Background on Recent DESI Vulnerabilities

Joseph Lorenzo Hall (UC Berkeley, School of Information; ACCURATE)

Summary

In the past year vulnerabilities have been reported in two Diebold Election Systems Inc. (DESI) voting systems, the AccuVote-OS optical scan system (AVOS) and the AccuVote-TSx (AVTSX) Direct Recording Electronic (DRE) voting system.

These vulnerabilities have serious implications for elections conducted on these systems and have magnified concerns with the federal certification process for voting systems. In both instances, the vulnerabilities can be attributed to software that is prohibited by the 2002 Voting System Standards (VSS). The machines containing this non-compliant software passed the security testing of the Independent Testing Authority (ITA) laboratories.[1] The vulnerabilities found in these DESI systems would permit an attacker, with only momentary physical access to the voting system, to change vote data, modify software and/or completely replace the firmware, operating system and voting application. DESI's inclusion of non-compliant software in voting systems, and the failure of the ITA to identify the departure from the VSS are further evidence that the federal certification and testing process are in need of retooling.

Background

Computer expert Harri Hursti examined the DESI AVOS and AVTSX voting systems with the consent of local election officials in Leon County, Florida and Emery County, Utah.[2] In both of these cases, Hursti found software features that are prohibited by Section 4.2.2 of the 2002 VSS. This section generally prohibits "self-modifying, dynamically loaded, or interpreted code" because of the opportunities it presents for the introduction of uncertified software. Such code is prohibited because it may be modified after ITA examination and could permit malicious modification or the introduction arbitrary errors.

In the examination of AVOS, Hursti found a proprietary software programming language called AccuBasic in residence on the voting system. AccuBasic is an interpreted language; it is translated, while the system is running, into executable code. The dynamic nature of AccuBasic – the fact that it is executed off of removable memory – and the lack of authentication of the software – technically ensuring that the software was legitimate – violate the provision of the VSS cited above. In response to the Hursti report, California Secretary of State sent the AccuBasic component back to the ITA, CIBER, for review after determining that the laboratory had not examined it.[3] The Secretary also commissioned a separate independent review by his Voting Systems Technology Assessment Advisory Board (VSTAAB).[4] Both reviews found significant, previously unknown, vulnerabilities associated with the AccuBasic interpreter as well

---

[1] CIBER, Inc. and Wyle Labs were the ITAs responsible for the AVOS and AVTSX vulnerabilities.

[2] Harri Hursti, "SECURITY ALERT: July 4, 2005, Critical Security Issues with Diebold Optical Scan Design", Black Box Voting, *available at:* http://www.blackboxvoting.org/BBVreport.pdf, and Harri Hursti, "SECURITY ALERT: May 11, 2006, Critical Security Issues with Diebold TSx", Black Box Voting, *available at:* http://www.blackboxvoting.org/BBVtsxstudy.pdf. (Black Box Voting has sponsored Hursti's work.)

[3] National Association of State Election Directors, Voting System Memory Card Issues, March 22, 2006, *available at:* http://www.nased.org/ITA%20Information/NASED%20Memory%20Card%20Report.pdf. CIBER, Diebold Election Systems, Inc. Source Code Review and Functional Testing, February 23, 2006, *available at:* http://ss.ca.gov/elections/voting_systems/diebold_code_review_final.pdf.

[4] David Wagner, David Jefferson, Matt Bishop, Chris Karlof and Naveen Sastry. Security Analysis of the Diebold AccuBasic Interpreter, VSTAAB, February 14, 2006, *available at:* http://ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf.

(cc) 2006, Joseph Lorenzo Hall, Some rights reserved. This work is licensed under a Creative Commons Attribution License: http://creativecommons.org/licenses/by/2.5/

as conditions that could only be caused by violations of Section 4.2.2 of the VSS. In the short term, the risks associated with these vulnerabilities can be significantly reduced through strict chain-of-custody requirements for the AVOS memory cartridges.

Hursti's examination of AVTSX identified a compound vulnerability. The AVTSX includes a "feature" that allows anyone to replace, simply and quickly, its existing software with arbitrary software. By inserting a memory cartridge[5] containing certain files into the machine and "rebooting"[6] the AVTSX, an individual could replace the firmware, operating system and voting application code with software that had not been approved through the federal process and without the knowledge or approval of the relevant election official. Section 4.2.2 of the 2002 VSS, cited above, requires software that uses programming features such as "pointer variables" and "dynamic memory allocation"[7] to include controls to protect against deliberate or accidental modifications. The AVTSX was found to lack such controls in violation of the VSS.

The AVTSX vulnerabilities – which are also present in its predecessor the AccuVote-TS – can be exploited with minimal physical access to a single machine. At least part of this vulnerability – the possible unauthorized replacement of voting application software – was identified by researchers in 2004 and published in the RABA report.[8] It is unclear why this vulnerability remained present in DESI machines after the publication of this 2004 report. The presence of this design flaw means that DESI voting systems have been vulnerable to substantial compromise for several years. Why DESI did not fix this problem, and in fact reproduced it in a subsequent model, after it was identified in 2004 remains unclear.

It is troubling that a voting system containing a violation of the 2002 VSS survived the federal certification and testing process. The federal testing process is the primary evaluation process required for voting systems in 80% of states. Given the importance of the federal process to ensuring the integrity of voting systems it is unacceptable that a flaw of this magnitude was not identified.

There appear to be two plausible explanations for the failure of the ITA to catch this violation of the VSS; neither is comforting, and both underscore concerns with the federal certification process raised by ACCURATE in comments to the Election Administration Commission on the proposed 2005 Voluntary Voting System Guidelines (VVSG).[9] First, it is possible that DESI disingenuously represented, or the ITA erroneously concluded, that the code was commercial off-the-shelf (COTS) software and therefore exempt from review.[10] ACCURATE critiqued this section of the VVSG as highly problematic because it allows certain software to bypass review.

Second, it is possible that the ITA reviewed the software in question and failed to catch the violation. If this is the case, it may highlight another flaw of the VSS singled out for criticism in ACCURATE's EAC comments. ACCURATE criticized the existing VSS and forthcoming VVSG for its use of functional instead of performance-based testing and the failure to adopt appropriate testing methodologies. Functional testing is limited; it can only check for features and/or vulnerabilities that can be predicted beforehand. The AVTSX failure proves that there are critical vulnerabilities, which violate the standards, that fall between items in functional

---

[5] The AVTSX holds vote software, data and other information on a removable memory cartridge.
[6] "Rebooting" refers to cycling the system's power off and then on again.
[7] "Pointer variables" and "dynamic memory allocation" are both methods in computer programming that allow software to manipulate data flexibly.
[8] "The PCMCIA card can be used to update the software on the AccuVote-TS terminal." RABA Innovative Solution Cell, Trusted Agent Report: Diebold AccuVote-TS Voting System, Jan. 20, 2004, at 19, *available at:* http://corporate.raba.com/news/TA_Report_AccuVote.pdf.
[9] ACCURATE, Public Comment on the 2005 Voluntary Voting System Guidelines, September 30, 2005, *available at:* http://www.law.berkeley.edu/clinics/samuelson/projects_papers/2005_vvsg_comment.pdf.
[10] See: VSS, Vol. II, §5.2 (Unmodified, general purpose COTS non-voting software is not subject to examination.).

(cc) 2006, Joseph Lorenzo Hall, Some rights reserved. This work is licensed under a Creative Commons Attribution License: http://creativecommons.org/licenses/by/2.5/

checklists. A testing lab, engaged in appropriate testing and staffed with computer security experts, should not have missed the violation found in the AVTSX.

The fact that we do not know why the federal certification system failed to identify and rectify these flaws is due to the lack of transparency around the federal certification process. Given that the ITAs do not provide information about their test plans and testing methods it is impossible to assess the origin of these security flaws without additional information from the ITA and the vendor. ACCURATE recommended that ITAs be required to release detailed information to the public about test plans, testing methods and test results of voting systems reviewed pursuant to federal standards.

It is critically important that state's using either of the DESI machines, the AccuVote-OS optical scan system (AVOS) and the AccuVote-TSx (AVTSX) Direct Recording Electronic (DRE) voting system, take steps to limit the risks posed by the recently identified vulnerabilities. The Election Administration Commission should be providing states with assistance in identifying and implementing mitigation strategies. The failure of the current federal testing and certification process to ensure that only machines compliant with existing federal guidelines are certified is a cause of deep concern. The ACCURATE project in its comments on the VVSG recommended several changes to the federal process that we believe would substantially improve the security—as well as other requirements—of voting systems. The Hursti reports are further evidence that the system is in need of reform. We recommend that action be taken to implement ACCURATE's recommendations.

(cc) 2006, Joseph Lorenzo Hall, Some rights reserved. This work is licensed under a
Creative Commons Attribution License: http://creativecommons.org/licenses/by/2.5/