California Diebold Report Confirms that Maryland's Voting System is Not Compliant with Federal Standards

Independent Security Analysis discovers dangerous vulnerabilities & recommends not using Diebold voting systems for statewide elections

A summary review of the "Security Analysis of the Diebold AccuBasic Interpreter", issued by the California Voting Systems Technology Advisory Board on February 14, 2006. The full 38-page report can be found at: http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf Also see www.SaveOurVotes.org .

The findings of this report have confirmed that Maryland's Diebold voting systems, both AV-TS touchscreens and AV-OS optical scanners, are not in compliance with federal standards because of the existence of banned interpreted code. The report also confirmed that the Diebold AV-OS system is vulnerable to the famous "Harri Hursti hack" that was demonstrated in a mock election in Leon County, Florida in December 2005. Further, the analysis discovered numerous additional bugs in the interpreter that "lead to another, more dangerous family of vulnerabilities." (page 2)

While the report listed short-term mitigation strategies that could be employed for use in local elections, they recommended not using the Diebold systems in statewide elections unless the vulnerabilities were fixed by re-writing the architecture of the system, because, "Larger elections, such as a statewide election, provide a greater incentive to hack the election and heighten the stakes." (page 36) Additionally, the mitigation strategies are only viable because of the existence of a voter-verified paper audit trail and mandatory audit requirement for all voting systems in California. The report emphasized that, "Successful attacks can only be detected by examining the paper ballots." (page 2)

The California Security Analysis supports the position by TrueVoteMD, in a January 25, 2006, letter to SBE Administrator Linda Lamone,

http://truevotemd.org/images/stories/leon-lamone%20on%20lttrhead.pdf that Maryland’s present voting system should be decertified and new testing be conducted because Maryland law requires compliance with federal voting system standards. While the California study applies specifically to the AV-TSx touchscreens and the AV-OS optical scanners and not the AV-TS machines used by Maryland, the findings are still relevant because the AccuBasic software language and the interpreter in question exist on all Diebold systems, including Maryland’s AV-TS touchscreens, as Diebold admitted in a memo to Pennsylvania authorities on January 5, 2006.

http://truevotemd.org/images/stories//diebold_pa_response.pdf

The report is very clear about the prohibition of interpreted code in the federal standards. On page 3, it states:

“*Interpreted code is contrary to standards:* Interpreted code in general is prohibited by the 2002 FEC Voluntary Voting System Standards and also by the successor standard, the EAC’s Voluntary Voting System Guidelines due to take effect in two years**. In order for the Diebold software architecture to be in compliance, it would appear that either the AccuBasic language and interpreter have to be removed, or the standards will have to be changed.”** (emphasis added)

Listed below are sections of the California study that demonstrate the seriousness of the security vulnerabilities of the Diebold system and that are relevant to the present controversy in Maryland. Some additional commentary is included.

page 2

“*Memory card attacks are a real threat:* We determined that anyone who has access to a memory card of the AV-OS and can tamper it (i.e. modify its contents), and can have the modified cards used in a voting machine during election, can indeed modify the election results from that machine in a number of ways. **The fact that the results are incorrect cannot be detected except by a recount of the original paper ballots**.” (emphasis added)

“*Harri Hursti’s attack does work:* Mr. Hursti’s attack on the AV-OS is definitely real. He was indeed able to change the election results by doing nothing more than modifying the contents of a memory card. He needed no passwords, no cryptographic keys, and no access to any other part of the voting system, including the GEMS election management server."

" *Interpreter bugs lead to another, more dangerous family of vulnerabilities:*"
(This longer paragraph describes other bugs that they discovered that go well beyond what Hursti demonstrated, including changing vote totals, modifying reports, changing names of candidates or races being voted on or inserting code into the running firmware of the machine.)

" *Successful attacks can only be detected by examining the paper ballots:"*

page 3

" *Interpreted code is contrary to standards:* Interpreted code in general is prohibited by the 2002 FEC Voluntary Voting System Standards and also by the successor standard, the EAC's Voluntary Voting System Guidelines due to take effect in two years**. In order for the Diebold software architecture to be in compliance, it would appear that either the AccuBasic language and interpreter have to be removed, or the standards will have to be changed."** (emphasis added)

page 6

(3rd paragraph) "It is widely acknowledged that a malicious person with unsupervised access to GEMS, even without knowing passwords, can compromise GEMS and the election it controls. This report does not address those threats, however."

page 11

(under Finding 1) *"There are serious vulnerabilities in the AV-OS and AV-TSx interpreter that go beyond what was previously known. If a malicious individual gets unsupervised access to a memory card, he or she could potentially exploit these vulnerabilities to modify the electronic tallies at will, change the running code on these systems, and compromise the integrity of the election arbitrarily."*

(further down this section)

"These vulnerabilities would not affect the normal behavior of the machine, and would not be discovered during testing."

Page 12

(5th paragraph) "It is hard to be confident that one has found all bugs….."

(6th paragraph) "None of the vulnerabilities we found would have been found through standard testing, so testing is not the answer."

page 13

The **Impact** section describes how an attack could:
- completely compromise an election,
- gain full control over all operations of the machine,
- manipulate the tallies in any way desired including waiting until it reviewed the end of day results before deciding whether or not to alter them,
- print fraudulent reports to prevent detection,
- tamper with the ballot images (touchscreens),
- erase all traces of the attack
- possibly even make the attack persist from one election to another

page 16

(5th paragraph, this could conceivably explain the numerous documented reports of certain candidates not appearing on the electronic ballot in Maryland's 2002, and 2004 elections.)

"On the AV-TSx, it could show the voter a wrong or incomplete list of candidates during vote selection; it could change the selections between the time when they are initially selected and when they are shown on the summary screen; and it could selectively target a subset of voters, based on how they have voted or on other factors."

page 16 – 17

"These bugs could be used to selectively trigger a crash only on some machines, in some geographic areas, or based on certain conditions, such as which candidate has received more votes. For instance, it would be possible to write a malicious AccuBasic script so that, when the operator prints a summary report at the end of the day, the script examines the vote counters and either crashes or continues operating normally according to which candidate is in the lead."

page 17

"It is important to note that even in the worst case, the paper ballots cast using an AV-OS remain trustworthy: in no case can any of these vulnerabilities be used to tamper with the paper ballots themselves."

(This is why TrueVoteMD recommends optical scan systems instead of touchscreens with a printer added on.)

"Attack code might be able to introduce fraudulent VVPAT records, compromising the integrity of both the electronic tallies and the paper records."

(further down the page)

“In this scenario, both the electronic tallies and the paper records are untrustworthy, so in the worst case the only recourse may be to hold another election.”

page 20

(The preceding section dealt with the issue of the cryptographic key protection for the memory cards that exists on the AV-TSx system. It points out how this protection is only valid if the crypto-key is reset from the default. But here, it also points out :)

“Of course, anyone who knows the cryptographic key can change the contents of the card and re-compute the MAC appropriately. This means that anyone with access to the GEMS server will have all the information needed to make undetected changes to AV-TSx memory cards.”

(and)

“In other words, if the operator of the GEMS server is malicious, or if any entrusted individual gains access to the GEMS server, all of the machines in the county [in MD that would be state] could be compromised. The AV-TSx cryptography provides no defense against this threat; instead it must be prevented by carefully guarding access to the GEMS server.”

page 20-21

(This section, Finding 4, discusses how the default keys are hard-coded in the source code, are the same across the country and that this vulnerability was published in the JHU/Rubin report of July, 2003 and revealed by Doug Jones to date from 1997 when he reported it to the vendor. Despite this, they remain in the source code today.)

“It had been our understanding that all of the vulnerabilities found in those investigations two years ago had been addressed. It is hard to imagine any justification for continuing to use this key after it had been compromised and revealed to the public. This is a serious lapse that we find hard to understand considering how widely publicized this vulnerability was.”

page 30 and on

(The **Mitigating the Risks** section starts here. TrueVoteMD maintains that a full testing of our AccuVote TS machines is mandatory, though, because the security features on our older TS model are known to be not as robust as the TSx model. In the strict defensive programming sense, even the TSx is described in this report as not being robust.)

Mitigation 1

(Basically, no one should be alone with the memory cards at any point. It is interesting here how the report talks about how memory cards are ballot boxes and should be treated with the same chain of custody requirements as paper ballot boxes. So, while the BOE often argues that paper is “almost impossible” to secure, this report shows that it is even more difficult to secure the electronic records.)

Mitigation 2

(Revise the source code to fix the vulnerabilities. And, they suggest “an independent source code review to make sure all vulnerabilities have been eliminated.”)

“Even if the interpreter source code is fixed, it would still be possible for an individual who can introduce a malicious AccuBasic script to cause fraudulent zero tapes and fraudulent summary reports to be printed. Depending on whether the arithmetic overflows are fixed, such an individual might also be able to pre-load a memory card with a positive or negative number of votes for some candidates.”

Mitigation 4

(Discusses how the architecture should be changed so that they do not store code on removable memory cards. The report discusses how this code is a part of the voting system “code” and therefore must be subject to testing and review by federal and state examiners. This point reinforces the position of TrueVoteMD that the present system must be tested and examined and is presently in non-compliance with the standards.)

Mitigation 5

“The FEC 2002 Voluntary Voting System Standards expressly forbid interpreted code in section 4.2.2.”

“To be in compliance it would seem that AccuBasic would have to be eliminated, or the standard would have to be changed.”

“It seems untenable to us that every time there is a change to the AccuBasic language or interpreter another round of detailed code review such as we have done would be required; however, an interpreter is such a delicate and powerful feature (from a security point of view) that we cannot recommend shortcuts in its examination either.”