Diebold Election Systems

Tom Watson – Examiner

January 19, 2006

Diebold Election Systems

The Diebold system was re-examined in Austin on January 19, 2006. The current releases of the sub-systems are as follows:

AccuVote -TSX - version 4.6.4– DRE voting machine with AccuView Printer Module
AccuVote -TS R6 - version 4.6.4 – DRE voting machine
AccuVote-OS Model D - version 1.96.4 – Precinct optical scanner
GEMS - version 1.18.24 – Election preparation, central-count tally and reporting system
VCProgrammer – version 4.6.1 – Software used to select correct ballot style for voter
Voter Card Encoder - Version 1.3.2 - Hardware used to select correct ballot style for voter
Key Card Tool – version 4.6.1 - Software used to generate security keys
ExpressPoll 2000/4000 – version 1.1.5 – Electronic poll book application

The system (excluding the ExpressPoll) is an upgrade to the certified Diebold system. The vendor stated that there are no significant functional differences from the system's previous version. The differences are primarily to the software coding in order to bring it up to the Federal 2002 standard. The upgrade to the Accuvote -TSX also incorporates the AccuView Printer Module for a voter verified "receipt". There are also cosmetic changes to the screen displays of the Accuvote -DRE's.

Findings

- Operating System access : the following is a direct quote from my previous report since the status has not changed:

  Diebold has not fixed the method used to keep an operator out of the operating system when a central count is being tabulated. A "key" in the Windows registry is used to prevent "escaping to the OS" which would allow unlogged access to the database. The key could easily be removed prior to the election tabulation by anyone with Windows administrator privileges. As stated in my previous report on the system, it would be better to check for the key upon entering the election-night tabulation mode. If the key is not present, it should be restored automatically. The Diebold representative said that they would agree to sell systems in Texas without administrator rights, the rights required to modify the Windows registry. This will be hard to verify so if this solution is allowed, I recommend it be so as a short-term solution only. This is an easy fix.

- Database encryption: the GEMS database is not encrypted. The vendor stated they were looking into databases which can provide encryption. I recommended the following in my previous report: *Diebold programs that need to read, insert or modify the database can be enhanced to decrypt or encrypt "on the fly". This is an additional measure to prevent access to the election setup or results data outside the controlled (and logged) access of the Diebold programs.*

The goal is a database which is encrypted and readable and write-able only through the controlled and logged access of GEMS. The encrypted data would be of little use to someone intent on tampering if they gained access from a program other than GEMS. This means that the encryption needs to be tied to the GEMS program – not just an encrypted database whose key (known by election personnel) could be used by another program to manipulate the data.

- The Key Card tool and AccuVote firmware have been enhanced so that the Administrator (used by election personnel) and Supervisor (used by a precinct judge) privileges have been split. This prevents a supervisor from deleting an election on the AccuVote machines. The key used to secure the election can and should be changed by the jurisdiction for each election. If the jurisdiction has not changed the default key, a message will display on the DRE's to indicate that the default key has not been changed.

- The AccuView Printer Module (AVPM) was demonstrated and worked well for the very small number of ballots cast on the TSX DRE for the examination. Since a voter "receipt" is not required, extensive scrutiny was not applied. However, the following was noted:

    - the printout was easy to read by the voter.
    - take-up reel has a mechanism that prevents the printed tape from being pulled out of the canister which keeps a poll worker from being able to see what any voter has voted.
    - a barcode can be printed in addition to the human readable print – this will facilitate a manual re-count.
    - if a ballot is "spoiled" because the voter doesn't agree with the printout, a clear message is printed below the ballot to indicate it as such.
    - the election can be configured so that the AVPM will not print a voter receipt.

- The ExpressPoll is an electronic poll book which runs on proprietary hardware and the Microsoft Windows CE operation system. If the jurisdiction has loaded the voter registration database into ExpressPoll, it can be used in a voting location to verify a voter's identity and automatically program the Voter Access Card with the correct ballot style. ExpressPoll has several other functions and benefits but they are not germane to the voting process.

  ExpressPoll should significantly shorten the voting queues in a precinct. It should also reduce errors in selecting the ballot style for the Voter Access Card. The vendor stated that a minimum of two ExpressPolls should be used in a voting location.

- Modem transfer was not available for the examination due to configuration problems with the equipment. It has subsequently been demonstrated and it work correctly.

- As per the previous finding, the vendor needs to bring a complete system and be prepared to demonstrate every function that may be used.

Conclusion

The Diebold system recorded and tabulated ballots correctly. It also handled the provisional ballots properly. I recommend certification for all sub-systems. I recommend that the AVPM not be used on the TSX DRE since a voter receipt is not required.

The operating system access and database encryption issues mentioned above are serious. Despite repeated suggestions Diebold has not sufficiently addressed these security weaknesses in GEMS. If not corrected in the next release, I recommend that GEMS certification be rescinded.

Tom Watson
Examiner