovery of incompetent management.

A Colorado Story

In Conroy versus Dennis, argued in the District Court of Denver County, Colorado, a group of voters held that the state had not carried out its own laws with regard to certification of electronic voting systems.[7] The state permitted the plaintiff's experts to access voting system vendor documentation under the terms of a Modified Stipulated Protective Order, agreed to on August 11, 2006. This order required that all parties to the case hold vendor trade secrets in confidence, and it distinguishes such confidential information from security information, defined as any information related to the security of the electronic voting system.

Under this protective order, the State of Colorado classified a large number of documents as containing security information. Among these were independent testing lab reports that were publicly available on the Internet, tutorials giving general security advice, and several documents purporting to be security

[5] Americans for Safe Access v. County of Alameda, *E-Voting Archive*, Electronic Frontier Foundation, http://www.eff.org/Activism/E-voting/archive.php

[6] *Respondents/Defendants County of Alameda and Dave MacDonald's Combined Response to Plaintiffs' Second Set of Specially Prepared Interrogatories*, Jan 18, 2007.

[7] Lawsuit to Halt State's Purchase or Use of DRE Computerized Voting Systems, *Colorado Legal*, Voter Action. http://www.voteraction.org/States/Colorado/CO_legal.html

specifications. Unfortunately, on closer inspection, the latter appeared to be public-relations documents intended to reassure anyone who might be nervous about voting system security. Furthermore, manuals intended for distribution to polling-place workers were classified as vendor trade secrets.[8]

It is unrealistic to believe that manuals distributed to thousands of polling places will remain in confidence – to consider such information to be trade secret is simply nonsense. Restricting access to the manuals governing polling-place procedures prevents election observers from being able to assess whether the procedures are, in fact, being followed. This second argument applies equally to the procedures at the election headquarters for setting up the machines before an election and for extracting results from the machines afterward.

In fact, this final argument also applies to most of the materials submitted by a voting system vendor to the government at the time a voting system is being considered for use. If the public cannot examine the approval process, including assessing the evidence considered during the approval process, the public cannot assess whether that approval process was actually carried out competently. What the court found in Conway versus Dennis is that the state had not carried its own law for approving voting systems.

International Examples

These problems are not confined to the United States. In the Netherlands, a group named Wijvertrouwenstemcomputersniet (We Do Not Trust Voting Computers) released a report on the security of the most widely used Dutch voting machine several months before the November 22, 2006 Dutch Parliamentary elections.[9] The government response to this was largely appropriate.[10] One Dutch voting machine was actually decertified, forcing Amsterdam to revert to using paper ballots at the last minute.

Unfortunately, this government response also included a very dangerous ruling: "You should not make voting machines available to third parties, even for demonstration purposes. This also applies to voting machines that you no longer use. Allowing unauthorized third parties access to the hardware and software can jeopardise the reliability of the voting process. ... Please contact the information desk if third parties approach you seeking access to a voting machine." In effect, this is an attempt to prevent future efforts by citizens' groups such as Wijvertrouwenstemcomputersniet from undertaking any further investigations of the voting systems used in the Netherlands.

In the 2005 presidential election in Kazakhstan, a locally developed electronic voting system, known as the Sailau system, was used to count approximately one third of the votes cast. Prior to use, this system was tested by an independent testing authority against standards set by the state. In this regard, Kazakhstan's approach to electronic voting parallels the approach taken in most other countries, including the United States and Holland. Unfortunately, the standards against which the voting system was tested were a state secret![11]

Holding such standards to be a state secret can be justified: Honest elections are a matter of national security. We routinely declare just about anything relating to national security to be secret. Why not our voting system standards? In the United States, our system of voluntary voting system standards has

[8] Douglas W. Jones, *Expert Report / Conroy et al v. Dennis*, September 5, 2006. http://www.cs.uiowa.edu/~jones/voting/conroy_v_dennis_jones.pdf

[9] Rop Gonggrijp, Willem-Jan Hengeveld et al, *Nedap/Groenendaal ES3B voting computer -- a security analysis*. http://wijvertrouwenstemcomputersniet.nl/other/es3b-en.pdf

[10] Netherlands Minister for Government Reform and Kingdom Relations (BZK), *Circular of 22 September 2006* and (expanded) *Circular of 25 September 2006*. http://www.wijvertrouwenstemcomputersniet.nl/Politek

[11] *Republic of Kazakhstan Presidential Election, 4 December 2005 -- Election Observation Mission Final Report*, Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights, Feb. 21, 2006.

always been public, but for fifteen years. we have routinely held the reports detailing conformance with these standards to be matters of trade secret and therefore not public.

An Attempt to do Better

The state of New York drafted new administrative rules governing voting systems in early 2006. In drafting these rules, considerable effort was made to open up the process to public scrutiny. For example, rule 6209.6 A makes all test procedures and independent testing laboratory reports public documents.[12] Furthermore, rule 6209.6 F (9) (c) makes all non-proprietary information submitted by the vendor public. This was not the case in the first and second drafts of this document, where rule 6209.6 C made the procedures public but did not mention the results of testing.[13] These changes were the result of considerable discussion with the New York Board of Elections.[14]

Unfortunately, section 6209.6 D (3) (c) states that "the vendor shall identify all documents or portions of documents which the vendor asserts contain proprietary information not approved for public release. The State Board shall agree to ... refrain from disclosing proprietary information ..." There appears to be no oversight of the vendor's decision to make everything proprietary, and no distinct requirement that the vendor distinguish between proprietary trade secrets and security critical documents. Nonetheless, the New York model hints strongly at a direction that should prove productive.

A Model That Might Work

The central problem we face is that neither legislators nor high-level administrators appear able to figure out what information about a secure computer system can safely be disclosed to the public. I propose, therefore, that this determination must be made by the system developers. Each document created by the vendor of a secure system ought to clearly document its intended readership and the extent to which the document reveals any secrets that might compromise trade secrets, on the one hand, and the security of the system, on the other hand. Where part of a document is intended for a general readership but other parts contain trade secrets or security critical information such as default passwords or encryption keys, the document should be split so that one entire document can be released to the public while the other parts are held in confidence. It is important to include such labels both on documents written about the secure system and on documents created by that system.

In the case of voting systems and other systems where public oversight is essential, the rules must mandate public release of all information that a member of the public interested in observing the process might need to see in order to see that the process is being carried out properly. This clearly includes the election worker manuals, not only those governing the polling place, but those that apply to every point during the election cycle from acceptance testing to post election auditing and archiving. Similarly, all election results must be released, including secondary results such as event logs, along with sufficient information about the data formats to allow public interpretation.

Just as we require independent testing authorities to assess the design and construction of the voting system, we should require independent assessment of the labeling on the related documents. The natural tendency on the part of private vendors is to label everything as critical and disclose nothing.

[12] Voting System Standards, Title 9 Subtitle V part 6209, *Official Compilation of Codes, Rules and Regulations of the State of NewYork*. http://www.elections.state.ny.us/NYSBOE/hava/voting_systems_standards-4-20.pdf

[13] Second Draft Voting System Standards, Title 9 Subtitle V part 6209, Official Compilation of Codes, Rules and Regulations of the State of NewYork. http://www.elections.state.ny.us/NYSBOE/hava/2ndDraftVotingMachineRegs.pdf

[14] Douglas Jones, *Regarding the Voting System Standards Proposed by the New York State Board of Elections in December 2005*, Jan. 23, 2006. http://www.cs.uiowa.edu/~jones/voting/NYvssCritique.pdf
Regarding the Voting System Standards Proposed by the New York State Board of Elections in February 2006, Feb. 24, 2006. http://www.cs.uiowa.edu/~jones/voting/NYvssCritique1.pdf

Without oversight, this will go unchecked. Even with oversight, there is the possibility that the independent testing authorities might fail to correctly assess some document labels. It must be possible to challenge the process, so there should be no documents the existence of which are secret, and there should be mechanisms by which independent experts can be brought in, under limited nondisclosure agreements, to check the work of independent testing authorities in the event that deliberate or accidental mislabeling may have occurred.

Finally, the local election officials should be bound, by law and administrative rules to release everything that is labeled for public release and nothing else. It is very clear that state and county election offices, as they are run today, do not include sufficient expertise to reason about what should and should not be released, and this appears to be true of many other government agencies as well.