FLORIDA DEPARTMENT of STATE

CHARLIE CRIST
Governor

KURT S. BROWNING
Secretary of State

July 31, 2007

Mr. David Byrd
Diebold Election Systems
PO Box 1019
Allen, Texas 750133

Dear Mr. Byrd:

As Chief Elections Officer, it is my responsibility to insure fair, accurate, secure, and uniform elections in Florida. On May 15, 2007, the Department of State contracted with Security and Assurance in Information Technology (SAIT) Laboratory at Florida State University to review documented, published issues with the Diebold Accuvote OS and the TSx, currently in the voting systems certification process in Florida.

SAIT Lab released its findings in a report to the Department of State on Friday, July 27, 2007. Based on the report, the Bureau of Voting Systems Certification has determined that certain vulnerabilities outlined must be corrected by August 17, 2007, to continue this certification. Failure to do so will result in a denial of certification. Please see the attached document for the required corrections.

It is my understanding that Diebold is currently making corrections to the optical scan firmware that will address issues contained in the SAIT Lab report. When an amended firmware version for the Accuvote OS has been submitted, we will move forward to resume the testing and certification process. As it pertains to the touchscreen, we will not certify the system with this application. However, we will work with you to resolve the issues with the TSx prior to your next application in October. This certification schedule will provide time for Diebold counties to upgrade the firmware for currently certified optical scan and touchscreen machines prior to the Presidential Preference Primary.

Although there are numerous issues listed in the report, many are administration in nature or pose no security risk. Upon certification, the Division of Elections will be issuing a technical advisory to the Supervisors of Elections who use the Diebold voting system. The advisory will outline suggested additional election and security procedures to mitigate the administrative issues outlined in the report. We will forward a copy of that advisory to your office for your information.

Please do not hesitate to contact the Director of the Division of Elections, Amy K. Tuck, if you have further questions or concerns regarding this correspondence or the SAIT Lab report. The Division will be contacting your office regarding the implementation of the modifications to these issues.

Sincerely,

Kurt S. Browning
Florida Secretary of State

Attachment

Attachment A

The following numbering system corresponds to the final report as provided by Security and Assurance in Information Technology Laboratory.

Required changes:

3.5 The Signature Flaw

The vendor's RSA signature verification is insecure (RSA is an algorithm for public-key cryptography). Signature comparisons generated with this method can be forged. The comparison employs what is called a SHA1 hash. The SHA1 hash entails 160 bits, which means that when the signatures are verified, only the 160 bits are verified and the remaining 1888 bits are not examined. Leaving these bits outstanding and not verified allows for a vulnerability for forgery attacks. This must be fixed in the certification to employ a standardized, widely accepted mode for public key verification. This will also be addressed in administrative procedures at the local level.

3.8.1.4 Attacker Can Hide Preloaded Votes

The system must mitigate the original published attack regarding preloaded votes with the changes in the RSA signature correction (see 3.5). However, because the memory card is not encrypted or authenticated it is still possible to load votes on a memory card. Election officials need to continue to restrict access to removable media and secure audit logging techniques should be employed.

3.9.1 AccuBasic Scripts Can Be Misused

The system allows AccuBasic code to perform conditional operations based on comparisons of data for such things as time, candidate names and other data. This might allow an attacker to hide exploits by manipulating this conditional data. The issue lies with the signature verification, which must be corrected in the certification (see. 3.5).

3.9.5 Unchecked String Operation: Allows Overwrite of Stack Memory

The unchecked string operations still exist in the code, other corrections in the software have already mitigated this vulnerability. This issue must be addressed and changed in the certification.

Administrative Procedures:

3.6 Optical Scan Memory Card Is Not Integrity Protected (see 3.8.1.4)

The data on optical scan memory cards is not encrypted or authenticated (except for the insecure signature on the AccuBasic script). This vulnerability can lead to potential attacks. Administrative procedures must be employed at the local level to limit access and possible exploitation.

3.8.1.1 Leaks Memory Card Contents

An attacker can copy the memory card contents to a laptop by connecting the laptop to the optical scanner. The attacker would turn the machine on, enter diagnostic mode by simultaneously hitting the "yes" and "no" buttons and selecting a menu option to dump the memory card's contents. The current method to copy memory card contents is to allow one to use the "yes" and "no" buttons. Elections officials must monitor access to the optical scan machine through local security procedures.

3.8.1.2 Supervisor PIN Not Cryptographically Protected

Diebold uses a method for shuffling the supervisor's PIN using the memory card's key. Thus, someone with access to the memory card and reader and knowledge of the shuffling algorithm can determine the PIN. Election officials must maintain security procedures over the voting terminals and the removable media.

3.8.1.5 Vote Counters Are Not Directly Checked for Overflow

Candidate ballot counters are protected from overflow by a total ballot counter. These individual candidate vote counters can hold as many votes as the total ballot counter, so there should be no overrunning of all vote counters. Consistency checks have been implemented so that possible exploitation of this flaw is prevented. Election officials must also strictly monitor access to both the optical scan machines and the memory cards.

3.10.1 AccuBasic Scripts Are Not Authenticated on the GEMS (Global Election Management System) Server

GEMS itself does no checks to the AccuBasic byte code because the system relies on the RSA signatures to verify the code. The corrections made to section 3.5 (above) will correct the signature verification issue. In addition, the elections officials must restrict access to the GEMS server.

3.10.2 Password Does Not Protect Access to GEMS or Audit Logs

The GEMS password authentication process can be defeated in what is a publicly known attack. In order to mitigate against this attack, election officials must protect access to

GEMS servers and must never connect GEMS servers to the Internet or an untrusted network.

No Security Threat:

3.8.1.3 No Authentication Between GEMS and the Terminal

The written code provides for mutual authentication between the GEMS (election management) server and the optical scan terminal. However, the concern on this validation is if devices were to connect via the Internet. In Florida, there is no interaction with the Internet.

3.9.1 Error Checking is Inadequate

The system does not provide descriptive display prompts as to encountered errors. The prompts merely notes that it "does" or "does not" work. The issue raised is that without these prompts, an attack might not be noticed. However, it has been determined that the error messages are capable of being printed out for use by trained, technical staff. The actual display only notices that it "does" or "does not" work to prompt poll workers, who would then contact elections officials staff.

3.9.2 Error Codes Returned by the AV-OS System are Ignored

The system returns a status code indicating the success or failure of script interpretation. The function that provides this return value is present in the code, but does not require further action. All errors are reported within the Abasic processing which is inside the system and can be accessed and reviewed.

3.9.4 Public Key Hard-Coded into the Source

Embedding the public key in the source code does not pose a direct security problem. However, having the public key hard-coded into the source code prevents the vendor from routinely changing the public/private key pair. This is a trade-off because the key cannot be changed by the election official, but also cannot be changed by anyone else.