# An Examination of Vote Verification Technologies: Findings and Experiences from the Maryland Study[1]

*April 15, 2006*

*Alan T. Sherman*, Aryya Gangopadhyay†, Stephen H. Holden†, George Karabatis†,*
*A. Gunes Koru†, Chris M. Law†,*

*Donald F. Norris**, John Pinkston*,*
*Andrew Sears†, and Dongsong Zhang†*

*National Center for the Study of Elections*
*of the Maryland Institute for Policy Analysis and Research*

*University of Maryland, Baltimore County (UMBC)*
*Baltimore, Maryland 21250*

**Department of Computer Science and Electrical Engineering*
*†Department of Information Systems*

***Department of Public Policy, and Maryland Institute for Policy Analysis and Research*

**Abstract.**
We describe our findings and experiences from our technical review of vote verification systems for the *Maryland State Board of Elections (SBE).* The review included the following four systems for possible use together with Maryland's existing Diebold AccuVote-TS (touch screen) voting system: VoteHere Sentinel; SCYTL Pnyx.DRE; MIT-Selker audio system; Diebold voter verified paper audit trail. As a baseline, we also examined the SBE's procedures for "parallel testing" of its Diebold system. For each system, we examined how it enables voters who use touch screens to verify that their votes are cast as intended, recorded as cast, and reported as recorded. We also examined how well it permits post-election auditing. To this end, we considered implementation, impact on current state voting processes and procedures, impact on voting, functional completeness, security against fraud, attack and failure, reliability, accessibility, and voter privacy.

Our principal findings are, first, that each system we examined may at some point provide a degree of vote verification beyond what is available through the Diebold System as currently implemented, provided the system were fully developed, fully integrated with the Diebold system, and effectively implemented. Second, none of the systems is yet a fully developed, commercially ready product.

This interdisciplinary study—the first of its kind—is of interest for the way in which it evaluates the systems, for the technical questions it raises about standard interfaces, and as a snapshot of the state of vote verification technologies and their commercial development.

**Keywords.**
Diebold AccuvoteTS, Diebold VVPAT, Direct Recording Equipment (DRE), computer system security, electronic voting systems, information assurance, Maryland State Board of Elections, MIT Selker VVAATT, parallel testing, Scytl Pnyx.DRE, VoteHere Sentinel, vote verification technology.

## 1 Introduction

On August 19, 2005, the *University of Maryland, Baltimore County (UMBC)* on behalf of the University's *Maryland Institute for Policy Analysis and Research (MIPAR)* entered into a memorandum of understanding with the State Administrator of Elections to provide a technical analysis of commercially developed vote verification technologies. This paper is a summary of Part 1 (Technical study) [Nor06a, Nor06b] of a two-part study.[2] Part 2 (Usability Study) was conducted by Herrnson and other researchers [Her06] at the University of Maryland, College Park. Separately, Norris [Nor06c] surveyed how Maryland registered voters feel about voting and voting technology.

We conducted this study at a time when concerns about electronic voting on *Direct Recording Electronic systems (DREs)*–otherwise known as touch screen voting systems–and independent verification of voting on DREs, have become a focus of national attention. Over the past year or so, a nationwide rush to adopt a solution to the "problem" of touch screen voting appears to have occurred. Twenty-six or more states, for example, have adopted or appear to be in the process of adopting requirements to include independent verification systems, nearly all based on a *voter verified paper audit trail (VVPAT).* Unfortunately, little is

[1] Support for this research was provided in part by the Maryland State Board of Elections. For our full report, see Norris, *et al.* [Nor06a, Nor06b].

[2] Although the State Administrator of Elections contracted with us for the study, we conducted the study completely independently.

understood about verification systems. In the absence of scientific data to support a move to VVPAT, and unlike many other states, Maryland commissioned a study before taking action.

Issues commonly raised for DREs include the following. Do they record, store, and count each voter's vote as the voter voted it? Can they be corrupted? Can they be effectively audited? Can their level of security be assessed accurately?

The focused charge of the UMBC study was to evaluate how effective certain vote verification systems are as a means for (1) providing independent verification of the vote recorded on the Diebold AccuVote-TS voting system used in Maryland, and (2) creating an acceptable audit trail. The information in our study is intended to help the citizens of Maryland, members of the General Assembly, the Governor's Commission on the Administration of Elections, the *State Board of Elections (SBE)* and the Governor in coming to informed decisions about how to administer elections in Maryland.

The UMBC study did not examine the security of the existing Diebold system, nor address the broader question of what election system Maryland ought to use. Also, the systems examined were examined only for possible use as verification systems, and not as stand-alone election systems. From the scope of the UMBC study, the reader should not infer that the UMBC study group advocates using DREs, verification systems, or any particular voting system. Similarly, the reader should not infer that the UMBC group is against any particular voting technology, including precinct-count optical scan.

A unique feature of the interdisciplinary UMBC study of verification technologies is that it was carried out within the context of the processes and conduct of real elections. To this end, we examined the detailed procedures used to conduct elections in Maryland, as defined by the SBE [Mar06].

The systems for possible inclusion in this study were VoteHere Sentinel, SCYTL Pnyx.DRE, MIT-Selker audio system, Diebold VVPAT, *Democracy Systems, Inc. (DSI)* VoteGuard, IP.Com, and Avante. VoteGuard is a visual system that includes a record of screen images from each DRE (and election management system). We also examined the SBE's procedure of "parallel testing" of the Diebold AccuVote-TS voting system. We used the Diebold DRE system as currently implemented in Maryland with parallel testing as a baseline against which to evaluate each vote verification system.

Ultimately, the following three systems were not included in the study. IP.Com did not meet the criteria of an independent vote verification system. Avante indicated it did not want to participate. DSI would not provide its system. UMBC signed a non-disclosure agreement with each of the other vendors to have access to their systems. DSI, however, required that UMBC also sign a non-compete agreement, which UMBC refused to do as a matter of policy.

The scope of work included six tasks.
(1) Technically review each vote verification system, including examining and testing all hardware, software, and documentation.
(2) Comparatively analyze the risks for each vote verification system (when used with the Diebold system and parallel testing) against selected review criteria, relative to each other and to the baseline Diebold system with parallel testing alone.
(3) Analyze the susceptibility to attack, fraud or failure of each of the verification systems.
(4) Assess the accessibility (*e.g.,* for individuals with disabilities, the elderly) of each vote verification system.[3]
(5) Assess the magnitude of effort and cost to implement and integrate each vote verification system with the current voting system and to maintain the integrated system.
(6) Estimate the impact of each vote verification system on the ability of voters to vote in the state's elections, on the State's current election procedures, and on the ability of election officials, election judges and volunteers to perform their jobs in actual elections and to adapt, manage, and use these systems effectively.

We took the position that our role was to provide the SBE with objective scientific assessments for each of the review criteria, and not to weight and balance these criteria.

For purposes of this study, *auditing* means the ability, through an alternative means and after the election is conducted, to establish that the votes recorded by the Diebold system correspond to the votes recorded by the independent vote verification system. *Vote verification* means the ability to confirm the accuracy of the Diebold system independently.

Although we carried out our study in the context of a particular Diebold System as used within Maryland elections, our work generalizes to most any DRE and any state.

We had agreed to provide a draft report by December 15, 2005, but we were unable to meet this deadline because we did not gain access to the VoteHere system until November 16, and to the Diebold VVPAT until December 20.

[3] Independently, researchers at the Center for Politics and Citizenship at the University of Maryland, College Park conducted a usability analysis [Her06].

The rest of this paper is organized in ten sections. Section 2 reviews previous work. Section 3 describes voting in Maryland. Section 4 summarizes our study methods. Sections 5–9 analyze each of the study systems. Section 10 discusses issues raised by our study, and Section 11 summarizes our conclusions and recommendations.

## 2 Background and Related Work

Voting methods in American elections have been called into serious question in recent years, specifically as a result of problems that occurred in the 2000 election in Florida [Cra03,Wan04, Cal01]. This election dramatically brought to the attention of the public the possibility of errors with punch card voting systems [Bei89a,Cra03]. Optical scans and lever systems have also been prone to undervoting (not voting in a race), overvoting (voting multiple times for one race) and misvoting [Cra03].

Due to these reported problems with other systems and as a result of the issues surrounding the 2000 presidential election in Florida, there has been movement toward electronic or touch screen voting [Cra03]. According to one study, the proportion of voters using electronic systems is expected to have increased from 13 to 29 percent between 2000 and 2004 [Wan04,Ele04]. Touch screen voting systems are also popular because it is felt that the systems are easy to use, more accessible to persons with disabilities, better able to accommodate multiple languages, prevent overvoting, provide quick results (with less human error), and eliminate costs associated with printing ballots [Bur03,Wan04]. A principal concern about touch screen voting systems is whether the underlying software of these systems can be trusted, especially whether the software can be trusted to record and count votes as cast by voters.

The election controversies of November 2000 also prompted a response at the federal level. In 2002, Congress passed the *Help America Vote Act (HAVA).* This legislation attempted to bring voting procedures, which until that point had been the responsibility of individual state governments, under the purview of the federal government [Kur04].

The bill was designed to combat a host of issues plaguing the voting process. Through a mix of new guidelines, requirements, and federal programs and funding, this legislation provides assistance for states as they update and improve their voting processes. Among other provisions, it requires states to upgrade away from the older voting systems, in this case mainly away from lever and punch card systems, and toward new touch screen and optical scan systems [Hol05].

HAVA also provided for the formation of the *Election Assistance Commission (EAC),* a federal body designed to promote the goals of the 2002 bill. Among other duties, the EAC was charged with helping the states successfully make the upgrade to new voting technology. The EAC would offer administrative and technical support, as well as provide grants to develop and test new election systems. It would also develop a program to test, certify and decertify election systems as they were introduced [Ele05].

What raised the concerns of critics of touch screen voting in this instance was that HAVA does not provide guidelines for states regarding performance tests on the newly approved voting technologies (especially touch screen voting systems), nor does it contain a requirement for any sort of independent verification systems [Kur04,Hol05,Pyn05].

There are also problems with the implementation timetable as far as providing access for disabled voters. Although the law did not go into effect until January 1, 2006, some voting system vendors are selling systems now, to be used for the foreseeable future, which do not meet the access standards of HAVA [Pyn05].

To address these criticisms, Representative Rush Holt (D-NJ) introduced the Voter Confidence and Increased Accessibility Act [Hol05]. According to Representative Holt's web site, the bill is chiefly concerned with a requirement that all voting machines produce a verifiable paper trail and a more general requirement for an "accessible voter-verification method." Finally, it addresses concerns raised by some security experts who warn of hacks and attacks if a voting system is ever connected to the Internet. Holt's bill prohibits such systems from being connected to the Internet or being attached to any insecure communication device. HR 550 has been relegated to a subcommittee, and it is unknown whether or how soon it will emerge, but it is important to note the bill because it encapsulates many of the concerns that lawmakers have about touch screen voting and limitations in HAVA's scope.

Several potential or actual problems have been identified around touch screen voting. First, problems exist on an individual level that might affect elections. These problems include voter trust in the system, readability of the touch screen systems, problems with smart cards (which prevent persons from voting more than once), issues around instructions and assistance to voters, ability to write in candidates, issues concerning the ability to administer the system, and privacy [Her05,Rub05].

To many, a greater concern involves the security of touch screen systems. Security issues include malicious programming, unintentional but nevertheless bad programming, equipment errors, tampering with hardware, system malfunctions including crashes, the inability to recount votes independently, and issues about the correct capture of votes [Bur03,Cra03, Hal04,Mac04,Rub05,Sel04, Wan04,Han02]. To correct these security issues, calls have been made for open source coding (which would allow for independent examination of programming of electronic voting systems), voter verifiable paper trails (which could also be used for auditing), and active testing programs of the equipment and software [Bei89a,Bru04, Sel04,Han02].

In 2004, less than 40 percent of voters actually looked at the VVPAT printer screen, compared its display to that on the DRE, and touched the DRE to indicate they had verified [Los04]. For additional observations on verification systems in real use, see Selker [Sel05].

## 3 Voting in Maryland

In 2001, the Special Committee on Voting Systems and Election Procedures recommended to the Governor and General Assembly that a statewide voting system be implemented in Maryland. Subsequently, House Bill 1457 (2001) was adopted. This bill required a statewide, uniform voting system for polling-place voting and a uniform system for absentee voting. After the law became effective, and as the result of an open, competitive bid process, the *State Board of Elections (SBE)* selected Diebold Election Systems, Inc., to provide a DRE voting system for polling-place voting, and an optical scan voting system for absentee voting.

This voting system was implemented in three phases. Phase I counties (Allegany, Dorchester, Montgomery and Prince George's Counties) implemented the voting system for the 2002 elections. These counties were selected because they used the oldest voting systems in the State: punch card for Montgomery County and lever machines for the others. The contract for Phase I was signed in 2002. The Phase II contract was signed in 2003, and Phase II counties implemented for 2004 elections. Phase III, which includes Baltimore City, will be implemented for the 2006 elections. With the completion of Phase III, Maryland will have almost 20,000 DRE voting units. Approximately 20,000 volunteers assist with elections.

By FY 2009, a total of about $95.5 million will have been spent by state government on this system. Of that amount, about $45.6 million will have been spent on hardware and maintenance, and almost $50 million on a variety of necessary support services including security measures, warehousing, transportation, voter outreach, support services, technical support, testing of various kinds, and project management. This amounts to a state government cost of almost $2.82 for every Maryland resident (5.6 million) and just over $5.10 for every Maryland registered voter (3.1 million) per year for each of the six years. This cost includes providing every jurisdiction in the state with all of the equipment needed to conduct an election, as well as some level of technical assistance and voter outreach.

Maryland has a dual election system in which the SBE and the *local boards of election (LBEs)* share authority and responsibility for administering elections. Each jurisdiction in Maryland (23 counties and Baltimore City) has a local board of elections. Under Maryland's Election Law Article, the LBEs and their staff are subject to the direction and authority of the SBE and are accountable to the SBE.

Election equipment, including the Diebold DREs and election management system servers are stored by each LBE.

## 4 Study Methods

In conducting this study, we examined both non-technical and technical aspects of the vote verification technologies. The non-technical aspects included implementation of these systems within the framework of the current Maryland election policies and procedures, and the impact of the vote verification technologies on these procedures and on voters and voting in Maryland. The technical aspects included data management, reliability, functional completeness, accessibility, election integrity and voter privacy. In this section we describe our study methodologies and evaluation criteria.

For each system and evaluation criterion, we reported our assessments in two ways: we assigned a subjective numerical rating from one (low) to five (high), and we wrote a narrative of the system's strengths and weaknesses. Table 1 presents these scores. Each system was evaluated as it would be used with the existing Diebold system and parallel testing.

We asked each vendor to define one particular version of their product, and to supply a testable reference implementation matching the given specification. None of the vendors fully complied with this request.

Each vendor meet with the study team at least once, and each vendor provided the study team with a sample product to test and examine. To various degrees, all of the evaluations were complicated by the preliminary states of development of the products, the lack of standard product configurations, insufficient detailed product information, and lack of access to Diebold software which must be modified to integrate the products.

### 4.1 Implementation

We estimated the one-time and on-going costs to integrate each verification system into Maryland elections, assuming a product configuration we defined. Product cost estimates were based on vendor comments, each of whom promised "to be competitive." Some of our cost estimates were based in part on data provided from other organizations, most notably the Asian Pacific American Legal Center, which provided an estimate of the impact of voter verified paper trail submitted to the California Assembly in 2004. Cost estimates also include required modifications to the Diebold system.

### 4.2 Impact on Voters and Election Procedures

We examined the ways in which adding vote verification technologies to the current Maryland process of elections would affect that process and the voters. We considered additional steps voters must take, the time required to vote, and the amount of assistance required.

One-time impacts on election administration include acquiring devices, making physical and software modifications to the Diebold system, transporting the devices to the LBEs, establishing storage procedures and locations at the LBEs, creating a training program for LBE officials, developing and implementing security procedures, developing a technical assistance program, developing a voter education program, and monitoring these one-time activities.

Continuing impacts include maintaining and servicing the devices, inventory and storage, transportation, on-going training, technical assistance, setting up and taking down equipment, managing and operating the devices during an election, assisting voters, dealing with recounts, and continuing voter education.

### 4.3 Data Management

We examined how well each system stores and manages data against hardware and software failures, power failures, natural disasters, voter error, and accidental or malicious attack. Among the many events that can happen include a voter aborting the voting process in the middle, and cables becoming disconnected. The system should remain accessible or restorable.

In carrying out this evaluation, we applied each or the following criteria, which we adapt from the FEC voting system standards for data management: protect against any single point of failure, protect against failure of any input or storage device, protect data entry and storage against tampering, log all events, detect and log exceptional events, and maintain awareness of system status through diagnostics.

One important issue is to enforce "atomicity" of votes cast. It is desirable for the DRE and verifier to maintain consistent data stores of the votes casts, even in the event of failures. Traditionally, this might be accomplished through a two-way protocol in which neither unit would record the vote until both units have the information needed to do so. Without atomicity, there is the possibility of "lost votes"—for example, a vote stored on the DRE but not on the verifier—and the two units might not agree on the tallies, even if they are both honest. For more on this issue, and its relationship with security, see Section 10. Except for Scytl, none of the systems made any attempt to achieve atomicity of votes cast.

### 4.4 Reliability

To assess reliability, we tested the high-level usage scenarios for the systems and looked for failures. Our test cases covered the main functionalities. For Votehere, however, the product lacked sufficient functional completeness to perform any reliability testing.

### 4.5 Functional Completeness

We determined the degree to which each system actually provides the functions given in its product specifications. As one metric, we computed the ratio of implemented functions to those promised.

### 4.6 Accessibility

To examine the accessibility of the four systems, we used the standards of Section 508 of the Rehabilitation Act of 1973, as amended in 1998, for procurement of electronic and information technology [Reh73]. Specifically, we used the following subsections of these standards:
Subpart B–Technical Standards self contained, closed products, Subpart C–Functional Performance Criteria, Subpart D–Information, Documentation, and Support.

We evaluated the four devices as self contained products in a laboratory at UMBC using an expert review based on accepted standards. The user-based assessment regarding use by individuals with disabilities is part of Herrnson's [Her06] companion study.

### 4.7 Election Integrity and Voter Privacy

We separately evaluated how well each system mitigates threats to election integrity, voter privacy, and reliable operations, focusing primarily on integrity and privacy.

*Election integrity* means that each voter casts his ballot as intended; the system records the ballot as cast; the system tallies the votes as recorded; and the Election Boards certify the results as tallied. *Voter privacy* means that no one (besides the voter) can learn how the voter voted. Many voters view privacy as a fundamental right that is vital to prevent coercion, vote selling, and bribery. *Resistance to disruption* means that it is difficult for an unintentional or malicious adversary to cause a delay, rescheduling, or stoppage of the election process. A major difficulty in conducting elections is to achieve both election integrity and voter privacy.

The evaluations are for the entire composite systems, when used in combination with Maryland's existing Diebold voting system and the security policies and procedures, including parallel testing, that have been adopted around it.

Evaluation criteria include votes cast as intended, votes recorded as cast, non-reliance on complex DRE hardware and software for integrity, physical security, protection of removable data devices, proper use of cryptography, sound key management, software implementation best practices, transparency, and prevention of vote correlations.

In assessing the systems, we also considered the following attack metrics: number of conspirators required, number of votes affected, number of machines, precincts, local election boards affected, cost (in dollars), time to carry out attack, computer resources needed (computer time, memory space), probability of detection, probability of success, required level of sophistication, and required knowledge, skills, and equipment.

## 5 Diebold AccuvoteTS with Parallel Testing

Parallel testing aims to detect widespread improper operation of DREs by carefully testing a sample of DREs randomly selected immediately before the election. The testing is performed on election day in a fashion that attempts to simulate exactly the true election experience. Volunteers "vote" on the sampled machines and also write down their votes on paper for later checking. SBE carries out parallel testing in partnership with the *Maryland League of Women Voters (LWV)*. This currently used video-taped process is the baseline verification system for our analysis.

Parallel testing adds significant value, provided the sample is indeed selected at random, the selected machines are not modified, and the selected machines cannot detect (*e.g.,* through signaling or perception of differences between the true and simulated election conditions) that they have been selected for parallel testing. Thus, significant care is required to carry out parallel testing properly.

Parallel testing does not detect possible widespread corruption of DREs where each corrupted DRE behaves properly unless signaled to behave maliciously.

Because the SBE already performs parallel testing, continuing this process should not require many, if any, additional state resources. The partnership with the LWV also helps keep on-going costs to a minimum. Because parallel testing is independent of actual polling, the impact on election administration is minimal and there are no privacy concerns.

See Appendix H of the full report [Nor06b] for a mathematical formula that computes the probability that the random sample will include at least one bad DRE. For example, if 50% of the 19,000 DREs in Maryland were corrupt, then sampling only 10 DREs would include a bad DRE with 99.9% confidence. However, if 1% of DREs were corrupt, then sampling 10 DREs would include a bad DRE with only 9.6% confidence; testing 100 units would increase this confidence to 63.5%. Currently, SBE selects a small number of machines, all from the same LBE.

## 6 Diebold VVPAT

The Diebold *Voter Verified Paper Audit Trail (VVPAT)* system consists of a small printer encased in a sealed take-up unit housing that attaches to the side of the DRE. After the voter selects his or her choices on the DRE, the DRE displays the voter's selections and requires the voter to print the ballot to begin the verification process prior to recording the votes. The voter's selections are directly sent from the DRE to the printer through an integrated serial port. The voter can view the printout through a glass panel.

If the selections displayed on the DRE correspond to the printout, the voter can accept and record his or her selections. Otherwise, the voter can reject the ballot and then modify his or her selections. At the end of an election day, the paper rolls that contain the printed votes must be moved from the printer and securely stored. When there is a need to conduct an audit or recount, the votes recorded on the paper rolls can be hand tabulated.

The Diebold VVPAT has a relatively fully functioning system. The system is simple. Because it is produced from the same DRE vendor, the system integration effort between the two ought to be relatively low.

During our testing, we encountered a high failure rate of the printer. Consequently, reliability of the Diebold VVPAT is low. Dealing with printer problems during an election would be challenging. At over $1,500 per unit (not including case and consumables), the Diebold VVPAT is also costly.

This system depends on the security and accuracy of counting the paper printouts. The system provides no cryptographic protection of the printed votes, and managing paper is fraught with significant security challenges. Moreover, the voter can verify only what goes into the paper storage unit; the voter cannot verify what comes out of the paper storage unit.

Each printout also contains an optical scan barcode that claims to encode the same information printed on the roll in plain text. Election officials could use these barcodes in counting the paper votes. Realistically, these bar codes cannot be checked in the voting booth. Moreover, they are generated from information sent from the DRE to the printer. As such, the barcodes cannot be trusted without trusting the DRE and the printer. Therefore, if the barcodes are used, they must be verified

The system raises threats to voter privacy because the paper roll preserves the order of the votes cast and can potentially be used to identify a voter and send clandestine signals. We could not evaluate accessibility because the vendor did not provide the equipment needed for such testing.

On general principles, it is problematic that the printer device is provided by the same vendor, Diebold, that produces the DREs. Thus, this system does not provide vendor independence in the verification-audit component. On the other hand, this concern is reduced somewhat given the simplicity of the printer unit.

## 7 MIT-Selker VVAATT

The *Voter Verified Audio Audit Transcript Trail (VVAATT)* system includes a voice-operated recorder that is connected to the DRE. The voter puts on headphones in the voting booth. Subsequently, every activity of the voter is spoken to the voter using an audio feedback mechanism and recorded on an analog audiotape. During an election audit, the tape can be played back and the votes can be manually counted and compared with those of the DRE.

One of the most significant advantages of this system is its use of audio verification: there is evidence that voters are much more likely to detect mistakes when checking with headsets than by looking on a separate screen or printed receipt. At $100 per unit for basic hardware, this system is also the cheapest.

The vendor for the VVAATT has a relatively well-developed prototype. The system is simple and easy to install. Since the tape recorder is independent of the DRE, integration with the DRE is easy. Being an analog audio record, this system eliminates the need to trust digital computers, provided no computers are used in automatically processing the tapes during a recount.

The system requires trust in LBEs to store the cassette tapes securely and in appropriate environmental conditions. The tapes have no cryptographic protection. Voters cannot verify what tapes are used in the recount process.

The vendor lacks a business plan for producing and marketing the large numbers of units that would be required if this product is selected. The system has significant accessibility problems (*e.g.,* to the hearing impaired) and is not resistant to disruption. The system currently provides only manual operations for playbacks and recounts of votes, making it very labor intensive, which might introduce significant impacts on election administration in the event of recounts.

As with the Diebold VVPAT, the audio recordings preserve the order of votes, permit voters to identify themselves through distinctive sequences of voting actions, and identify the language heard by the voter. These features pose threats to voter privacy. Although not included in the system provided to UMBC, an option exists for each voter to pick up a recording unit from a common basket of units to carry into the voting booth. At greater risks of damage to the equipment, this option partially addresses the drawback of recording vote order.

## 8 Scytl Pnyx.DRE

The Scytl solution is a device attached to the DRE that displays and stores an independent electronic record of the votes cast, providing a check against the threat that a malicious DRE might record a different vote from the one cast.

Once the voter has selected his ballot choices on the DRE, the DRE sends these choices to the Scytl device, where the voter can verify them.

Scytl automates the post-election audit process. Election board members can automatically check whether the DRE tally of the votes is consistent with the votes recorded by the verifier.

The accessibility of Scytl received the most favorable rating among the systems examined. However, there are still important improvements needed to make it fully accessible. The system is well documented and the vendor provided us with the necessary documentation (*e.g.*, use-cases) to improve our understanding of the system.

Scytl digitally signs the votes before storing them. During audit and recounting, a mixing protocol ensures privacy by shuffling the decrypted votes. Scytl is engineered well from security point of view and implements standard security protocols well.

However, Scytl requires complete trust in its software to ensure that the vote recorded in the verifier is the vote displayed on the verification screen. The digital signatures do not change this fact. In this sense, the voter cannot verify either the DRE or Scytl tally.

Scytl is a software intensive solution. It lacks some of the functionality given in its specifications, but implements more than half of the specified system. There were, however, frequent failures in operation. The vendor was helpful and made some recommendations to solve some of the problems, yet some important failures persisted.

The implementation of this solution will require additional development effort because Scytl must communicate with Diebold's DRE software to receive votes in appropriate file formats, and Scytl requires the DRE to receive an acknowledgment from the verifier. In addition, the cryptographic protocols in this solution will put some burden on the officials at the SBE and LBEs. For example, keys needed for audits and recounts must be generated and distributed among election officials. Each units costs approximately $500.

## 9 VoteHere

VoteHere provides a method of voter verification of election integrity, based on receipts and complicated mathematical cryptography [Nef04,Gre03].[4] In the voting booth, the voter enters his ballot choices on the DRE and verifies those selections on a printed "receipt" (audit record), which he may take home. The receipt defines an encrypted ballot; the receipt does not reveal how the voter voted. After the voting process, the voter may check that a copy of this receipt (and thus his ballot as cast in the voting booth) is included in the official election data posted on a public web site. Anyone, using trusted complex mathematical software of his choice, can verify that the official results are consistent with the posted data.

DREs require trust in proper implementation of computer system security to safeguard *voting machines*; by contrast, VoteHere requires trust in cryptography (that can be checked by experts) to enable voters and observers to verify the correctness of *election results.*

All VoteHere software is open source, of high quality [Dal05], and election integrity depends little on this software. VoteHere provides very high election integrity, provided that enough voters verify their votes in the voting booth, enough voters check that their receipts are in the official data, and enough verifiers check the tallies against the data—regardless of whether voters understand VoteHere's complicated underpinnings.

Disadvantages include the following. First, the product is not functionally complete, existing only as a reference library without application software. Second, the voter's experience in the voting booth is slightly complicated. Third, because the system is complicated to understand, election officials will have to be educated in it and will also have to be able to educate voters, and some voters might not have confidence in a system they do not understand. Fourth, voters with limited eyesight might have difficulty reading the receipt, and the planned functionality for alternative user interfaces is not yet available. Fifth, election officials must set up and maintain an authenticated web site. Sixth, as configured, there is no attempt to maintain consistency between the Diebold and VoteHere systems, even when both units are honest. Seventh, as is true for all systems under study, the system requires integration with the DRE display software. Each unit costs approximately $500.

## 10 Discussion

In this section we discuss a variety of issues raised by our study.

Some people now say the SBE asked the "wrong question" in having our study group consider only the possibility of adding a verification audit system to the existing Diebold system. Some of these critics, who now advocate replacing the DREs with a precinct-count optical scan system, now state they would have liked us to examine fundamentally different alternatives to the Diebold system. There are many important questions that the SBE ought to consider. We simply answered one such question that we were asked to answer and take no position on other possible questions, nor the relative merits of such questions.

The SBE framed the question in the way it did largely because, in 2005, the Maryland General Assembly mandated such a study. Although Governor Ehrlich vetoed this legislation, the SBE felt such a study was important and secured approval from the Department of Budget and Management to

[4] For a detailed description of the VoteHere system defined for the Maryland study, see the full report [Nor06a,Nor06b].

proceed with it. In addition, Maryland is already financially committed to paying for Diebold machines through 2012, regardless if it continues using those machines. Even if one believed that Maryland should ultimately switch to a fundamentally different system, it does not necessarily follow that it would be good public policy to spend an additional $25–50 million to purchase a new system now.

There is some merit to the strategy of enhancing voting assurance through the use of independent verification audit systems connected through a standard interface. An adversary would have to compromise two systems rather than one, increasing the adversary's difficulty, cost, and chance of detection.

There are also fundamental limitations to this strategy. Any such add-on system will increase cost and complexity, as well as the chance for failure or disruption. There are more components to go wrong, and more chances for the parts to end up with conflicting tallies. If each component depends on the other, then either component can cause both to fail. If an adversary can subvert one system, it might not take much additional difficulty also to subvert the second system. Furthermore, it may be difficult in practice to achieve true independence of components. By contrast, simplicity tends to lead to enhanced assurance.

For the products we examined, it is necessary to integrate the verification-audit system with the existing Diebold system. Currently, this task is highly problematic. There are no interface standards. Modifying any Diebold software requires cooperation from Diebold. Although Diebold is contractually obligated to cooperate, it is not commercially motivated to do so because it sells a competing product. Also, someone other than Diebold must pay for such modifications. National standards for interfacing voting system components would be very helpful in overcoming these problems.

Data management issues related to recording the votes are important, yet only Scytl made any attempt to address the following issue. The DRE and verifier comprise a two-part distributed system, where each of the two units contains a repository of votes cast. In such system, casting a vote in the booth is an atomic transaction spanning the DRE and the Verifier. The two repositories should remain consistent, *i.e.,* should record the same votes. If atomicity is not enforced, the two repositories may not record the same votes, leading to a difference in the vote counts between the DRE and the Verifier—exhibiting the phenomenon of unrecorded votes. This data management issue also has security implications.

It is nontrivial to implement a solution to the above data management problem that has satisfactory security properties, and theoretical research on the Byzantine generals problem [Lam82] imposes some limitations on what is possible. The two-way handshake protocol of Scytl creates an undesirable situation in which each unit (DRE, verifier) can cause the other to fail. Also, a bidirectional connection between DRE and verifier might facilitate two corrupt units to agree on a consistent, but fraudulent, tally.

At least one vendor, VoteHere, did not fully accept the ground rules imposed by the SBE that the new product be an add-on verification-audit system, rather than a separate stand-alone system that simply uses the existing DRE as a front-end user interface. Although VoteHere mentioned that alternative designs could be worked out, its main suggestion was for their system to provide the sole official election results. Its logic was that because its system provides provable voter-verified election integrity, a second tally would be unnecessary. We do not fully agree with this point of view: to the extent to which it is beneficial to have two independent systems, it would be better to enable the DRE to provide an independent tally, regardless of the high assurance of VoteHere.

From the beginning, the SBE stated that it would consider procuring only sufficiently developed commercially ready products. Soon it became apparent that none of the "products" met this condition. Most of the vendors sought a different sort of arrangement: to open a dialog and partnership with the SBE toward developing a system for Maryland.

It is a bad idea for governments to buy products that are not functionally complete and that either do not have positive records in the market place or that cannot be fully and effectively tested in simulated elections to ascertain their performance characteristics.

However, there are situations where it is appropriate for governments to engage in creative well-managed partnerships with industry to promote applied research and product development, especially for emerging technologies that promote social good. Moreover, voting technology, including receipt-based voting, is such a situation. Thus, we would be happy for Maryland to consider investing prudently in such a partnership, perhaps in combination with other states. Such a partnership could include discounts on possible future product purchases, and strict performance guarantees on any resulting products.

By 2007, Maryland will have spent approximately $96 million on Diebold equipment. A small fraction of that expense invested in a creative partnership might greatly facilitate and accelerate the development of promising new voting technologies, such as high-assurance receipt-based systems. We recommend that all states invest at least 2% of their expenditures for voting machines on research in better voting technology.

Regardless, for all of the products examined, it is unfortunate that the vendors did not do a better job at providing each of the following essential elements: detailed product description including functional specifications, testable reference implementation meeting the functional specification, product performance data from a real or mock election, security and privacy analysis, and appropriate documentation.

It would be unreasonable to require, as some states do, that any new voting system first be proven through official use in some other state. If all states adopted such a policy, there would be no innovation. Instead, it ought to be sufficient to provide performance data from a suitable mock election, carried out by an independent testing organization.

## 11 Conclusions, Findings, and Recommendations

In this study we have examined four vote verification systems, as well as the SBE's method of parallel testing. We examined them using the following criteria: implementation, impact on voters and election administration, data management, functional completeness, reliability, accessibility, election integrity, and privacy. Table 1 gives our summary ratings.

Table 1 presents ratings from 1 to 5 for each criterion for each system including parallel testing. A rating of 1 means that the system (when used with the existing Diebold system and parallel testing) does not meet the criterion at all, and a rating of 5 means that a system meets a criterion completely.

We chose not to average any of the scores for two reasons. First, different persons or organizations might assign different weights to each of these criteria. For example, for some, security may have the greatest importance, while for others, the impact on voters and election administration may be foremost. Second, for some of the systems, some of criteria did not apply, or we were unable to conduct some tests because vendors did not provide the full range of equipment necessary.

In terms of election integrity, each system under study requires a different type of trust. For example, parallel testing requires the voter to trust that the selection of units to be tested is random and that the selected units cannot be signaled to behave properly. VVAATT and VVPAT require the voter to trust that the audio or paper tapes are stored securely and counted accurately. Scytl requires the voter to trust that the system works as claimed: the voter cannot examine or verify system software for himself. VoteHere requires voters to trust cryptographers of their choice that certain security properties are true (mainly, that trusted software of their choice can verify that the posted results are consistent with the official election data).

Verification systems that preserve voting order (VVAATT and VVPAT) notably degrade voter privacy. All verification systems have the potential to degrade voter privacy by increasing risks without correcting existing vulnerabilities. Similarly, all verification systems typically increase the risk of disruption by increasing the number of components and processes that can go wrong.

**Table 1: Summary evaluations of vote verification systems.** Table 1 presents ratings from 1 to 5 for each criterion for each system including parallel testing. A rating of 1 means that the system (when used with the existing Diebold system and parallel testing) does not meet the criterion at all, and a rating of 5 means that a system meets the criterion completely. *N/A* means *not applicable* because voters do not participate. *N/E* means *not evaluated* because the vendor did not provide the necessary equipment. Although parallel testing perfectly preserves voter privacy because it does not use real voter data, it does not correct the threats to voter privacy created by Diebold AccuvoteTS. Therefore, parallel testing receives the same privacy score as the baseline score for Diebold.

| | Parallel Testing alone | MIT-Selker VVAATT | Scytl | Diebold VVPAT | VoteHere |
|---|---|---|---|---|---|
| Implementation | 5.0 | 3.5 | 2.2 | 1.5 | 2.0 |
| Election Administration | 4.0 | 2.5 | 2.0 | 2.0 | 1.0 |
| Data Management | 1.2 | 1.8 | 2.5 | 1.3 | 1.3 |
| Functional Completeness | 5.0 | 2.5 | 4.0 | 5.0 | 1.0 |
| Reliability | 5.0 | 4.0 | 2.0 | 2.0 | N/E |
| Accessibility | N/A | 1.0 | 3.0 | N/E | 2.0 |
| Election Integrity | 3.0 | 3.5 | 4.0 | 3.5 | 5.0 |
| Privacy | 3.0 | 1.5 | 2.5 | 1.5 | 2.0 |

### 11.1 Findings

We now summarize the principal findings of our study. First, each of the systems that we examined—only one of which provides for a pure paper solution—may have something to offer the State of Maryland in terms of vote verification. But this would be true only if the system were fully developed, fully integrated with the Diebold DREs and effectively implemented.

Second**,** none of these systems is a fully developed, commercially ready product. None of these products had been used in an election in the U.S. (The Scytl system has been used outside the U.S., and a different version of the Diebold VVPAT has been used in the U.S.).

Were Maryland (or any organization) to decide to acquire any of these products, anywhere from a relatively small to a considerably large amount of money and effort would be required on the part of the vendor to produce an actual product and make the product ready for use in actual elections.

Third, introducing any of these vote verification products would involve both potential benefits and the following costs.

(1) All of these products would impose significant one-time implementation and on-going management burdens (cost, effort, security) on the SBE and the LBEs.

(2) To a greater or lesser extent, all would increase the complexity of the act of voting.

(3) To a greater or lesser extent, all would increase the amount of time required to vote.

(4) All would likely, in balance, approximately double the amount of effort required to administer elections, because two systems would have to be managed. It is true, however, that some products include election management tools that could facilitate certain aspects of election management.

(5) All would offer the potential to affect voter privacy adversely.

(6) These products would have both potentially positive and potentially negative impacts on security (*i.e.,* increase the possibility that votes will be recorded and counted as cast, and increase the possibility of disruption).

(7) None of the products are fully accessible to individuals with visual or hearing impairments, and none of them fully meets the accessibility standards of Section 508 of the Rehabilitation Act.

(8) Integration of these systems will require the cooperation of Diebold to develop and/or ensure the viability of a working interface between the vendor's product and the Diebold system.

### 11.2 Recommendations

Based on the evidence from this study, we could not recommend that the State of Maryland adopt any of the vote verification products that we examined at that time.

No election system, regardless of the technology involved, is foolproof nor is any election system completely immune or secure from fraud and attack. Indeed, there is a long and inglorious history of election fraud in the U.S. that dates back to the founding of the country or before and involves nearly all methods and technologies of voting. It would be prohibitively costly to make any election system—or an information system for that matter—totally secure.

Regardless of what the state does in the near term with regard to vote verification, 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. These additional measures might include: randomly selecting DREs for the test the day before the election; ensuring that the persons responsible for parallel testing are not the persons who loaded the software; selecting a larger number of DREs, possibly from more than one jurisdiction for testing; and ensuring that conditions for the test are as nearly identical to a real election as possible. The SBE should continue to monitor and record the parallel test carefully.

To summarize, each of the products we examined could, if fully developed and properly implemented and managed, offer some value in the area of vote verification. However, none is fully developed. Additionally, potentially significant tradeoffs exist with all of them (*e.g.,* greater election integrity and potential for degraded privacy), and all would require considerable cost and effort to implement and to manage during elections. For these and other reasons, we could not recommend that the state of Maryland acquire and implement any of them at that time

## Acknowledgments

We thank the many people who contributed to the Maryland study of vote verification technologies. Among these people are CoPI Charles Nicholas; graduate student assistants Markus Dale, Kevin Fisher, Rosa Heckle, Kenny Khoo, Evan Perlman, Mohammad Ammar Sheikh, Tonya Zimmerman; and undergraduate student Assistant Chiedozie (Fred) Unachukwu.

We thank Linda Lamone, State Administrator of Elections, and her staff, particularly Ross Goldstein, Deputy Administrator and Nikki Trella, Election Reform Director, for their assistance during the course of this study, including providing details about voting procedures in Maryland.

We also express our appreciation to Anne Roland (MIPAR and Public Policy) Gay Warshaw (MIPAR) for editorial assistance, and to Richard Carback for helpful comments.

## References

[Bei89a] Beiler, David. (1989a). A Short in the Ballot Box. *Campaigns & Elections. 10*(2), 39-41.

[Bei89b] Beiler, David. (1989b). Shortfall in the Sunshine State. *Campaigns & Elections.* 10(2), 40.

[Bru04] Brunvard, Erik, John Carter, Alan Dechert, David L. Dill, Kathy Dopp, Gensh C Gopalakrishnan, David Hanscom, Michael Jones, Arthur Lee, Jay Lepreau, Kent Seamons, Peter Shirley, Barbara Simons, Association for Computing Machinery, Pamela Smith, and Phillip Windley. (2004). Response to 'American Attitudes about Electronic Voting' Survey and Advice for Utah's Voting Equipment Selection. Memo. Retreived from UtahCountVotes.org/Voting_systems.pdf on 11/2/2005.

[Bur03] Burmester, Mike and Emmanouil Magkos. (2003). Towards Secure and Practical E-Elections in the New Era. In Dimitris Grizalis (Ed.). *Secure Electronic Voting.* (p. 63-76). Boston: Kluwer.

[Cal01] Cal Tech/MIT. (2001). Cal Tech/MIT Voting Technology Report: What is, What could be, Fast Facts. Retrieved from www.vote.caltech.edu/media/documents/july01/fast_facts.pdf on 11/3/2005.

[Cra03] Cranor, Lorrie Faith. (2003). In Search of the Perfect Voting Technology: No Easy Answers. In Dimitris Gritzalis (Ed.). *Secure Electronic Voting*. (p. 17-30). Boston: Kluwer.

[Dal05] Dale, Markus. (2005). Static analysis of the VoteHere VHTi reference implementation source code using Flawfinder and RATS. CMSC-691 Information Assurance Project Report, University of Maryland, Baltimore County (December 28, 2005), 14 pages.

[Ele05] Election Assistance Commission. (2005). About the EAC. Retrieved from http://www.eac.gov/about.asp?format=none.

[Ele04] Election Data Services Press Release from 2/12/04 called New Study Shows 50 Million Voters will use Electronic Voting Systems, 32 Million Still with Punch Cards in 2004. Retrieved 1/10/06 from www.electiondataservices.com.

[Gre03] Green, R., and J. Adler, Threat analysis, VoteHere (2003), unpublished manuscript, 24 pages. http://www.votehere.net/downloads.php

[Hal04] Hall, Thad E. and R. Michael Alvarez. (2004). *American Attitudes about Electronic Voting: Results of a National Survey.* Salt Lake City, UT: Center for Public Policy & Administration.

[Han02] Hanging Bytes, Pregnant Bits. (2002). *The Economist Technology Quarterly. 364*(8291), 8.

[Her05] Herrnson, Paul S., Benjamin B. Bederson, Bongshin Lee, Peter L. Francia, Robert M. Sherman, Frederick G. Conrad, Michael Traugott, and Richard G. Niemi. (2005). Early Appraisals of Electronic Voting. *Social Science Computer Review. 23*(3), 274-292.

[Her06] Herrnson, Paul S., Benjamin B. Bederson, Charles D. Hadley, Richard G. Niemi, Michael J. Hanmer (with staff assistance). 2006. The Usability of Four Vote Verification Systems: A Study Conducted for the Maryland State Board of Elections. College Park: Center for American Citizenship and Politics, University of Maryland College Park. Accessed 6/2/06. Available online at www.elections.state.md.us/citizens/voting_systems/MarylandReport2-15-06.pdf

[Hol05] Voter Confidence and Increased Accessibility Act (HR 2239 in the 108th Congress, HR 550 in the 109th Congress).

[Kur04] Kurlantzick, Joshua. (2004). 2000, the sequel: in theory, the Help America Vote Act was Congress' attempt to prevent the catastrophes of the last election from happening again; in fact, it may have made things even worse. *American Prospect.* 15 (10), 22-5.

[Lam82] Lamport, L., R. Shostak, and M. Pease. (1982). The Byzantine generals problem. *ACM Transactions on Programming, Languages, and Systems.* 4 (3): 382–401.

[Los04] Los Angeles County, CA Register/Recorder. 2004. DVD of Video of Voting on VVPAT in Las Vegas, NV, 2004 General Election.

[Mac04] Machlis, Sharon. (2004). Public, Security Experts' E-Voting Views Differ Sharply: Experts Worry More about Errors in E-Voting than Does the Public. *Computerworld. 2004* (August 6), unknown. Retrieved from www.computerworld.com/printthis/2004/0,4814,95094,00.html on 11/2/2005.

[Mar06] Maryland State Board of Elections. 2006. Description of roles of the SBE and the Local Boards of Elections. Email communication, January, 2006.

[Nef04] Neff, Andrew C., Practical high certainty intent verification for encrypted votes, technical document (October 14, 2004), unpublished manuscript, 24 pages.

[Nor06a] Donald F. Norris, PI, Andrew Sears, and Charles Nicholas, CoPIs. Anne V. Roland, Ed. Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, John Pinkston, Andrew Sears, Alan T. Sherman, and Dongsong Zhang (2006). A Study of Vote Verification Technologies. Part I: Technical Study, Prepared for the Maryland State Board of Elections, February 2006. 68 pages. Accessed 3/28/06. Available online at http://www.umbc.edu/mipar/

[Nor06b] Donald F. Norris, PI, Andrew Sears, and Charles Nicholas, CoPIs. Anne V. Roland, Ed. Aryya Gangopadhyay, Stephen H. Holden, George Karabatis, A. Gunes Koru, Chris M. Law, John Pinkston, Andrew Sears, Alan T. Sherman, and Dongsong Zhang (2006). A Study of Vote Verification Technologies. Part I: Technical Study Appendices, Prepared for the Maryland State Board of Elections, February 2006. 75 pages. Accessed 3/28/06. Available online at http://www.umbc.edu/mipar/documents/VoteVerificationAppendiceswebversion.pdf

[Nor06c] Norris, Donald F (2006). Maryland registered voters' opinions about voting and voting technology. Prepared for the Maryland State Board of Elections, February 2006. 31 pages. Accessed 3/28/06. Available online at http://www.umbc.edu/mipar/documents/VoterOpinionsReport-FINAL_000.pdf

[Pyn05] Pynchon, Susan. (2005). Diebold touch screens don't meet disability requirements (FL). *News-journalonline.com*, June 28 2005. Accessed 9/8/2005 Available online at: http://www.verifiedvotingfoundation.org/article.php?id=6072

[Reh73] Section 508 of the Rehabilitation Act of 1973, as amended in 1998, for procurement of electronic and information technology (Authority: 29 U.S.C. §794d.). Available online at www.section508.gov

[Rub05] Rubin, Aviel D., Dan S. Wallach, Dan Boneh, Michael D. Byrne, Drew Dean, David L. Dill, Douglas W. Jones, Peter G. Neumann, Deidre Mulligan and David A. Wagner. (2005). *A Center for Correct, Usable, Reliable, and Transparent Elections (ACCURATE)*: *A Research Proposal for an NSF CyberTrust Center.*

[Sel04] Selker, Ted. (2004). Fixing the Vote. *Scientific American, 291*, 90-97.

[Sel05] Selker, Ted. (2005). A Day of Poll Watching Reno/Sparks Nevada, *User Experience Magazine,* spring 2005.

[Wan04] Wang, Tova Andrea. (2004). *Understanding the Debate over Electronic Voting Machines.* New York: The Century Foundation.