October 3, 2006

Voter Verified Paper Ballots: Seat belts for Election Safety

Verified Voting's Testimony for the Committee on House Administration's hearings on Electronic voting machines: verification, security, and paper records

ABSTRACT

Secure, reliable, usable, accessible , and verifiable voting systems are critical to ensure accurate, transparent, fair, and inclusive elections. A number of states and local jurisdictions have deployed systems that meet all of these goals, but others have had substantial problems, particularly with Direct Recording Electronic (DRE) touchscreen systems. There is overwhelming evidence that currently-deployed DRE voting systems suffer from security vulnerabilities, reliability problems, and usability issues that put the integrity of our elections at risk and erode public confidence in election results. Procedural solutions that only address the physical security of voting machines are inadequate to protect against these risks.

As the experience of many states and local jurisdictions has demonstrated, the only effective voting solution available today is a system of voter-verified paper ballots (such as precinct-based optical scan voting systems combined with accessible ballot marking devices), that are used to conduct compulsory manual audits of electronic tabulations. Some touchscreen systems that produce individual ballots as well as accessibility for voters who are disabled or do not speak English have proven to be useful supplements to optical scan systems, but poorly-designed and crudely-built voter-verifiable paper audit trail (VVPAT) DRE printers that are unreliable have put requirements for voter-verified paper audit trails into question.

As a result of failures in paperless DRE voting technology, significant numbers of eligible voters have already been denied their right to vote, e.g., because they were turned away from their polling place because of inoperative voting machines. Failures in VVPAT technology have meant such machines failed to properly record votes that were correctly cast. As a result, some election results have been compromised due to such failures of DRE technology -- failures that could have been prevented had computer scientists' earlier warnings been heeded.

In light of the very serious security, reliability, usability, and verifiability problems with recently-deployed, HAVA-mandated voting systems that have become apparent during subsequent elections in a number of States, it is time for Congress to revisit HAVA and enact legislation to ensure that all voting systems enable eligible voters to cast their votes and have those votes counted in a manner that is secure, accurate, verifiable, accessible, and reliable. Any updates to HAVA must also ensure end-to-end transparency so that all aspects of the voting process are open to and observable by the public, from the testing and certification of machines through the final tabulation and canvass of the ballots. Voter confidence in our electoral process will only be restored if citizens are able to monitor and verify the process by which election results are reached.

Durable paper ballot records are like seat belts. We need to use them to prevent serious injuries to our democratic system when inevitable and sometimes serious incidents occur. Just as some early

seatbelt technology was awkward to use, the answer is not to throw out seat belt requirements, but rather to improve seat belt technology and legislation.

Most Voting Experts and Advocates Share Many Goals In Common

Although different voting experts, advocacy groups, and public officials differ on what voting equipment can best meet the our needs for accurate, reliable, secure, accessible, and transparent elections in the United States, most of us share a number of fundamental goals, including:

- *accuracy:* voting equipment should faithfully record and preserve the voting intentions of individual voters and minimize the numbers of votes lost;
- *verifiability*: all voters must have the opportunity to verify that their votes have been recorded correctly;
- *fairness:* voting equipment and procedures must not favor any particular candidate, party, or group nor exclude any eligible voters from casting a ballot;
- *reliability:* voting equipment and procedures must be sufficiently robust that breakdowns are rare, maintenance and upgrades relatively easy, and failures do not result in keeping voters from voting;
- *usability:* voting equipment must be easy for poll workers to set up and operate and for voters to use -- even poll workers and voters who are not experienced with computers;
- *accessibility:* voters should be able to vote independently and in private
- *trustworthiness:* voting equipment and procedures must be sufficiently transparent that both experts and the general public can have verifiable confidence that each stage of the election process has minimized the possibilities of fraud and error.

These are not mutually exclusive goals; they can be achieved through careful selection of voting technologies.

It has repeatedly been said that the States are the laboratories of our democracy. The last four years (i.e., from the enactment of the Help America Vote Act to the present) represent a national experiment in which thousands of jurisdictions have evaluated which voting technology will best achieve these goals. Now that most jurisdictions have completed that process, it is instructive to review the results from those "laboratories".

A Clear Majority: Optical Scan Paper Ballots

As a recent report from Election Data Services (EDS 2 Oct 2006) documents, many states and local jurisdictions have adopted new voting technology in the past four years since HAVA made federal funding available for that purpose. Lever, punch card, and paper-only systems have been almost completely replaced by optical scan and direct recording electronic (DRE) touchscreen equipment.

From November 2000 to November 2006, the EDS study estimates that the number of counties using Optical Scan equipment increased from 1,279 to 1,752 (41% to 56%), and the number of counties primarily using DRE technology) increased from 309 to 1,142 (10% to 37%). In terms of estimated registered voters, 84 million (49%) are in jurisdictions that will use optical scan technology and nearly 66 million (38%) are in jurisdictions that will use DREs in the November 2006 elections. (for the full report, see http://www.edssurvey.com/files/NR_VoteEquip_Nov-2006wTables.pdf)

Thus, a clear majority of jurisdictions have chosen to deploy optical scan paper ballot systems, and some states[1] have successfully used this technology for over 20 years. In addition, some states (e.g., Alabama, New Mexico and Michigan[2]) which had previously deployed DRE voting machines in some counties decided to retire those machines and convert to a precinct-count optical scan (PCOS) voting system statewide. And Connecticut, which had previously planned to replace its lever machines entirely with DREs has abandoned that plan and instead will deploy PCOS technology statewide.

These jurisdictions have realized that PCOS technology offers many advantages over DREs, including:

1. All voters use the same ballot, regardless of whether they vote absentee or in-precinct.
2. PCOS is scalable: only one scanner is needed per precinct regardless of number of voters, so long lines are rare.
3. Optical scan is a mature technology used reliably for over 20 years.
4. Optical scan paper ballots are inherently voter-verifiable and don't require VVPAT printers.
5. In the case of recounts or manual audits, optical scan paper ballots are much easier to hand-count than continuous-roll paper tapes printed by VVPAT printers attached to DREs.

A Clear Majority: Voter-Verified Paper Record[3] Requirements

There is widespread popular support for voter-verifiable paper ballots as the simplest, easiest, and most cost-effective way to maintain and improve the quality of our elections. To date, 28 states[4] have passed voter-verified paper record requirements, and another eight states[5] are deploying voter-verifiable equipment statewide, through their recent HAVA purchases. Thus 36 states (over 70%) have concluded that systems providing voter-verifiable paper records are necessary for trustworthy elections.

In addition, VVPR legislation has been introduced in several other states[6], and the legislatures of several pivotal states have come very close to enacting VVPR requirements recently.[7] That those bills have not yet passed has more to do with fiscal concerns or political maneuverings of a few powerful committee chairs.

Thirteen states have already explicitly required mandatory audits of the voter-verified paper records.[8]

---

[1] http://www.tulsaworld.com/OpinionStory.asp?ID=061001_Op_G6_Simpl24546
[2] http://www.michigan.gov/documents/Uniform_Voting_System_2_71047_7.pdf 2003
[3] It is important to note that voter-verified paper records (VVPR) are not limited to voter-verified paper audit trails (VVPAT) attached to direct recording electronic (DRE) voting machines. The broader term includes paper ballot-based systems such as the precinct-count optical scan used in more jurisdictions nationwide than any other system. Paper ballots, marked by the voter, are inherently voter-verified.
[4] Before 2000, NH and SD had statutes requiring paper ballots. IL, MI and NV passed voter-verified paper record requirements before the end of 2003. In 2004, AK, CA, ME, MO and OH added requirements, and NV became the first state to fully implement VVPAT with DREs. Details at:http://verifiedvoting.org/article.php?list=type&type=13#state.
[5] AL, MA, MS, ND, NE, OK, RI, WY
[6] Twelve states and the District of Columbia have introduced and/or are currently considering a VVPR requirement.
[7] E.g. Maryland, where this year such legislation passed unanimously in one chamber but was denied a meaningful hearing in the other, despite urging by the Governor; Iowa, where the bill passed unanimously in one chamber but was attached to un-passable language in the other; Tennessee, where a legislative study committee is set to review the matter; Virginia, where strong bi-partisan bills were tabled due to budget issues, but not rejected.
[8] http://verifiedvoting.org/downloads/ManualAudits-06-06.pdf

Several bills[9] in the U.S. House of Representatives would require voter-verified paper records (VVPR), of which H.R. 550 is the clear leader with 219 bi-partisan co-sponsors; it also provides the most comprehensive and effective solution. A majority of Members of the U.S. House of Representatives are on record as supporting this bill, while an even larger majority are on record as supporting legislation to enact a VVPR requirement for all voting systems used in federal elections.

Earlier this year, the US League of Women Voters passed a resolution in support of the use of voter-verifiable paper ballots/records for routine audits, and decrying the lack of a recountable audit trail in "paperless" electronic voting systems.[10] It is time for legislators and elections officials to discard the discredited assertion that non-voter-verifiable records (be they invisible electronic records or paper reprints of those records) are acceptable for audits of vote tallies from electronic voting systems.

DREs Without Independent Verification Are Inherently Insecure

Many flaws in the security design of DREs have been discovered over the last three years, as described below. However, these serious problems are all described in the context of *external* attacks, by people who do not have legitimate access to the voting machine internals.

It is crucial to note that there are many people with *legitimate* access to voting machine internals, who are capable of perpetrating "insider attacks," and that current technology allows no direct way to prevent or even detect such attacks by certifying the system design or software. ***The only feasible solution is to have an independent way of checking the results recorded by the machine.***

The only acceptable solution that is currently available and certified is a paper record of the vote that the voter can verify for correctness before the vote is cast. This enables an independent check, since the paper records can be manually counted and compared with the electronic results. If there is an error on the paper record, the voter can see it and report and correct it. If there is an error in the electronic record, it can be caught because it will disagree with the paper record.

There are a variety of other proposed methods for independent verification, including end-to-end cryptographic systems, audio-tape copies of the ballots, and photographs of computer screens. Most of these schemes are not currently available and certified. Those that are certified are too complex for voters and poll workers to understand, or have other gross deficiencies.

The possible existence of paperless independent verification in the future is neither a rationale nor an excuse for purchasing or using totally insecure and untrustworthy paperless technology now.

DRE Security Problems Have Been Documented Extensively

In contrast to optical scan technology, paperless DRE technology suffers from a number of severe problems, including security, usability, reliability, and trustworthiness. Over the past 3 years, a number of in-depth studies of voting system security have been published, and each one has

[9] http://www.verifiedvoting.org/legis
[10] http://www.verifiedvotingfoundation.org/article.php?id=6363

identified extremely serious security vulnerabilities involving paperless[11] electronic voting systems -- vulnerabilities that pose grave risks for our electoral system. These studies include:

1. "Analysis of an Electronic Voting System", Tadayoshi Kohno, Adam Stubblefield, and Avi Rubin, Johns Hopkins University and Dan Wallach, Rice University, July 2003.[12]
2. "Risk Assessment Report Diebold AccuVote-TS Voting System and Processes ", Science Applications International Corporation, September 2003. (An official report commissioned by the State of Maryland).[13]
3. "Direct Recording Electronic (DRE) Technical Security Assessment Report", Compuware Corporation, November 2003 (An official report commissioned by Ohio's Secretary of State)[14]
4. "Trusted Agent Report Diebold AccuVote-TS Voting System", RABA Innovative Solution Cell (RiSC), Dr. Michael A. Wertheimer[15] Director, January 2004. (An official report commissioned by the State of Maryland).[16]
5. "Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed" (GAO-05-956)", GAO, October 2005.[17]
6. "Security Analysis of the Diebold AccuBasic Interpreter ", Dr. David Wagner, Dr. David Jefferson, Dr. Matt Bishop, California State Voting Systems Technology Assessment Advisory Board, February 2006. (An official report commissioned by the Secretary of State of California).[18]
7. "Diebold TSx Evaluation: Critical Security Issues with Diebold TSx", Dr. Harri Hursti, Black Box Voting, May 2006. [19]
8. "The Machinery of Democracy: Protecting Elections in an Electronic World", Lawrence Norden, et al.; Report of the Brennan Center's Task Force on Voting System Security, June 2006[20]
9. "Security Analysis of the Diebold AccuVote-TS Voting Machine", Ariel J. Feldman, J. Alex Halderman, and Dr. Edward W. Felten, Center for Information Technology Policy and Dept. of Computer Science, Princeton University, September 2006. [21]

Many of these reports, especially those published this year, address critical security concerns related to the use of removable memory cards in electronic voting machines. (While problems with these cards are not the only security problems identified in these reports, they are among the most serious.) These memory cards are routinely used to transfer information from one machine to another, much like floppy disks were used in the first generation of personal computers. Examples

---

[11] By "paperless electronic voting systems", we refer to those systems that do not produce a voter-verifiable paper ballot (VVPB) , hence systems that are "paper-less". While we acknowledge many existing DRE systems contain an internal printer used to print paper "zero tapes" prior to the opening of the polls and "summary tapes" once the polls are closed, we still refer to such machines as "paperless" unless such machines are also equipped with a printer that produces a VVPR. We use the term "paperless" rather than "VVPR-less" because it is more readable.

[12] https://www.eff.org/Activism/ E-voting/20030724_evote_research_report.pdf

[13] http://www.verifiedvoting.org/downloads/votingsystemreportfinal.pdf

[14] http://www.sos.state.oh.us/sos/hava/compuware112103.pdf

[15] Dr. Wertheimer now serves as the Assistant Deputy Director and Chief Technology Officer in the Office of the Deputy Director of National Intelligence: http://www.dni.gov/press_releases/20051031_release.htm,

[16] http://www.raba.com/press/TA_Report_AccuVote.pdf#search="raba report diebold".

[17] http://www.verifiedvoting.org/article.php?id=5826

[18] http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf

[19] http://www.blackboxvoting.org/BBVtsxstudy.pdf

[20] http://www.brennancenter.org/programs/downloads/Full%20Report.pdf

[21] http://itpolicy.princeton.edu/voting/ts-paper.pdf

of such usage include the authorized installation of certified software updates, the downloading of ballot formats for an upcoming election, or the uploading the votes cast by voters in an election that has just ended. Some of these operations are performed by poll workers, some by election officials, and others by technicians employed by the voting system vendor, presumably under the supervision of election officials.

In all of the recent reports , various modes of attack are described by which an adversary who obtains unauthorized access to a removable memory card located in an electronic voting machine can corrupt the vote tallies and voting records produced by that machine. The first few of these reports focused on the potential for such unauthorized access to occur either while a voting machine was at, or in transit to or from, the polling place for an election.

Vote-Stealing Code Can Be Spread By Virus-Infected Memory Cards

The seriousness of DRE security vulnerability was recently documented in a September 2006 publication of the security vulnerability study by the team of researchers at Princeton University led by Prof. Edward Felten. That study revealed (and demonstrated) a previously unexplored vulnerability posed by such removable memory cards: their ability to transmit a computer virus that spreads between voting machines and memory cards whenever the latter is plugged into the former. In this manner, a single infected card could introduce such a virus into a population of voting machines, many weeks or even months before an election. Over time, as unsuspecting elections officials moved memory cards between voting machines in the course of routine election activities (e.g., downloading ballot formats or uploading votes) , they could unknowingly spread the virus to more machines. As the Princeton team demonstrated, that virus could be used to introduce vote-stealing software onto all such infected machines.

This discovery by the Princeton team invalidates an oft-repeated assertion by voting system vendors and other proponents of paperless electronic voting machines: that such machines are immune to computer viruses because they are never connected to the Internet. Just as humans can be infected with viruses in multiple ways, so can computers -- and voting machines. Long before the Internet existed, computer viruses spread between early PC's via floppy disks moved from one machine to another, just as the removable memory cards are now moved between voting machines.

Thus, even if, for the sake of argument, one assumes that effective mitigation procedures can be implemented in practice to prevent (or at least detect) any tampering with the removable memory card in a voting machine while it is at (or in transit to or from) the polling place, that does not ensure that that memory card or voting machine was not already infected, long before it was configured and secured (i.e., tamper-evident tape applied) in preparation for shipment to the polling place. Even more insidious is the fact that the memory card and/or machine might have been unknowing infected by an honest election official or poll worker in the course of routine and fully-authorized election-related activities performed by those individuals. Once a machine is infected, that infection can only be detected or disinfected by means of a very labor-intensive process conducted by a relatively-skilled technician.

While the expert who identified the specific vulnerabilities described in the Princeton study was given access to that system to examine it (and justifiably so, given earlier revelations about poor security design in these systems), we have no way of knowing if or how many other persons with sufficient access (and ill intent) may have quietly uncovered these vulnerabilities earlier.

Currently, tens of thousands of such vulnerable machines are deployed nationwide, and many of them have been deployed since 2002, i.e., fully four years before the publication of the Princeton study and the concerns it has now raised about the risk of such infections. Thus, many of those machines were in circulation long before the mitigation procedures were issued by several states earlier this year. Accordingly, some of those machines may have been infected prior to the application of these mitigation procedures. Putting such mitigation procedures into effect at this late date may be about as effective a means of preventing infection as first starting to apply mosquito repellent several years after moving to a malaria-ridden region.

It is currently unknown what fraction of vulnerable DRE machines and memory cards may already be infected with viruses of the type demonstrated in the Princeton study, and answering that question would require a costly and time-consuming forensic examination of *all* such machines and memory cards currently in circulation, as well as disinfection of any machines or cards found to be infected. And unless such disinfection is complete across all machines in a jurisdiction (or until such DREs are re-engineered to provide immunity to such viruses), disinfected cards or machines could become re-infected if exposed to any card or machine that was still infected.

Unfortunately, most states have not ordered such examinations of their deployed DRE machines, either because they lack the resources to do so or they optimistically assume that no such infections have yet occurred. Based on the extensive spread of viruses throughout other forms of electronic technology (e.g., personal computers, cell phones, and even ATM machines[22]), it seems both risky and naive to assume that no such viruses are already circulating among DRE voting machines whose inherent design places that at very high risk to such viruses.

This problem cannot be solved in any practical sense by the application of tamper-evident tape or by applying, at this late date, strict chain of custody procedures for machines and memory cards which may already be infected. The only viable solution today is employ a system of voter-verified paper records that are checked via compulsory manual audits of those records.

Physical Chain of Custody Is Not Sufficient

In response to the alarm raised by those reports, a number of states (e.g., Ohio[23] and Florida[24]) issued advisory warnings recommending that local jurisdictions employ specific mitigation measures, including stricter procedures for monitoring the chain of custody for such voting systems as well as the use of serially-numbered tamper-evident tape to seal the access doors that cover the slots into which the removable memory cards are inserted. Some states, such as California, took stronger action, temporarily suspending or delaying certification of such voting systems and then certifying[25] those systems conditional on the strict application of such mitigation measures. Assuming that such measures could be counted on to prevent any unauthorized access to these vulnerable removable memory cards from occurring or going undetected, state election officials argued that these measures would be sufficient to eliminate the risks associated with these use of these cards.

---

[22] "Nachi worm infected Diebold ATMs", http://www.theregister.co.uk/2003/11/25/nachi_worm_infected_diebold_atms/

[23] http://www.sos.state.oh.us:80/sos/electionsvoter/advisories/2006/Adv2006-03.pdf

[24] http://election.dos.state.fl.us/pdf/memorandum.pdf

[25] http://www.ss.ca.gov/elections/voting_systems/cert_doc.pdf

Unfortunately, while such mitigation measures seem like they should be effective in theory, strict enforcement of such measures has so far proven to be very difficult for poll workers and elections officials to carry out in an actual election environment. For example, during recent elections (e.g., California's June 2006 primary election or Maryland's September 2006 primary) in jurisdictions where such mitigation measures were required (e.g., San Diego County, CA or Baltimore County, MD), the actual effectiveness of such measures has been questionable at best. Poll workers in those jurisdictions have reported numerous problems with the tamper-evident tape, including:

1. difficulty in determining when a tape has been tampered with, because the resulting change is appearance is hard to discern visually[26]
2. having inadequate training to know whether a legitimate piece of tape has been removed and replaced by a counterfeit piece.[27]

In addition, California's statewide requirement for maintaining a strict chain of custody for such electronic voting system conflicts with San Diego County's longstanding practice of sending such voting systems home with poll workers in the days or weeks preceding the election. As a result, such machines were left unattended and unsupervised for lengthy periods of time in poll workers' homes, garages, vehicles, or other potentially-insecure locations. Consequently, the state-imposed "chain of custody" requirement that was part of these mitigation measures was not strictly enforced, despite the fact that the State's certification of the voting system used in that county were conditional on the strict enforcement of that requirement.

Thus, these sorts of mitigation measures that only address the physical security of voting machines(either while they are located at the polling place or are in transit to or from that location) are difficult to implement in practice, given the performance of the tamper-evident tape currently in use, the skill and training level of poll workers, and the currently-funded methods for distributing massive numbers (e.g., 10,000) of voting machines to large numbers (e.g., 1,500) of polling places in counties such as San Diego, California. Accordingly, such mitigation measures are inadequate to address the previously-documented security risks associated with the use of these removable memory cards.

Although we entrust election procedures to our dedicated election officials and poll workers, we must ensure that the integrity of our elections never hinge on protocols so complex that they exceed their skills and training. And we must ensure that any mitigation procedures (implemented to address security vulnerabilities in voting systems) are not so fragile and intricate that they won't be strictly applied and enforced.

Certification Procedures Are Woefully Inadequate

It is important to be absolutely clear: the insecure paperless voting systems described here made it all the way through the existing federal certification process, despite the fact that these security vulnerabilities that were first mentioned in January 2004,[28] and recently expanded upon.[29] No certification system, even improved over today's systems, can catch all such vulnerabilities.

---

[26] http://avi-rubin.blogspot.com/2006/09/my-day-at-polls-maryland-primary-06.html
[27] http://cha.house.gov/hearings/Testimony.aspx?TID=1324
[28] http://www.raba.com/press/TA_Report_AccuVote.pdf
[29] http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf (California Secretary of State); and www.blackboxvoting.org

Nor will a certification system catch ballot programming errors, since such programming is unique for each election and thus does not go through the certification process. Ballot programming errors (not uncommon, and generally representing honest mistakes rather than sinister plots) pose a very significant risk to the accuracy and verifiability of elections conducted on paperless DREs. Tighter certification systems will do nothing to protect against such risks.

Paperless DRE Systems Are Neither Trustworthy Nor Fail-Safe

Simply put, existing paperless DREs cannot be made trustworthy. No paper trail printed post-election, without the benefit of voters confirming that the document represents their intent, can change that. Neither can the application of tamper-evident security tape. The suggestion that a reprint of unverifiable electronic ballot images, never reviewed nor confirmed accurate by the voters, can be used to conduct a meaningful audit has been soundly and repeatedly discredited.

Existing paperless DREs represent a *system* problem that cannot be resolved by *procedures*. Established organizations such as the Brennan Center have concluded that paperless DREs are *not* trustworthy[30], and the addition of VVPAT, audited to check machine tallies for accuracy, is the only way to *make* such systems trustworthy[31]. One must change the system itself: deploy an independent paper record of voter intent, confirmed by the voter, to use as the audit document and the true record of the vote.

Another critical function of voter-verified paper records, apart from security is that they provide a vital seat belt in case of accidents and other emergencies. VVPRs resolve the problems that occur when machine malfunctions result in lost electronic vote information.

A voter-verified paper record printer, for example, would have resolved the problem in Carteret County, NC in 2004 when 4400+ votes were irretrievably lost, affecting the outcome of a statewide race in which the margin was less than 2000.[32] After that unfortunate (and costly) event, NC passed a voter-verified paper record law. Each election, new examples arise – either of situations where votes were irretrievably lost, but could have been recovered if a VVPR requirement were in place, or of problems discovered and resolved because VVPR systems were in place.

A problem encountered with the scanner component of a paper ballot system need not result in lost votes. If the marked ballots are correctly managed, retained and recounted, votes can still be counted in a number of different ways. But a DRE which fails may lose these votes forever.

---

[30] U.S. GAO (see: http://www.verifiedvoting.org/article.php?id=5826), Johns Hopkins Institute, Raba Trusted Agent Report for MD's legislature and the Brennan Center's Task Force on Voting System Security: http://www.brennancenter.org/programs/downloads/Full%20Report.pdf

[31] Carter-Baker Commission (see http://www.verifiedvoting.org/article.php?id=5824), CA Voting Systems Technology Advisory Board, League of Women Voters (June 2006)

[32] http://www.wral.com/news/3891488/detail.html

[35] Testimony to the EAC from a Nevada election official regarding their initial implementation of VVPAT printers somewhat contradicts these concerns for one vendor's design; he said it was relatively simple, in the particular system they used, to change the printer cartridges and it could be done during the voting day with minimal interruption.

DREs Require More Extensive Secure Ballot Boxes

A fundamental distinction between DREs and paper-based systems that is often overlooked involves both the transparency and number of ballot boxes associated with each type of system. And this distinction has a profound effect on the level, complexity, and effectiveness of the procedures that elections officials and poll workers must employ to ensure the security of the ballot boxes.

In any voting system where ballots of record are paper (such as PCOS), each precinct has one (and only one) ballot box that is typically some sort of locked receptacle into which the optical scanner deposits the paper ballots after scanning them (or into which voters directly deposit their ballots in the case of a central-count optical scan or hand-counted paper ballot system). Security requirements for such ballot boxes are relatively simple. Prior to election day, the empty ballot box for each precinct requires no special security precautions because it not only contains nothing of value, it contains nothing at all.

On the morning of election day, at the opening of the polls, there is a simple and publicly-visible and verifiable process by which poll workers, along with the first voter of the day, can confirm that the ballot box really is empty: they can open the lid, look inside, feel the inside with their hands, or perform whatever other reasonable means of physical inspection they care to employ to verify that that ballot box really is empty. Once so verified, the lid is closed and locked in place, and the first voter of the day permitted to deposit his or her ballot. From that point on, until that ballot box is transported to the tabulation facility and unlocked, that ballot box is under the watchful eye of the all of the poll workers and observers at that polling place or at the tabulation facility. Once the canvass is completed, the ballot box is unlocked, emptied, and no longer requires that it be securely stored or access to it controlled and logged. Thus, each precinct requires only one such ballot box, and the security of that ballot box need only be monitored from the morning of election day until the completion of the canvass for that election.

In a DRE-based system, each precinct has at least as many ballot boxes as it has DREs, since the removable memory card in each machine each constitutes a separate, electronic ballot box. (In addition, each DRE has one or more redundant internal memories, each of which constitutes a "backup" electronic ballot box.) If the DREs and removable memory cards are always transported to and from the polling place as a sealed unit, then the number of distinct items for which "chain of custody logs" must be maintained is simply the number of DREs, whereas if they are transported in separate packages an even larger of items needs to be logged and tracked.

In addition, the security requirements for these electronic ballot boxes (both the removable memory cards and the DRE machines with their redundant internal memories) are much more extensive than those for the ballot boxes used for paper ballots. Each electronic ballot box must be subject to strict security protocols and chain of custody procedures at all times, even between elections. Otherwise, if there is a lapse in such procedures and a malicious individual obtains even brief access to either a removable memory card or a DRE machine, the potential for infection exists. Once such an infected memory card or machine enters the equipment pool in a given jurisdiction, elections and poll workers can unknowingly spread that virus as cards are moved between machines during routine operations that occur either during or in-between elections.

Unlike simple locked boxes that are used as ballot boxes for paper-based voting systems, poll workers and polling place observers have no direct method for verifying that any of the electronic

ballot boxes deployed at a given precinct are indeed empty (or uninfected) on the morning of election day. The only method they have is to ask the DRE to print out a "zero tape"; in other words, the poll workers and observers can't verify for themselves that the electronic box is empty, they have to ask the DRE and take its word. As Dr. Felten's demonstration illustrates in such a compelling way, if the DRE or its memory card is infected with a virus carrying a vote-stealing payload, then the "zero tape" printed by the DRE has little meaning. Further, some systems' software allows for the retroactive printing of a "zero tape" – well after voters have begun casting votes on the device – rendering it essentially meaningless.

In summary, systems which have a paper ballot of record impose a considerably lower security burden on elections officials and poll workers, because only one ballot box is needed per precinct, and it only needs to be secured from the start of the election until the end of the canvass for that election. In addition, it provides poll workers a direct and transparent means of verifying that the ballot box is empty at the start of the election. In contrast, a DRE system imposes a much higher security burden, because multiple (electronic) ballot boxes are needed per precinct and those need to be secured at all times. Furthermore, those electronic ballot boxes are opaque and poll workers have no direct means of verifying at the start of the election that they are either empty or uninfected.

Thermal Paper Rolls Are Not Adequate For VVPR

While many of the security and verifiability problems with DREs can be addressed by the addition of voter-verifiable paper record (also referred to as voter-verified paper audit trail, or VVPAT) printers, to date, the reliability and overall performance of such printers has been mixed. While elections officials from Nevada (the first state to deploy VVPAT printers) have testified to the EAC that such printers have performed well since their introduction in 2004, other jurisdictions, such as Cuyahoga County, Ohio, reported significant problems with their VVPAT printers during the primary elections of 2006. Accordingly, significantly better designs and operational procedures for such printers must be developed to address the serious reliability concerns that were raised in Cuyahoga County. In addition, printers that fail to perform reliably once deployed should have their certification suspended until such reliability problems are resolved.

In addition, VVPAT printers that print onto rolls of thermal paper present additional problems. First, they potentially compromise ballot secrecy, because votes are recorded onto the paper roll in the same order in which ballots are cast. Someone keeping track of the order in which specific voters cast their votes on particular machines could then deduce from such paper rolls how those voters had cast their votes. Second, in the case of a recount or manual audit, it is cumbersome and time-consuming for election officials to hand count votes recorded on such rolls of paper, especially given that such paper may be relatively thin and can potentially be damaged during the handling that would occur during such recounts or audits.

For all these reasons, such thermal roll paper VVPAT printers represent a poor method for enabling DRE voting machines to produce a voter-verified paper record. However, such printers represent just one possible method for providing a VVPR. Rather than fail to implement VVPR requirements because some of these types of printers were badly designed and have performed poorly, the proper solution is to either

improve the design of such printers or switch to a different technology for producing the VVPR.

It is instructive to compare the development of VVPAT printers to the evolution of seat belts in cars. Automobile vendors initially fought the requirement for seat belts: "they won't be effective, they will cost too much, most people won't use them," etc. The first generation of seat belts were not so effective, not comfortable to wear, and most people didn't use them. However, the public and the government rejected arguments that requirements for seat belts were a bad idea, or that the push for seat belts should be abandoned because of poor initial implementation. Requirements expanded, and vendors produced more effective and more comfortable seat belts. Information campaigns target those who forget to buckle up.

VVPAT/VVPR requirements are the seat belts for already-deployed voting systems, a necessary protection to ensure those systems are secure, accurate, reliable, and auditable. Some vendors have been resistant to put significant effort into this technology, and some first generation VVPAT systems may not be well-designed, reliable, or user friendly. It is no surprise that some election officials may find such systems difficult to deploy or that some voters may not verify the printouts from VVPAT printers.[35] Improved standards and public pressure will compel vendors to do a better job of implementation. And just as information that seat belts save lives caused many more drivers to actually use them, improved education about the crucial nature of the independent paper record will increase the public's scrutiny.

RECOMMENDATIONS

1. In order to address extremely serious voting system security vulnerabilities, a voter-verifiable paper record must be produced by all voting systems to enable voters to verify that their votes have been recorded properly.

2. Mandatory manual audits of the voter-verifiable paper records from a sample of precincts selected at random must be used to check the electronic tallies produced by voting systems. Without such audits, the VVPRs alone provide insufficient benefit.

3. Jurisdictions using DRE voting systems must implement a reliable means of providing VVPR, either by attaching *reliable* VVPAT printers to their DREs or by phasing out their DRE systems and converting to precinct-count optical scan systems (as Michigan did) augmented with accessible electronic ballot marking devices to ensure accessibility.

4. Any DRE+VVPAT system must have safety measures to maintain the consistency of the paper and electronic records, such as refusing to accept more electronic votes when the printer is not functioning properly.

5. In order to be certified for use, VVPAT printers must be highly reliable when set up and administered by average poll workers with average training