

## **Introduction**

Pennsylvania's Department of Elections issued an amended certification report for the Diebold TSx system on January 17, 2006 that certifies the TSx for use in Pennsylvania. That report was issued subsequent to a report denying certification to Diebold's precinct-based optical scan (OS) systems, based in large part on security vulnerabilities identified by computer security expert Harri Hursti. Questions were raised whether such vulnerabilities may also exist in the Diebold TSx (touchscreen DRE) system.

The report asserts that additional security precautions that Diebold has applied to the interpreted code that is stored on the removable memory cards used by the TSx (e.g., use of digital signatures) provide adequate protection against unauthorized access to and modification of that code or to other data stored on those cards. However, it provides no details regarding the technologies used to implement those precautions. Without a discussion of the specifics of the digital signatures, no one can determine the validity of their argument that the interpreter is "inaccessible".

Furthermore, the certification report describes the specific configuration of the TSx that Pennsylvania used to conduct its certification tests. According to the most recently-posted (12/22/2005) list of voting systems that have completed the federal certification process and received a NASED System ID number, the specific TSx configuration that Pennsylvania used for its certification tests does not appear to have completed federal certification at the time the State conducted its tests nor by the date on which Pennsylvania's certification report was issued;<sup>i</sup> neither are we aware of any notice that such federal certification has been completed at this time. Accordingly, Pennsylvania's decision to certify this configuration of the TSx system may have been premature and thus might subject to legal challenge.

## **The Questions**

Pennsylvania's recently-issued (January 17, 2006) amended certification report for the Diebold TSx implicitly attempts to address several related questions:

1. Does Diebold's AccuBasic interpreted code (which is present on the memory cards of both their TS and TSx DREs and on the precinct count version of their optical scanners) violate the FEC 2002 Voting Systems Standard's (VSS) prohibition on the use of interpreted code?
2. Is the same security vulnerability that has been documented in Diebold's precinct count optical scanner (i.e., the "Hursti Hack") also present in the TSx?
3. Are there procedural requirements that PA can impose (as a condition for state-level certification) that at least partially address either of these first two questions?

Because the report does not explicitly pose these specific questions, for the most part it fails to give explicit answers to them. However, some answers are implied "between the lines."

## **The Short Answers**

#1. No, provided one accepts Pennsylvania's interpretation of a rather vague and ambiguous exemption clause (Section 6.4.1(e)) of the FEC 2002 VSS. [However, if one accepts that interpretation, then it must apply equally to the TSx and OS systems.]

#2. No, provided one accepts the assertions made by:

- a) Diebold, in their letter responding to PA's queries [contained as Appendix A of the certification report]
- b) Michael Shamos, who was apparently permitted to review and analyze the relevant Diebold source code

#3. Yes.

The report implies that the risk of undetected modification of the contents of the removable memory cards employed by the OS and TSx systems can be reduced through procedural means, including "careful handling and storage procedures and the effective use of seals"; such procedures are one of the conditions that Pennsylvania has imposed for certification of the TSx . However, the report implies that such procedures, by themselves, provide insufficient protection against unauthorized access to or modification of the contents of such memory cards. If such procedures did provide sufficient protection, then Pennsylvania would not have had a valid basis for denying certification to Diebold's precinct count optical scan (OS) system.

The report also appears to argue that bogus .abo files (interpreted code that has been tampered with) would not be as harmful on the TSx as on the OS because what the TSx stores on the removable memory card are ballot images rather than counters. The point may be that without counters, it may be impossible to store -N ballots for one candidate and +N ballots for another so that the number of ballots at the end of the election balances out (as Hursti had demonstrated).

It is unknown whether the "digital signatures" on the TSx memory cards prevent modified code from being executed. No details about the digital signatures are given, so it is possible no one other than the vendor knows if they conform to cryptographic best practices or not. Furthermore, the report seems to concede that someone with root privileges on the GEMS server could modify a script and get a legitimate digital signature using GEMS.

### **The Long Answers**

Both the Diebold TSx and precinct-count optical scan systems contain interpreted code on the removable memory card used in these machines. Diebold openly admits this; no debate.

Where there is debate:

- Does the FEC 2002 VSS contain an absolute prohibition on the use of such interpreted code, or does it contain an exemption (a.k.a. loophole) that permits the use of such interpreted code if "certain conditions" are met?

In this report, Pennsylvania appears to make the case that Section 6.4.1(e) of the FEC 2002 VSS does indeed provide such an exemption if:

- a. this rather vague and ambiguous clause is correctly interpreted by Pennsylvania, and
- b. Pennsylvania imposes additional security procedures (i.e., requiring "the use of effective seals" so as to prevent "the substitution of memory cards after pre-election testing), as a condition for state-level certification, in order to ensure that the "certain conditions" required to qualify for the §6.4.1(e) exemption (under their interpretation of that clause) are indeed met.

Unfortunately, the wording of this clause (§6.4.1(e)) is quite terse and imprecise, leaving it open to various interpretations. This clause reads:

*After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible.*

The term "accessible" is imprecise in this context. It does not indicate to what or to whom or by what means the listed items (source code, compilers, or assemblers) shall not be "accessible". In addition, this clause is imprecise with regard to the period of time over which the listed items shall not be accessible.

While it specifies a starting time ("After initiation of election day testing"), it specifies no corresponding ending time. Since the machine will be used in multiple elections held on different dates, there must clearly be an implied ending time in order for the explicitly-specified starting time to have any meaning.

Thus, one might infer that a more precise reading of this clause would be:

*"After initiation of election day testing, no source code or compilers or assemblers shall be resident or accessible [until after the polls have been closed, the final summary tape has been printed, and the memory card (on which the vote totals and/or electronic ballot images are stored) has been removed.]"*

The State of Pennsylvania is attempting to interpret this clause (§6.4.1(e)) in a manner that enables them to exempt Diebold's AccuBasic interpreted code from the prohibition defined in §4.2.2. In paragraph 3 on page 6 of their report, they argue:

*"6.4.1(e) is applicable. It states that after Election Day testing, no source code be resident or accessible. The 'source code' in this case is the input to the interpreter, namely, the .abo file. The code becomes 'accessible' if some person has the ability to replace the TSx memory card after it has been installed in the TSx and subjected to pre-election testing."*

Some of these points are debatable. Does "source code" really mean the interpreted code (i.e., the .abo files), as indicated here? Does "accessible" mean "modifiable without detection", as this seems to imply? It is also debatable whether the contents of the TSx memory cards (i.e., the interpreted code .abo files and/or the electronic ballot images) are truly not modifiable without detection.

Thus, Pennsylvania appears to interpret §6.4.1(e) of the VSS as meaning:

*"After initiation of election day testing, no source code or compilers or assemblers shall be resident [in the voting machine] or accessible [to 'some person']."*

Thus, they are assuming two distinctly different implied objects (i.e., a voting machine and some random person) as being respectively referenced by the words "resident" and "accessible". It is unclear whether that represents a valid interpretation of this clause.

In trying to infer the actual intent of the authors of the FEC 2002 VSS, one should look at the

context within which this clause (§6.4.1(e)) appears:

Section 6: Security  
Section 6.4: Software Security  
Section 6.4.1: Software and Firmware Installation  
Section 6.4.2: Protection Against Malicious Software

Note that §6.4.1(e) is placed within the section on "Software and Firmware Installation", and not in the section on "Protection Against Malicious Software"

If one assumes, for the sake of argument, that Pennsylvania's reading of §6.4.1(e) is the correct reading, then one can argue that Diebold's AccuBasic interpreted code does qualify for the exemption provided by §6.4.1(e) if (and only if) the State can guarantee that the memory card containing that interpreted code is not accessible [*to a person*] until after the polls have closed and the final summary tape has been printed.

Pennsylvania apparently plans to provide that guarantee in two ways: first, by requiring "careful handling and storage procedures and the effective use of seals" to ensure that the counties using the "TSx shall not permit the substitution of memory cards after pre-election testing" (on page 8, their report makes that requirement their #1 condition of three that must be met in order for the TSx to be certified for use in that state), and second, through the use of digital signatures to assure the integrity of contents of those TSx memory cards.

However, that analysis ignores whether other types of hacks are feasible on the memory card of the TSx. In some ways, it is more vulnerable than the memory card on the OS (optical scan) system, because the memory card of the TSx can be plugged directly into and modified by any commonly-available laptop computer, as opposed to the memory card of the optical scan system which can only be read and modified by using a rather obscure crop scanning device. A laptop computer presumably has far greater computing capability (than a crop scanning device) for regenerating digital signatures as are used on the TSx memory cards.

The argument that the interpreted code (the .abo files) contained on the memory cards is 'inaccessible' to a hacker hinges on the effectiveness of the digital signatures that (supposedly) prevent illegitimately modified .abo files from being executed by the AccuBasic interpreter contained within the AccuVote-TSx. Cryptographic schemes are notorious for subtle errors that cause them to be easily broken. They must be implemented and evaluated by experts, using the best available technology. Given Diebold's past history of incompetent use of cryptography (as documented in the Johns Hopkins/Rice report at <http://avirubin.com/vote.pdf>), it is odd that no specific details about the digital signature are presented in the Pennsylvania report. Indeed, there is no indication in the report that the author of this report did any evaluation of the scheme other than listening to Diebold's assertion that the .abo files are digitally signed.

Since Pennsylvania appears to be arguing that procedural means (i.e., "careful handling and storage procedures and the use of effective seals"), by themselves, provide insufficient protection and hence cannot guarantee the integrity of the interpreted code or data stored on the removable memory cards (else they would not have denied certification to Diebold's OS system), they must clearly demonstrate that the safeguards that Diebold has allegedly provided for the TSx (i.e., digital signatures, removal of counters from the memory cards) are sufficient to "ensure that the software tested and approved during the qualification process remains unchanged and retains its integrity", as required by §4.2.2 of the FEC 2002 VSS.

Unfortunately, based on the extremely limited technical information provided in Pennsylvania's certification report for the TSx , we cannot assess whether the security features that Diebold describes for the TSx are sufficient to meet the requirements elaborated by §§4.2.2 and 6.4.1(e) of the FEC 2002 VSS.

## CONCLUSIONS

1. Pennsylvania's decision to certify the TSx appears to hinge on their interpretation **of §§4.2.2 and 6.4.1(e)** of the FEC 2002 VSS. Given the ill-defined wording of those sections, that interpretation should be reviewed by an attorney well-versed in election law, government regulations, and the interpretation of such standards documents.
2. If Shamos' analysis is accurate, then the use of interpreted code on the memory card of the TSx represents a different level of risk than the use of such code on the memory card of Diebold's precinct count optical scanners, because the former does NOT appear to be directly vulnerable to the exact same "Hursti Hack" to which the latter is clearly vulnerable. However, the memory card of the TSx, unlike the op-scan memory card, can be plugged into and modified by any laptop computer and therefore is **subject to a different class of risks**.
3. Pennsylvania's conditions for certifying the TSx (i.e., requiring "careful handling and storage procedures and the use of effective seals...") can only (potentially) address concerns of tampering with interpreted code on memory cards **if their** election procedures also require that **each TSx voting machine be subjected to "Election Day testing"** conducted after the memory cards have been inserted into all machines and "sealed". If "Election Day" testing is performed only on some machines, then malware could be installed on the memory cards of some of the TSx machines prior to when the seals are applied, and go undetected if that machine did not undergo subsequent "Election Day" testing.
4. Even if **all** TSx machines are subjected to "Election Day" testing after the memory cards are installed and seals applied, such "Election Day" testing (conducted with the machine operating in "test mode") may not be sufficient to detect the presence of any malware (with appropriate digital signatures) installed onto the TSx memory card prior to its insertion into the machine.
5. To the extent that completion of federal certification is a prerequisite to the State's certification testing and the granting of State certification, Pennsylvania's decision to certify the TSx on January 17, 2006 may be premature and thus possibly subject to legal challenge, since it appears that the specific TSX configuration that Pennsylvania tested has not completed federal certification. Specifically, the following components of that configuration (which is specified on page 8 of the certification report) are not yet certified at the federal level: GEMS election management system software 1.18.25 and Election Media Processor 4.6.2. Furthermore, the remaining items listed in that configuration do not appear as being certified under a single NASED System ID number, and thus do not correspond to a consistent configuration that has received federal certification.
6. The federal certification of all TSx configurations has been called into question by the California Secretary of State's office because Diebold failed to submit for ITA review either the AccuBasic source code used to generate the .abo files on the removable memory card or the source code for the AccuBasic interpreter itself. As a result, **NO** configuration of the TSx

has been certified for use in California because of Diebold's failure to submit that code to ITA review, and certification of the TSx in California will not occur (if at all) until the relevant ITA laboratories have received and completed their review of the source code for Diebold's AccuBasic interpreter and the AccuBasic code (\*.abo files) that are contained on the removable memory card and executed by that interpreter. This raises addition concerns about Pennsylvania's decision to certify the TSx while the ITA's review of that software is not yet completed.

The concerns raised in this analysis may or may not provide sufficient grounds for challenging Pennsylvania's certification of the TSx.

Ironically, the Diebold letter suggests looking at the printed copies of the ballot images to make sure the report from the machine hasn't been hacked. But voters have never seen those printed copies of ballot images, and had no opportunity to confirm that their votes were accurately recorded.

The most reliable safeguard is a voter-verified paper record, used in mandatory random manual audits. Since the TSx as certified lacks a voter-verified paper record, no reliable audit can be conducted. While the memory card vulnerability of the OS is significant, legitimate audits can be carried out with that system using the paper ballots marked and verified by the voters.

Bob Kibrick  
Legislative Analyst, Verified Voting Foundation

David Dill, Founder  
Verified Voting Foundation

---

<sup>i</sup> According to a 2004 staff report of the California Secretary of State's Office, Diebold misrepresented the status of the TSx system in federal testing in order to obtain state certification, and despite promises, failed to obtain federal qualification through NASED on the system as submitted. For these and other reasons, California decertified the TSx system. Cf. [http://www.ss.ca.gov/elections/ks\\_dre\\_papers/diebold\\_report\\_april20\\_final.pdf](http://www.ss.ca.gov/elections/ks_dre_papers/diebold_report_april20_final.pdf)