c/o 3548 Beechwood Boulevard
Pittsburgh, Pennsylvania 15217-2767
412-421-0178
voter@VoteAllegheny.org

California's State-Level Red-team analysis and it's implications for Pennsylvania.

Collin Lynch.

(collinl@cs.pitt.edu)

07/31/07

The California Department of State recently completed a survey of the security and accessibility of almost all of the voting systems used in the state. The study and its results were recently published and are available online.[1] This survey included expert accessibility studies which I will address elsewhere and a security assessment. Said assessment involved an independent red-team exercise in which team members took the role of outside attackers and developed attacks aimed at altering vote totals, denying use of the system to other voters and otherwise undermining the systems integrity. Neither the Federal ITA's nor the State-level carry out such tests. Instead they assume, incorrectly, that elections occur in a cooperative environment with no malevolent agents.

The study included the Diebold-TSX, Hart eSlate and Sequoia Edge. Together these systems are used in 21 Pennsylvania Counties. ES&S failed to submit its equipment for inspection. At present the California Department of State is considering sanctions. All of the systems examined have been certified in multiple states and passed numerous official certifications. All of the systems exhibited numerous security holes and were vulnerable to many low-tech exploits. Said exploits should work as well in Pennsylvania as they did in California.

I will discuss each of the three systems in turn beginning with Diebold. I will then analyze some of the implications of this study for the state of Pennsylvania, and conclude with a discussion of future directions.

1 California Secretary of State - Voting Systems Review - http://www.sos.ca.gov/elections/elections_vsr.htm

Diebold.

Diebold systems examined included the Diebold TSX using the same firmware version (4.6.4) as is certified for use in Pennsylvania. Diebold AccuOS Central Count optical scanner (again same firmware version 2.0.12 as in Pennsylvania). And the GEMS election management system (software version 1.18.24, Pennsylvania uses 1.18.25 which, according to examiner statements differs only in supporting the "Pennsylvania Method" straight-party voting).

The Diebold TSX system is used in Washington, Somerset, Armstrong, Clairon, Warren, Potter, Tioga, Lycoming, Bradford, Sullivan, Union, Northumberland, Schylkill, Carbon, Lehigh, and Pike Counties. At 16 counties it is the second most commonly used system in the commonwealth.

As part of their GEMS inspection they uncovered a number of problems including:

1. Deliberately constructed "back door" accounts that enabled the systems to be entered and results altered without a password.
2. Deliberately disabled or reduced security logging on the Windows systems.
3. Methods to alter or corrupt vote totals on the tabulation system.
4. Untraceable methods for altering vote totals within the GEMS system without producing a record in the security logs.
5. Preprogramming vulnerabilities that allow a machine to be rigged in advance so as to not record a vote.
6. Methods to seize remote control of the GEMS networking components and from them the GEMS tabulation system.
7. Methods to install malicious software without detection via a USB key.

As part of their TSX study the team discovered that:

1. It is possible to circumvent physical security of the systems using commonly available tools. This grants complete access to the machines.
2. Previously discussed security holes including those mentioned in the Princeton Study[2] are still present. These permit the undetected installation of software including viruses and the corruption of vote totals.
3. They discovered particularly that viruses installed on a TSX could spread to the central tabulation computer. Said infection could then spread "downstream" to other TSXs.
4. Successful attacks may be mounted by a comparatively low-skilled voter in the voting booth that will grant them total control over the machine. Said attacks may allow them to corrupt software, alter vote totals or any other malicious task.
5. Specifically crafted inputs to the voter accessible input-fields (e.g. write-in candidates) may be used to corrupt the machine and possible take further control.
6. "Low-tech" attacks that would corrupt or disable the VVPAT, in some cases without detection until the end of the day.
7. Alteration of vote totals on the close-of-day PCMCIA card was possible.
8. It is possible to obtain security information from the district-level PCMCIA card that would enable further attacks on other TSX machines or the Central Tabulation System.

The authors further identified attack scenarios which would allow electronic ballot box stuffing by any individual voter without the need for prior security information.

2 Feldmen, Halderman and Felten (2006) *"Security Analysis of the Diebold AccuVote-TS Voting Machine."* http://itpolicy.princeton.edu/voting/

Hart.

The red-team examined the Hart InterCivic voting system version 6.2.1, Judge's Booth Controller version 4.3.1, eScan version 1.3.14 and eSlate version 4.2.13. All are more recent versions of the system than those certified for use in Pennsylvania.

Hart InterCivic systems are used in four counties: Lancaster, Bedford, Blair and Fayette.

When examining the central tabulation software the team discovered:

1. An undisclosed "back-door" user name and password allowing access to the vote database.
2. Buffer overflow attacks allowing corrupted data to be inserted from a voting system.
3. Mechanisms to compromise the "protected environment in which the system runs.
4. Mechanisms to bypass all device certification allowing bad data to be written into the system.

When examining the Judge's booth controller the team was able to discover mechanisms to cast multiple ballots without special access, alter the vote totals with precinct-level access and violate the local network by introducing untrusted devices.

When examining the eSlate the red-team identified mechanisms to surreptitiously print multiple ballots, cast multiple ballots and record the audio track used for visually-impaired voters. This last attack would allow a surreptitious violation of voter privacy for those voters with visual problems.

Examination of the eScan identified mechanisms to overwrite the system software, access administration commands without a password and alter vote totals or configuration settings. These attacks were comparatively low tech and required no special tools or dedicated skills.

Sequoia.

The red team examined the Sequoia AVC Edge version 2 (Models I and II) with firmware version 5.0.24. This is the same version as is certified for use in Pennsylvania. They also examined WinEDS version 5.1.012 while Pennsylvania employs version 5.2.012.

The Edge is employed in York County. Montgomery County employs the Sequoia Advantage system which also incorporates WinEDS for election reporting.

In examining the Edge the authors found:

1. Previously known attacks allowing for electronic ballot-box stuffing were still possible.
2. Arbitrary code execution is possible allowing for the firmware to be corrupted or replaced.
3. Attacks that replace vote files on the Edge are possible.
4. Mechanisms to violate or void the system checks.
5. Methods to forge or rewrite result cartridges.
6. An absence of result-level security.
7. Easily by passable physical security seals.
8. Mechanisms to author direct attacks using off-the-shelf U3 based USB keys of the type used in Allegheny County's 2002 election by ES&S Staffers.

The authors also confirmed that previously known electonic ballot-box stuffing attacks were still possible.

Analysis.

In absence of any post-election auditing the security of our elections rests entirely on the advance inspections. The premise has always been that the Federal ITAs and the State Inspectors will filter out any systems exhibiting security holes. As this study and previous studies like it show this premise is false. Indeed far from ruling out all insecure systems the State has willingly certified and deployed systems that are not secure even during the time a voter spends in the booth.

Worse yet the authors of the California Studies noted that they had comparatively little time to test the systems. As they stated on page 6 of the overview:

> "The short time allocated to this study has several implications. The key one is that the results presented in this study should be seen as a 'lower bound'; all team members felt that they lacked sufficient time to conduct a thorough examination, and consequently may have missed other serious vulnerabilities. In particular, Abbott's team reported that it believed it was close to finding several other problems, but stopped in order to prepare and deliver the required reports on time. These unexplored avenues are presented in the reports, so that others may pursue them. Vigna's and Kemmerer's team also reported that they were confident further testing would reveal additional security issues."

When system problems were identified in previous years the promise was made that such problems will be found and patched quickly. The presence of known vulnerabilities in still-certified systems belies this and instead points to a lack of updates. Moreover said process still rests on the viability of the advance inspections. Said inspections have not, as is shown here, caught even the most glaring security holes, nor can they be expected to. No advance inspection, however well-funded or well staffed can be relied upon to identify all security holes. Even deliberately constructed holes such as the password-free backdoor account found in the Diebold GEMS system may still go by unnoticed.

This point was echoed by the authors of the SAIT study in Sarasota Florida.[3] Said study examined the iVotronic systems that were used in Sarasota County's recent elections. The study cost an estimated $300,000, involved hundreds of hours of code review alone, and took several months overall. Despite that the authors, one of whom is Dr. Michael Shamos, examiner for the Commonwealth of Pennsylvania commented:

> "There are fundamental limits on the ability of manual source code review to find defects in computer software. Manual code review is an imprecise process, guided by best practices and analyst intuition. It is impossible to check all code paths that might be executed in any nontrivial computer program. Also, in any nontrivial computer program, it is impossible to exhaustively enumerate and analyze the full state space that the code inhabits. Moreover, humans are fallible: just as the original software programmer can miss a defect in the code they write, so too can independent reviewers overlook subtle defects and bugs in the code." (pp. 19)

3 Yasinac, et al. (2007) *"Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware" http://election.dos.state.fl.us/pdf/FinalAudRepSAIT.pdf*

Previous studies of this type such as the aforementioned Princeton study have been dismissed by vendors and examiners on the grounds that attackers would not have full access to the system. As such the operational vulnerabilities of this type would be concealed. However as the authors of the California Study note this premise is dangerously false. Through dumpster diving, use of inside men and other mechanisms determined attackers and not-so-determined ones can always and do always obtain information on their target of choice. Good security practitioners often operate on the assumption that any would-be attacker possesses a complete copy of the target system. And that if any hole exists it will be found, and exploited. One should never base security decisions on the assumption of ignorant or unfunded attackers, especially given the amount of money on offer in any election cycle.

While there is often a tendency to "shoot the messenger" in these situations that urge is wrong. The authors of this and other similar studies are pointing out dangers with a goal of improving our security not impairing it. The ones to fear are the individuals who discover such holes and sell them to the highest bidder, or just alter elections for their own ends.

Conclusion.

This study like others before it illustrates not the vulnerabilities of a particular machine or software package but the vulnerabilities of our election system as a whole. Under our present inspections system crippling security vulnerabilities go unnoticed by the vendors, the Federal ITAs and the States. Said vulnerabilities, though discovered in California apply equally well in Pennsylvania. As such they may be exploited to alter not just a local election but State and Federal elections as well. Moreover we have no reason to believe that they went undiscovered in other competing equipment that was not covered by the California audit.

There is no single improvement or set of improvements to the inspections process that could rule out such vulnerabilities in the future. Even if existing equipment was redeveloped from the ground-up using high-assurance methodologies it would still not be proof-positive that they are safe. Elections are not conducted in cooperative environments and we cannot count on every player to play nice, or for every machine to be deployed cleanly.

Ultimately the only robust solution is the implementation of a reliable audit mechanism coupled with proper and open audit procedures. Said audits may be used to identify and correct, post-hoc, election issues that no amount of advance inspection can prevent. The best present mechanism for this is Voter-Verified Paper Ballots. While such a change may seem costly we must weigh it against the costs of election failure. How much money is in the Commonwealth's Budget? How much is in the federal? How many die in a war? At present our elections are fundamentally insecure and we cannot allow that.