Review of Recent Information Security Issues Involving Maryland's Voting Technology

For

The State of Maryland's Office of the Attorney General

By
M. Glenn Newkirk, President

InfoSENTRY Services, Inc.
Two Hannover Square, Suite 2330
Raleigh, NC 27601
USA

29 March 2006

InfoSENTRY Services, Inc.
www.infosentry.com
Phone: 919.838.8570

Table of Contents

Introduction

The closeness of the 2000 Presidential Election and the problems with many states' inadequate elections infrastructure remain as the ghosts of elections past. Passage of the Help America Vote Act (HAVA) in 2002 aimed to address many of those infrastructure inadequacies. However, instead of simply providing a new set of rules and tools, HAVA brought with it many new problems and concerns.

High atop the list of concerns was the adequacy and security of the new hardware, software, networks, and operations involved in voting systems. Sensational revelations appeared soon after HAVA's passage concerning the new technologies, in particular with computerized Direct Recording Electronic (DRE) computerized voting systems. Forgetting the security problems that had been inherent and endemic in older voting systems and often failing to follow industry-standard approaches to security and continuity assessments, many election critics focused their attention solely on weaknesses of DREs. As is natural in a market economy, competitors with other technologies almost certainly contributed to the "fear, uncertainty, and doubt" about DREs. DRE vendors naturally focused on their products' advantages over the competitors' offerings.

Most states had a patchwork of older voting technologies (such as punchcard systems, lever voting machines, older optical scan machines, and manual ballot reading operations) and some newer DRE systems. Maryland moved aggressively to replace its patchwork with a more uniform, current voting system. This system was a DRE, "touchscreen" system and an election management system, GEMS, sold by Diebold Election Systems, Inc. (referred to simply as "Diebold" throughout this report).

Maryland, like Georgia before it, implemented the statewide system in a short timeframe. The State used the system in its elections in 2004, most notably in the landmark, heavy-volume 2004 Presidential Election. The very rapid implementation project involved not only the acquisition and deployment of the hardware and software in polling places throughout the state, but it involved training and support for thousands of pollworkers and a statewide voter awareness and education campaign. The result was an election with fewer problems than one might normally expect in a state the size of Maryland and with as many pollworkers as Maryland had to train on the new system in a very short time period.

A report issued by the CalTech/MIT Voting Technology Project (Stewart III, Charles, Residual Vote in the 2004 Election: Working Paper #25. February 2005) noted the results of election reform efforts in Maryland and other states. While listing a number of well thought-out caveats about attributing too much importance to a single causal factor for improvements, the report noted that several states had achieved an increase in overall voting accuracy:

> "The Caltech/MIT Voting Technology Project has championed the use of the "residual vote rate" as a measure of voting machine accuracy ever since it began examining voting machine performance in the wake of the 2000 presidential election. The residual vote rate in a county is the percentage of all ballots cast that did not record a vote for president. In a mechanical sense, a vote can fail to be counted either because there was no vote for president on an individual's ballot (an "undervote") or multiple marks (an "overvote")."

The report went on to note:

> "Confining ourselves to the thirty-five states for which we can calculate residual vote rates in both 2000 and 2004, seven had residual vote rates above 2% in 2000, compared to only two in 2004. Of these thirty-five states, five had residual vote rates below 1% in 2000, compared to fifteen in 2004. Florida and Georgia saw the biggest decreases in the residual vote rate, by 2.5% and 3.1%, respectively. They were also among the states that engaged in the most significant election reform efforts across the past four years." (Emphasis added.)

We added the emphasis to note that Maryland was another state that made significant changes in its election administration by a widespread installation of a new DRE voting system and an accompanying increase in uniformity of procedures in the Maryland's polling places.

The CalTech/MIT report noted in its multivariate analysis, both controlling for and including other factors rather than simply whether a state had switched to a new or a particular type of voting equipment, the following comment:

> "Here we discover that there may be particular gains to be had when a jurisdiction that already uses optical scanners chooses to use the newest generation of DREs."

While this report neither started nor ended as an endorsement for any one kind of voting technology, the report's main data table indicated that Maryland's residual vote rate (that is, the percentage of all ballots cast that did not record a vote for President) in 2004 dropped to 0.3% from a 2000 residual vote rate of 0.5%. This drop gave Maryland the lowest residual vote rate of any state after it instituted its uniform DRE voting system and the common, consistent set of operations and processes that accompanied the change to the new technology. [1]

Nonetheless, critics continue to express security concerns, typically aimed at DREs and particularly aimed at those manufactured by Diebold. Various groups in Maryland State Government contracted with Science Applications International Corporation (SAIC) and RABA Technologies to study the security of the Diebold voting system. (SAIC. Risk Assessment Report, Diebold AccuVote-TS System and Processes. September 2, 2003 and RABA Technologies. Trusted Agent Report, Diebold AccuVote-TS Voting System. Columbia, MD: January 20, 2004.) The SBE implemented the vast majority of the reports' recommendations, even some which proved to be impractical when used in elections.

In the same timeframe, the State of Ohio released security reviews of several vendors' voting systems, including Diebold's AccuVote-TS system. (Compuware Corporation, Technical Security Assessment Report. Columbus, OH: November 2003 and InfoSENTRY Services, Inc. Computerized Voting Systems Security Assessment.

[1] The report's data table also lists Nevada as having a 0.3% residual vote rate in 2004. That state also converted to all DREs for the 2004 Presidential Election. Many voters in Nevada voted on the newly implemented Sequoia DREs equipped with a contemporaneous paper ballot printing capability. The remaining voters, most often in Clark County, voted on an older, open-face version of Sequoia's DREs. The primary source of paper ballots in the 2004 Presidential Election in Nevada came from mail-in absentee voters.

Columbus, OH: November 2003.) These reports contained dozens of recommendations for security enhancements to the Diebold voting system and Diebold's organizational security processes. Both of the third-party firms subsequently reviewed Diebold's actions to correct security problems found in the reports. They subsequently released reports indicating that Diebold had remedied the vast majority of the security issues. (Compuware Corporation, Diebold Direct Recording Electronic (DRE) Technical Security Re-Assessment Report. Columbus, OH: August 18, 2004 and Compuware Corporation, Diebold Direct Recording Electronic (DRE) Technical Security Re-Assessment Report. Columbus, OH: January 26, 2005.)

A recent event triggered a fresh round of concerns about the security of Diebold voting systems. The issue arose during a review of the firm's optical scan voting systems in Leon County, Florida. According to published reports, election administrators in that county allowed a group substantial access to the Diebold voting technology with a charge to determine if any security weaknesses existed. (Sancho, Ion, Special Report: Black Box Voting Attempts to Penetrate The Leon County Florida Optical Scan Voting System. Tallahassee, FL: undated.). The results, now commonly known as the "Hursti Hack," pointed to potential vulnerabilities for a malicious person, who might have similar access to the system, to make undetected modifications in vote tabulation results.

In reality, the "hack" was neither a hack nor was it a detailed security assessment. It was the technical equivalent of providing someone who stated an intent to rob you with your house keys, your credit card numbers, your checkbook, your Social Security number, your mother's maiden name, your pet's name, and a floor diagram to your house in the morning and being surprised when you came home in the evening to find that you had been robbed. A main participant in the Leon County security penetration effort and other election critics apparently have acknowledged that the attack would not be possible if the election administration employed security precautions typically recommended by vendors and election professionals.

Nonetheless, the effort provided information on a specific vulnerability of the Diebold system under a specific set of circumstances. It also triggered subsequent reviews of the Diebold system. The most publicly watched reviews occurred in California.

California's Certification Efforts

Diebold voting systems have traveled a rocky path in California. California's previous Secretary of State leveled charges of various problems and security breaches against Diebold. Among the issues involved were those of deploying incorrect or uncertified system versions in various counties.

Two parallel courses of action occurred. A new California Secretary of State moved forward with a strong examination and certification process that involves multiple and detailed levels of examination prior to a system's certification. The second course of action was at Diebold. Partially as a result of the findings in the Leon County, FL, incident, Diebold re-submitted its software to the ITA for additional examination and submitted the software in question to CIBER for a separate security assessment.

With the development of a new, detailed examination and certification process, the events in Leon County came to the attention of California's Secretary of State.[2] The Secretary required Diebold to resubmit particular portions of its voting system through the Federal ITA process for additional review. At the same time, the Secretary submitted the Diebold system in question to California's own election system examination groups.

The result of California's efforts and the review by the Federal ITA was issuance of a conditional certification to Diebold. The following excerpt from a letter from a senior elections staff member in the California Secretary of State's office, states the fundamental case for certification. (McDonald, Bruce. Letter to Mr. Dave Byrd. Sacramento, CA: February 17, 2006.)

> "It is of particular significance to this office that the state's expert reviewers have clearly stated that the vulnerabilities that they believe to exist are easily managed by use and security procedures, many of which are already established practice and in use in California."

The extended quote below from Secretary of State McPherson's news release details California's statement of certification to Diebold along with the conditions imposed for maintaining the certification. (McPherson, Bruce. News Release: Secretary of State Bruce McPherson Grants Certification with Conditions for Voting System--McPherson requires additional use procedures and security measures." Sacramento, CA: February 17, 2006.)

> "Secretary of State Bruce McPherson today announced his decision to certify with conditions the Diebold TSX and Optical Scan (OS) voting systems for use in California's 2006 elections. The decision comes after months of thorough review of both voting systems, their compliance with both state and federal laws and the completion of an additional security analysis by independent testers from computer labs at the University of California, Berkeley.
>
> Among the requirements, systems must: undergo a first-in-the-nation requirement for a "volume test" to ensure the systems will withstand election day levels of activity, deposit a copy of the system source code and the binary executables with the Office of the Secretary of State, and establish a California County User Group to review the system and ensure voter usability…
>
> After the completion of the federal and state certification requirements, as well as a complete and thorough review of the voting system components, Secretary McPherson requested that Diebold undergo an additional security analysis of the source code on the system's memory card. Computer scientists at the University of California, Berkeley laboratory conducted the additional security review of the memory card components for both systems. The independent reviewers concluded that while some of the code on the memory cards should be rewritten for an improved long-term solution, the problems identified are "manageable" and "the risks can be mitigated through appropriate use procedures."

[2] The events in Leon County, Florida also came to the attention of the Maryland State Board of Elections. The State Board's Administrator reportedly contacted Diebold immediately with an expression of concern and a demand for an assessment of the Leon County study's relevance to Maryland's voting system and a demand for remedial actions if necessary.

Of course, not all groups and factions agreed with the Secretary's conclusions and with the certification decision. Some pointed to the conditional nature of the certification as an indication that neither Diebold's touchscreen nor its computerized optical scan voting systems operated securely.

However, the issuance of a conditional certification is neither rare nor an indication that a particular system is not secure and safe for use. In Pennsylvania, where we serve as one of two examiners for voting system certification, it is common to issue a certification with conditions for all types of voting systems. Virtually all systems have functional and security anomalies when examined closely. Voting system certifications frequently take those anomalies and conditional requirements to correct them into account when preparing certification recommendations. As was the case in California's certification of Diebold, these conditions typically aim to provide additional assurance that the vendor's product or service continuously improves in order to remain in compliance with state or Federal standards. (Cortés, Pedro, Examination of the Diebold Election Systems' AccuVote TSX Electronic Voting System, OS Optical Scan Units and GEMS Election Management Software. Harrisburg, PA: December 22, 2005, and Cortés, Pedro, Amended Certification of the Diebold Election Systems' AccuVote TSX Direct Recording Electronic Voting System and Certification of the AccuVote OS Optical Scan Central Count Reader CC 2.0.12. Harrisburg, PA: January 17, 2006.)

We note that Maryland has developed an integrated set of security policies and procedures that can be built upon for the specific technology now in place throughout the State. (Maryland State Board of Elections. AccuVote Voting System Voting System Security Processes. Annapolis, MD: October 27, 2005.) Maryland has already subjected the Diebold TS voting system and the GEMS election management software to a "volume test," like the one mentioned in the California Secretary of State's certification, during actual use in the 2004 Presidential Election with no material volume-related anomalies or security incidents.

Other Test Reports and Federal Standards

In addition to citations from previous reports, Diebold contracted with CIBER to perform a detailed security assessment of the interpreter that was subject of a great deal a discussion. The following quotes are from CIBER's final report. (CIBER. Diebold Election Systems, Inc. Source Code Review and Functional Testing. Huntsville, AL: February 23, 2006.)

> "The TSX interpreter inspected appears to be ready for an election…"
>
> "The interpreter had three security vulnerabilities and a small number of requirement violations that were not capable of being exploited by malicious code or operators. Of the three serious problems, they can be fixed with minor code changes."
>
> No issues were discovered with the compiler that impacts the security of the system. There were no findings in the inspection of the AccuBasic Scripts that would materially impact the security of the system."

The comment is important because the TSX interpreter referenced in the CIBER report is the same as the interpreter involved in Maryland's voting systems. Language from the

following email addresses this issue. (Henry, Thomas J. Email to Mr. Mark J. Davis. Washington, D.C.: March 9, 2006.)

> "You have asked whether the AccuVote-TS and the AccuVote-TSX are the same with respect to their (1) memory cards, (2) AccuBasic interpreter, and (3) defenses against the so-called "Hursti hack." I have conferred with my client, who has confirmed that, if the version of the BallotStation is the same, the code is the same whether running on an AccuVote-TS or an AccuVote-TSX. Thus, the memory card contents, AccuBasic interpreter, and defenses would be the same on both."

This most recent report and the affirmation from Diebold about the applicability of the results to Maryland's voting system provided yet the latest indication of the readiness of the voting system to support secure voting in Maryland. Diebold's affirmation is easily subject to documentation and testing.

The Federal certification authorities also recognized the importance of the operational issues in the Leon County, FL, incident, which involved optical scan voting technology. The National Association of State Election Directors (NASED) developed and released an amendment to its qualification standards for all voting systems that include a memory card that stores or transfers election data. (Steinbach, Sandra. Voting System Memory Card Issues. National Association of State Election Directors: March 2006.)

> "To prevent corruption of memory cards NASED hereby adopts an official addendum to the qualification of all voting systems that include a memory card that functions to store and transfer ballot images or tabulation data:
>
> 1. Throughout the life of the voting system, the election official shall maintain control of all memory cards and keep a perpetual chain of custody record for all of the memory cards used with the system. Programmed memory cards shall be stored securely at all times with logged accesses and transfers.
>
> 2. Immediately after the memory card is installed in the voting station, the card shall be sealed against unauthorized access. The voting station shall not be set into election mode until after the memory card is sealed inside.
>
> 3. Use controlled serialized seals that are tamper resistant and resistant to inadvertent breakage along with verifiable seal logs.
>
> 4. In post-election mode, print the results report prior to removing the memory card from the optical scanner. If additional reports other than the results report are available, print these as well."

We note that the Maryland State Board of Elections' (SBE) published and implemented security processes for the State's touchscreen voting systems already include these operational steps as a result of its previous security assessment and reviews.

These reviews, tests, and certifications point to the current technical sufficiency of the voting systems used in Maryland to conduct an election safely and securely, providing adherence to the SBE's published security plans, policies, and procedures. They provide a technical foundation for the simple factual observation that the Maryland SBE and Local Boards of Elections (LBEs) have used the system successfully and securely through a Presidential Election in 2004. They also point to the need for Maryland's SBE and LBEs to have industry-standard policies and procedures to maintain a "defense-in-depth" security capability for its election systems.

Maryland's Voting Security Plan

In addition to all the technical steps taken as a result of the studies, Maryland has also implemented various physical and operational security steps to provide layers of security and defense in depth.

As noted in a previous section, the Maryland SBE has prepared a security process manual that covers the life cycle of use for its voting system. (Maryland State Board of Elections. AccuVote Voting System Voting System Security Processes. Annapolis, MD: October 27, 2005.) The SBE used certified information systems security professionals and its senior elections staff to prepare this detailed plan. It covers the physical, technical, and operational mitigations suggested by (1) previous security assessments, (2) recommendations made subsequently in California, and (3) operational requirements stated subsequently in the NASED qualification requirements referred to in a previous section.

Subsequent to the development of this security process document, the Maryland State Board of Elections commissioned an academic organization to examine alternative technologies for vote verification. (National Center for the Study of Elections, University of Maryland, Baltimore County, A Study of Vote Verification Technologies Part I: Technical Study. Baltimore, MD: February 2006.) In addition to recommending against purchasing any of the technologies in the study, the report concluded the following:

> "Regardless of what the state does in the near term with regard to vote verification and vote verification systems, in future elections, it should expand the use of parallel testing. The state should also undertake a full-scale assessment of the security procedures and practices around its current voting system. We say this even with the knowledge that the SBE's security procedures are reasonable and prudent and that the SBE's system of parallel testing reduces considerably the possibility of widespread fraud and attack on the system." (Emphasis added.)

We concur with these recommendations, particularly for a periodic, full-scale security assessment to review and improve the SBE's existing voting System security processes.

RECOMMENDATION: The Maryland State Board of Elections should have periodic independent security audits of the State election system's security policies and procedures to assess (1) the need for changes and updates of those policies and procedures in light of statutory changes to election laws, changes to its election technology, and new threats, and (2) the degree to which the State and Local Boards of Elections comply with the documented security policies and procedures.

Conducting periodic audits of any information system security plan is an increasingly accepted and expected practice for information systems. The National Institute of Standards and Technology (NIST), which HAVA mandates to play a significant role in election security, states the expectation clearly (Swanson, M. and Guttman, B.,

Generally Accepted Principles and Practices for Securing Information Technology Systems. Washington, D.C.: September, 1996.

> "System users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare and procedures become outdated over time. These issues make it necessary to reassess periodically the security of IT systems."

Alternatives under Consideration

We understand that the State is considering replacement of its current computerized touchscreen voting system with another computerized voting technology. The consideration is to replace its existing Diebold DRE voting system and software with the computerized AutoMARK ballot printing system and the ES&S M-100 computerized optical scanner. Using this system, the general public will mark selections on paper ballots and insert them into the M-100 for computerized scanning and tabulation. The AutoMARK VAT (Voter Assist Terminal) provides a technology to meet the physical accessibility requirements of HAVA.

The AutoMARK, which was certified by the Federal certification authorities in 2005, uses the Windows CE operating system. It receives election and ballot instructions resident on a memory device programmed through the AutoMARK Information Manager (AIM). The AIM module is now an integral part of ES&S's Unity election management software. Voters using the AutoMARK can rely on its physically assistive devices, such as a special keypad, audio translation device for ballot choices, or a "sip-and-puff" interface.

Upon completion of ballot choices on the AutoMARK, the voter issues a command for the device to print a paper ballot for insertion into the M-100 computerized optical scanner. The M-100 "reads" and accepts data input from the paper ballots in the same manner as it "reads" paper ballots prepared by other voters by means of pen or pencil marks. The AutoMARK computer system relies on software in at least three critical areas:

1) the Unity/AIM software to setup the election and define the ballot structures,
2) the election "program" that resides on the memory card inserted in the AutoMARK VAT, and
3) the operating system and firmware in the AutoMARK VAT.

While the AutoMARK does not permanently store the results of the voter's ballot selections for subsequent tabulation, it does temporarily hold the results of the voter's ballot selections for instructing the print mechanism about the positions on the paper ballot at which it should make identifiable marks.

There is no assertion in this report that the AutoMARK is not secure. The issue is that the computerized voting device and its attendant software do not appear to have been subjected to the same level independent, third-party, publicly available security assessments, source code review, and functional examination as has the Diebold system now in place in Maryland. From a systems security perspective, the proposed change presents a double standard. The State is proposing to convert from a computer system that various Federal and third-party security assessments have studied, found fit for its purpose, and made reasonable recommendations for continuous improvement to

another computer system about which the State has received few, if any, third-party security assessments, independent security source code reviews, or audits.

Another issue for Maryland's careful consideration and review is how the process by which the M-100 handles "mismarked" ballots fits into Maryland's election laws and operational procedures. In an acceptance test of the M-100 in Wake County, North Carolina, our firm documented that "mismarked" ballots, such as those on which voters circle candidates names or place "X" marks by candidates names instead of correctly filling in the "bubble" on the ballot, go into the regular ballot bin (that is, the left-side ballot bin) along with all properly marked ballots, even though they might be tabulated by the M-100 as a blank ballot or an undervoted ballot. They do not go in the right-side ballot bin, which holds exceptional ballots, such as those with write-in selections.

The result of this M-100 ballot operation, if it is programmed to handle mismarked ballots in this manner for Maryland, will be that in any "hand to eye" recount of the paper ballots, the results will almost certainly vary from the machine totals. If there is no manual recount, the mismarked ballots might not be counted properly in the election. (InfoSENTRY Services, Inc. Acceptance Test Results of the M-100 Computerized Optical Scan Voting System Units in Wake County. Raleigh, NC. March 20, 2006.)

Election officials who do recounts from the M-100 must have the thermal paper tape results tapes available to reconcile the number of "blank ballots" and "undervotes" on the results tapes against the individual number of mismarks that exist on the ballots. They must review every ballot to determine if it contains a clear indication of voter intent that the computerized optical scanner missed because of its programming. This potential increases the likelihood (1) that the intent of voters who mismark ballots will go undetected unless Maryland decides to tabulate all ballots manually or (2) that the likelihood for requests for manual recounts in relatively close elections will increase. The first outcome results in "lost votes." The second outcome results in substantially higher election administration costs and slower resolution of elections.

While this situation is not in and of itself a security issue, it is one that has the potential to affect the accuracy of election results, the confidence of voters that the system actually tabulates their ballots in the manner they intended, and the number of manual recounts requested in Maryland. An alternative will be for Maryland to require the vendor to re-program the system to handle mismarked ballots in a different manner. Under any circumstance, Maryland will need to develop detailed procedures, user documentation, and a training program in a very short period of time if it replaces its current DRE technology with this optical scan technology for the 2006 elections. Various jurisdictions across the country are learning about the risk of project failure posed by such a radical change in such a short period of time.
