

You Can't Trust Maryland's Paperless Voting Machines

**Submitted by the Campaign for
Verifiable Voting in Maryland
www.TrueVoteMD.org**

Three formal reviews have produced three failing grades for Maryland voting:

Johns Hopkins University: "If we do not change the process of designing our voting systems, we will have no confidence that our election results will reflect the will of the electorate."
July 23, 2003

SAIC: "The [voting] system as implemented in policy, procedure, and technology is at high risk of compromise." September 2, 2003

Maryland Legislative Services: "In each instance the team found vulnerabilities [in all components of Diebold voting systems] that could be exploited by malicious individuals."
January 2004

February 4, 2004

**To: The House Ways and Means Committee
The Senate Education, Health and Environmental Affairs Committee**

**Re: Comments and Analysis of the Department of Legislative Affairs
Report, "A Review of Issues Relating to the Diebold Accuvote-TS Voting
System in Maryland"**

**From: The Campaign for Verifiable Voting in Maryland, www.TrueVoteMD.org
Contact: Kevin Zeese, 301-270-6150 or kevinzeese@freshaircleanpolitics.org**

Date: February 4, 2004

The paperless electronic voting system of Maryland has been reviewed formally three times. Each time the reports produced alarming findings of potential manipulation of the election or unintentional inaccurate voting. This report focuses on the most recent report by the Maryland Legislative Services Division highlighting areas of agreement, areas of disagreement and misstatements made at the briefing before your committee.

The Campaign for Verifiable Voting, made up of citizens of all parties throughout the state of Maryland, is urging support for HB 53 which requires a voter verified paper ballot for the purpose of independent audits and recounts of electronic vote counts.

We are pleased with many of the findings of the Department of Legislative Affairs Report, but we are concerned with several misstatements made in the briefing to your committee as well as a major area of potential manipulation of elections that was not reviewed by the Department's report. The Department did an excellent job analyzing the potential for outsider attacks on the voting in Maryland but the Legislative Services Report failed to examine the potential of an insider attack or software problems.

**I. The Maryland Legislative Services Report failed to Examine the
Potential for An Insider Error or Insider Attack on Voting**

Although outside attackers receive the most publicity in the mass media, the consensus among computer security experts is that inside attackers are both a more likely threat to the system and more likely to succeed in their attacks. The Johns Hopkins Information Security Institute found this to be a "considerable" threat. The types of insiders were described by Johns Hopkins as election officials (from poll workers to the County and State Boards of Elections), developers of the software systems and the developers of the embedded operating systems that run the machines. Each of these insiders could affect the outcome of an election, and none of them were considered as possible threats to the system by the MLS Report.

It would be far easier for someone to fix an election by modifying the software at Diebold's installation or elsewhere before it is delivered to election offices to install on all the machines. It is easy to imagine that one person could tamper with the software that is installed on all the machines. Obviously, it is a serious oversight to consider difficult small-scale threats by outsiders while ignoring easy large-scale threats by insiders.

The Johns Hopkins study found that there was no evidence of “control process that restricts the developer’s ability to insert arbitrary patches into the code.” Therefore “a malicious developer could easily make changes in the code that would create vulnerabilities to be later exploited on Election Day.”

Johns Hopkins concludes:

“If any party introduces flaws into the voting system software or takes advantage of pre-existing flaws, then the results of the election cannot be assured to accurately reflect the votes legally cast by the voters.”

In discussing this critical gap in the Legislative Division report with computer software security experts they agreed on the following items:

1. Large software projects, such as the Diebold machines have code that is so complex, that no manual inspection process, nor automated analysis can uncover carefully crafted malicious code.
2. No conceivable review process, not just the current ITA process, can stop sophisticated insider attacks on computer systems. Indeed, the Maryland SAIC report included such a disclaimer saying: “SAIC cannot guarantee or assure that risks, vulnerabilities and threats other than those addressed in this report will not occur nor can we guarantee or assure that, even if the State of Maryland implements the recommendations we have proposed, the State's business, facilities, computer networks and systems, software, computer hardware and other tangible equipment and assets will not be compromised, damaged or destroyed.” When SAIC testified before your committee they stated that they were 99.999% certain that malicious software could be hidden in the software code and not discovered by anyone.
3. It is impossible to achieve an adequate level of assurance using paperless electronic voting using current technology for three reasons: First, we don't know how to eliminate software bugs. Second, we don't know how to make computer systems secure from attacks. And third, there is no way to make sure the software you want to be running on a system actually IS the software that is running (as opposed to some other software that acts the same except when malicious code is triggered).

Maryland Legislative Services assumed that the Independent Testing Authority (ITA) is responsible for checking security. In fact, the ITA is only minimally required by FEC regulations to be concerned with security because the regulations they are enforcing have little to say about security. Indeed, after the Johns Hopkins/Rice Report, the ITA was defended by people saying that the criticism of them was unfair because they weren't supposed to be checking security.

Regarding ITA’s activities, we don't know the answers to basic questions about what they do. Their reports are proprietary. For example, some vendors say they review the source code; others say they've never gotten a comment on the source code.

Another source of insider attack on the vote count is at the Board of Elections. Election board members are open partisans. While, we do not accuse them of corruption, we do not think voters should need to rely on their honesty to ensure the accuracy of the vote. An independent voter verified paper ballot protects the Board of Elections by providing an irrefutable check and balance that the voters will trust.

In addition to an insider trying to affect the election results, another common problem is software malfunctions. A bug or glitch in the software, or a virus, or some other malfunction should be expected when dealing with computers but the review by Maryland Legislative Services did not examine this potential either. This has been the most common problem with paperless electronic voting throughout the country.

We can put a man on the moon. We cannot stop sophisticated insider attacks on computer systems. Therefore a second system to independently audit and recount the vote is needed – voter verified paper audit ballots are essential for every vote case on electronic voting machines.

The insider threat is a real one that is relevant, regardless of the quality of the ITA.

II. Every component of the Diebold Paperless Voting Machines are Vulnerable to Outsider Attack.

The findings of Maryland Legislative Services Division on the potential for outside attack were consistent with the findings of computer security experts from throughout the United States. The key conclusion was:

“The team focused on smart card, AccuVote-TS terminal security, and the methods used to upload results of an election. In each instance the team found vulnerabilities that could be exploited by malicious individuals. [Emphasis added.]”

Unfortunately, these findings were made after the Board of Elections claimed to have added the security requirements of the SAIC report. While the report recommended a number of fixes to deal with these problems in briefing the committee they also acknowledged that new challenges will constantly face voting and therefore there will need to be constant vigilance and constant security upgrades – thus some paper audit ballots are essential.

A. Security Updates to the Operating System Have Not Been Properly Applied

Regarding ongoing security, the track record of the equipment providers and the Board of Elections is not a very good one. As the report noted, the Dell computer used in vote counting was 15 security patches behind in updating security flaws then, and is likely even more so now. In addition, many of the problems with the Diebold machines noted in this report were highlighted in a July 23 report by the Johns Hopkins Information Security Institute – the Board of Elections has still not implemented them and will not be able to do so in time for the March primary.

When Delegate Leroy E. Myers, Jr. said at the briefing that – if this were Halloween, you’d be scaring me – and then asked to compare the accuracy, reliability and security of the Diebold system with other voting systems he was told that – “the difference here is the risk here is greater – with electronic machines when the problem happens it is catastrophic.”

When asked about a potential virus attacking the computer voting systems and how that would affect the vote count, the response at the briefing: “All bets are off.”

To be fair to the Board of Elections, applying patches to a large number of computer that are a part of a complex system is not something to be done lightly. Computer journals are rife with examples of mission-critical applications that have stopped working as a result of a patch being applied. However, this merely points up the fact that the operating system is too complex to be the only record of votes cast. A voter-verified paper trail is absolutely essential when faced with systems of this complexity and fragility.

B. Attaching Printers to Only Some of the Machines is Not Sufficient and Creates New Security Concerns

As a result of the need for constant security upgrades the report concluded that some form of voter verified paper ballots for the purpose of audits is needed in all voting precincts. Indeed, this security fix was the only thing on which all the consultants all agreed saying:

“In discussions amongst the team members, there was no single consensus recommendation, except that the introduction of voter-verifiable paper receipts is absolutely necessary in some limited form. The number of software vulnerabilities such receipts mitigate, the amount of savings they introduce by lowering the procedural requirements, and the trust they garner are likely to be just as cost effective in the long run as a fully locked-down all-electronic system.”[Emphasis added.]

Thus, the recommendation is to upgrade all the machines software to allow for printing of a paper audit ballot verified by the voter, upgrade all machines to be printer capable, but only allow for a small fraction of the votes to actually have a paper audit trail.

Unfortunately, attaching printers to only some of the machines does not resolve any security problems and creates additional issues. The software in the machines can detect whether there is a printer attached or not, and will know if the machine is printing a ballot as a part of completing the vote. As a result, malicious software can simply avoid cheating if it knows it is running on a machine that has a printer attached. Furthermore, the fact of adding a printer to some machines will result in two configurations of the voting terminals. There is way to ensure that both configurations will behave identically, even absent any malicious intent. How many times have you added a driver or attached a device — such as a digital camera — to a computer, only to discover that some totally unrelated device — such as your sound card — has stopped working?

Beyond these immediate technical issues, what happens if there is a discrepancy between the electronic vote count and the voter verified paper ballot on the machines with printers

attached? Under this proposal there will be no way to independently audit the ballots cast on the machines without printers. Such a discrepancy between electronic and paper votes on some machines, that cannot be checked for other machines, will create election chaos and make it impossible to declare a result of the election.

C. Adding Tamper Seals to the Machines Makes Certain Types of Voting Fraud Easier

The recommendation in the Trusted Agent report that the voting terminals be sealed by using tamper tape would actually make it easier to conduct a denial-of-service attack against particular precincts. Once the tape is in place, if a malicious individual were to merely slit the tamper tape on all or even some of the machines, there would be no way to know if any tampering had actually occurred.

While the report recommends using two layers of tape, one outside the bay and one inside the bay so that a simple slitting of the outside tape is no sufficient to compromise an election, the report also provides evidence that the system is still vulnerable to this sort of attack.

First of all, merely slitting the outside tape would result in a significant delay of the voting process, as an election judge would need to unlock the machine, verify that the internal seal was still intact, and re-seal the outside of the bay. Beyond this, slitting the internal tape is relatively easy. Lock picking skills are not necessary, according to the report:

Maryland has ordered approximately 16,000 AccuVote-TS terminals each equipped with two locking bays and supplied with two keys accounting for 32,000 locks and keys. *Surprisingly, each lock is identical and can be opened by any one of the 32,000 keys.* Furthermore, team members were able to have duplicates made at local hardware stores. It is a reasonable scenario to assume that a working key is available to an attacker. [Emphasis in the original.]

Once the cutting was discovered, the likely result in that polling place would chaos, as no one could be sure as to what might have been tampered with. If the cutting was discovered late in the day then no one who had voted prior to that time could be sure that their ballot had been accurately recorded. Furthermore, the polling place would be closed down for some time while evidence was collected and backup procedures activated, depriving people who are time-constrained of the opportunity to cast their votes.

This technique requires no additional equipment beyond a long fingernail. It is closely related to other well-known types of vote tampering from the Jim Crow era that seek to deny people in particular precincts the right to vote by making it extremely inconvenient to cast their ballots, thus removing entire districts of support for particular candidates. Older methods relied on cruder techniques such as pulling a fire alarm or removing street signs; simply slitting the tamper tape takes seconds, is difficult to observe, and does not require any special skills.

III. Misstatements: Cost and Recount

Maryland Legislative Services made two critical misstatements in their briefing to the committee. First, concerning the cost of upgrades and second, concerning the ability of paperless voting machines to conduct recounts.

A. Maryland should not have to pay for upgrade to voter verified paper ballot audits when other governments get them for free.

When jurisdictions have required a voter verified paper audit record, Diebold has provided such upgrades for no charge. This is true in four California counties that have purchased the machines. When Mr. Karl Aro testified that a voter verified paper ballot would be very expensive he did not mention that Diebold has provided such upgrades to other jurisdictions for free when it is required. This critical omission misstated the reality Maryland faces – there should be no cost for an upgrade to a voting system that is secure and can be trusted.

Maryland seems to have been consistently overcharged by Diebold. We seem to have paid \$5,000 per machine while California paid \$2,800 per machine when press reports on the cost of Diebold machines are reviewed. In emails Diebold employees have urged that Maryland be charged up the “yin-yang” for upgrades to voter verified paper ballots and to make it “prohibitively expensive” for Maryland, while giving free upgrades to four California counties – it seems Maryland is paying more and getting less.

Maryland should require that voting include voter verified paper ballots. If Diebold cannot provide Maryland the same price they have provided California counties then the contract should be cancelled.

B. The Diebold Machines Cannot Conduct Independent Recounts.

While the Diebold machines are capable of printing the ballots, they only do so after the voter has left the voting booth and after the software has counted the vote. Thus, when Alleghany County conducted a so-called recount in the 2002 election, the only result that was possible with such a recount was the same result – after all, they were only recounting whatever the software had counted the first time. If the Diebold software had incorrectly recorded a ballot the first time — whether as a result of a hardware malfunction, a software bug or malicious tampering — it would incorrectly report the vote the second time, with no independent way to confirm the result.

Mr. Aro testified before the committee that the recount in Alleghany resulted in the same as the first count. He did not testify that no other result was possible since the same software was essentially counting again. When I mentioned this to him after his testimony he agreed that the machines really do not conduct an independent recount. While not as egregious as the previous example, once again his omission misled the committee into thinking that the Diebold machines actually conduct a recount.

Conclusion

The advantage of the voter verified paper audit ballot are two-fold: (1) the voter verifies the vote before the software counts it; (2) the paper ballot is printed before the software counts it. Therefore, there is the possibility of a real recount, an independent recount — independent of Diebold hardware and software — one in which the voter has verified the ballot and therefore will have confidence in the result. A close electoral victory, like the upset vote in Alleghany County in the last election, is cast in doubt with paperless machines that cannot conduct independent recounts.

While the Maryland Legislative Services Division recognized the essential need for voter verified paper ballots they did not go far enough – voter verified paper ballots for independent audits and recounts are essential for every Maryland vote, not just a fraction of them.