Annotated Bibliography of Expert Reports on Voting Systems

Edited by Rady Ananda
December 11, 2007

REPORTS ANNOTATED:

Compuware Corp. DRE Technical Security Assessment Report for Ohio, November 2003. Accessed December 11, 2007. http://www.sos.state.oh.us/sos/hava/compuware112103.pdf

Epstein, Jeremy. Improving Kentucky's Electronic Voting System Certifications. Letter to Kentucky Attorney General Greg Stumbo. September 28, 2007. Accessed December 11, 2007. http://ag.ky.gov/NR/rdonlyres/1B3F7428-0728-4E83-AADB-51343C13FA29/0/votingexpertletter.pdf

Feldman, Ariel J., J. Alex Halderman, and Edward W. Felten. Security Analysis of the Diebold AccuVote-TS Voting Machine, Center for Information Technology Policy and Dept. of Computer Science, Woodrow Wilson School of Public and International Affairs, Princeton University, 2006. Accessed December 11, 2007. http://itpolicy.princeton.edu/voting/ts-paper.pdf

Fischer, Eric A. Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues, Congressional Research Service CRS Report for Congress, November 4, 2003. Accessed December 11, 2007. http://theory.lcs.mit.edu/~rivest/voting/reports/Fischer-ElectionReformAndElectronicVotingSystemsDREs.pdf

Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Waalega, Evan Hollander, and Michael Gerke. Review and Security Analysis of the Diebold Voting Machine Software, Security and Assurance in Information Technology Laboratory Florida State University, July 27, 2007. Accessed December 11, 2007. http://election.dos.state.fl.us/pdf/SAITreport.pdf

Gainey, David, Michael Gerke, and Alec Yasinsac. Software Review and Security Analysis of the Diebold Voting Machine Software Supplemental Report, Security and Assurance in Information Technology Laboratory Florida State University, August 10, 2007. Accessed December 11, 2007.
http://election.dos.state.fl.us/pdf/DieboldSupplementalReportFinalSubmission.pdf

Gonggrijp, Rop, and Willem-Jan Hengeveld. Studying the Nedap/Groenendaal ES3B Voting Computer: A Computer Security Perspective. Presented August 6, 2007 at the USENIX/ACCURATE Electronic Voting Technology Workshop, Boston, USA. Accessed December 11, 2007.
http://www.wijvertrouwenstemcomputersniet.nl/images/c/ce/ES3B_EVT07.pdf

Goodwin-Gill, Guy S. Free & Fair Elections. International Parliamentary Union, 2006. Accessed December 11, 2007. http://www.ipu.org/PDF/publications/Free&Fair06-e.pdf

Hertzberg, Steven. DRE Analysis for May 2006 Primary Cuyahoga County, Ohio, Election Science Institute, August 2006. Accessed December 11, 2007. http://bocc.cuyahogacounty.us/GSC/pdf/esi_cuyahoga_final.pdf

Hoke, Candice. California Top-To-Bottom Review ('TTBR') of Voting Technology. Cleveland State University Center for Election Integrity, 2007. Accessed December 11, 2007 http://urban.csuohio.edu/cei/TTBR_Summary-Voting_Tech.pdf

Harry Hursti, Critical Security Issues with Diebold Optical Scan Design, The Black Box Report Security Alert: July 4, 2005. Accessed December 11, 2007. http://www.blackboxvoting.org/BBVreport.pdf

Kiayias, A., L. Michel, A. Russell, and A. A. Shvartsman, with the assistance of M. Korman, A. See, N. Shashidhar, and D. Walluck. Security Assessment of the Diebold Optical Scan Voting Terminal, UConn VoTeR Center and Department of Computer Science and Engineering, University of Connecticut, October 30, 2006. Accessed December 11, 2007. http://voter.engr.uconn.edu/voter/Report-OS_files/uconn_report-os.pdf

Kiayias, A., L. Michel, A. Russell, and A. A. Shvartsman, with the assistance of S. Davtyan, A. See, and N. Shashidhar. Security Assessment of the Diebold TSx Voting Terminal, UConn VoTeR Center and Department of Computer Science and Engineering, University of Connecticut, July 16, 2007. Accessed December 11, 2007. http://voter.engr.uconn.edu/voter/Report-TSX_files/TSXVoting_Terminal_Report.pdf

Mercuri, Rebecca. Affidavit filed in Squire v. Geer, Franklin County (Ohio) Court of Appeals, 06APD-12-1285.

Norden, Lawrence, Chair, Brennan Center Task Force on Voting System Security. The Machinery of Democracy: Protecting Elections in an Electronic World, Brennan Center for Justice at New York School of Law, June 27, 2006. Accessed December 11, 2007. http://www.brennancenter.org/dynamic/subpages/download_file_39288.pdf

Organization for Security and Co-operation in Europe, Office of Democratic Institutions and Human Rights. Election Observation Manual, 2005. Accessed December 11, 2007. http://www.osce.org/publications/odihr/2005/04/14004_240_en.pdf

Ryan, Thomas P., and Candace Hoke. GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards, 2007. Accessed November 25, 2007. http://www.usenix.org/events/evt07/tech/full_papers/ryan/ryan.pdf

U.S. Commission on Federal Election Reform. Building Confidence in U.S. Elections. September 2005. Accessed December 11, 2007. http://www.american.edu/ia/cfer/report/full_report.pdf

U.S. Government Accountability Office. Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, But Key Activities Need to Be Completed, September 2005. Accessed December 11, 2007. http://www.gao.gov/new.items/d05956.pdf

Wagner, David. Written Testimony before the Committee on Science and Committee on House Administration U.S. House of Representatives, July 19, 2006.

Wertheimer, Michael A. Trusted Agent Report: Diebold AccuVote-TS Voting System (report prepared under cover of RABA Innovative Solution Cell on behalf of Maryland General Assembly Department of Legislative Services, Annapolis, Md.) January 2004. Accessed December 11, 2007. http://www.raba.com/press/TA_Report_AccuVote.pdf

ANNOTATIONS:

Compuware Corp. DRE Technical Security Assessment Report for Ohio, November 2003. Accessed December 11, 2007. http://www.sos.state.oh.us/sos/hava/compuware112103.pdf

Confidential report prepared for Ohio Secretary of State Ken Blackwell. High risks include:

> With access to the supervisor card, someone could guess the four digit PIN. The four digit PIN is a factory default from Diebold and cannot be changed. In our test it was guessed in less than two minutes of testing.
>
> Smart Card Writer - with access to the small handheld writer, someone could use a voting card more than once while at the voting booth.
>
> Diebold's voting system uses MS Access as the database to store the Ballot definition, Audit logs and Tally results. The Database has no password protection. The audit logs and the tally results can be changed.

Epstein, Jeremy. Improving Kentucky's Electronic Voting System Certifications. Letter to Kentucky Attorney General Greg Stumbo. September 28, 2007. Accessed December 11, 2007. http://ag.ky.gov/NR/rdonlyres/1B3F7428-0728-4E83-AADB-51343C13FA29/0/votingexpertletter.pdf

Review of Diebold/Premier, Hart InterCivic, and ES&S.

The review relies on the completeness and accuracy of the testing by the Independent Testing Authorities (ITA) for conformance to voluntary Federal guidelines (Voting systems Standards 2002). However, it has been well established that the ITAs do not adequately perform this role.

The ITA reports used for Federal certification and included in the review packages used by the SBE certifiers are cursory…. (as) reinforced by the fact that none of the ITAs identified the flaws found by the California or Florida source code review teams.

Because the ITA reports are of limited value, the quality examination of the machines as part of the certification processes is crucial, but it too can best be described as cursory.

The security of all of the machines appears to be extremely dependent on their never coming in contact with malicious code, as once that occurs there are few defenses or recovery mechanisms. This is sometimes referred to as the M&M model of security: there is a hard crunchy exterior that protects a soft chewy interior.

Short-term recommendations include developing written rules and procedures avoiding network connectivity and using sniffers to detect same, changing and properly storing all encryption keys and passwords, checking that physical seals are unbroken, and checking that the version of hardware and software being used is that which was certified.

Some long-term recommendations include a more thorough certification process, additional security measures, avoiding use of continuous tape so that voter privacy is better protected, and review of software source code for all machines used in Kentucky.

Feldman, Ariel J., J. Alex Halderman, and Edward W. Felten. Security Analysis of the Diebold AccuVote-TS Voting Machine, Center for Information Technology Policy and Dept. of Computer Science, Woodrow Wilson School of Public and International Affairs, Princeton University, 2006. http://itpolicy.princeton.edu/voting/ts-paper.pdf

The Diebold AccuVote-TS and its newer relative the AccuVote-TSx are together the most widely deployed electronic voting platform in the United States [8]. In the November 2006 general election, these machines are scheduled to be used in 357 counties representing nearly 10% of registered voters (~ 15 million).

All of Maryland and Georgia—will employ the AccuVote-TS model. More than 33,000 of the TS machines are in service nationwide.

The machine is vulnerable to a number of extremely serious attacks that undermine the accuracy and credibility of the vote counts it produces.

Malicious software running on a single voting machine can steal votes with little if any risk of detection. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss. We have constructed demonstration software that carries out this vote-stealing attack.

Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute. In practice, poll workers and others often have unsupervised access to the machines.

AccuVote-TS machines are susceptible to voting-machine viruses—computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre- and post-election activity. We have constructed a demonstration virus that spreads in this way, installing our demonstration vote-stealing program on every machine it infects.

While some of these problems can be eliminated by improving Diebold's software, others cannot be remedied without replacing the machines' hardware. Changes to election procedures would also be required to ensure security.

Fischer, Eric A. Election Reform and Electronic Voting Systems (DREs): Analysis of Security Issues, Congressional Research Service CRS Report for Congress, November 4, 2003. Accessed December 11, 2007.
http://theory.lcs.mit.edu/~rivest/voting/reports/Fischer-ElectionReformAndElectronicVotingSystemsDREs.pdf

This is a comprehensive report on several expert studies of electronic voting systems. Problems noted include:

> There appears to be an emerging consensus that in general, current DREs do not adhere sufficiently to currently accepted security principles for computer systems, especially given the central importance of voting systems to the functioning of democratic government.
>
> The ballot itself consists of redundant electronic records in the machine's computer memory banks, which the voter cannot see. This is analogous to the situation with mechanical lever voting machines, where casting the ballot moves counters that are out of view of the voter. In a lever machine, if the appropriate counters do not move correctly when a voter casts the ballot, the voter will not know, nor would an observer. Similarly, with a DRE, if the machine recorded a result in its memory that was different from what the voter chose, neither the voter nor an observer would know.
>
> The same is true with a computerized counting system when it reads punch cards or optical scan ballots. Even if the ballot is tabulated in the precinct and fed into the reading device in the presence of the voter, neither the voter nor the pollworker manning the reader can see what it is recording in its memory.
>
> Malicious computer code, or *malware,* can often be written in such a way that it is very difficult to detect.
>
> DRE software is moderately complex, and it is generally accepted that the more complex a piece of software is, the more difficult it can be to detect unauthorized modifications.
>
> Most manufacturers of DREs treat their software code as proprietary information and therefore not available for public scrutiny. Consequently, it is not possible for experts not associated with the companies to determine how vulnerable the code is to tampering.
>
> Scientists at the California Institute of Technology and the Massachusetts Institute of Technology performed the most extensive examination of security. The Caltech/MIT report identified four main security strengths of the electoral process that has evolved in the United States:
>
> - the openness of the election process, which permits observation of counting and other aspects of election procedure;
> - the decentralization of elections and the division of labor among different levels of government and different groups of people;
> - equipment that produces redundant trusted recordings of votes; and
> - the public nature and control of the election process.

The report expressed concern that current trends in electronic voting are weakening those strengths and pose significant risks.

Gardner, Ryan, Alec Yasinsac, Matt Bishop, Tadayoshi Kohno, Zachary Hartley, John Kerski, David Gainey, Ryan Walega, Evan Hollander, and Michael Gerke. **Review and Security Analysis of the Diebold Voting Machine Software**, Security and Assurance in Information Technology Laboratory Florida State University, July 27, 2007. Accessed December 11, 2007. http://election.dos.state.fl.us/pdf/SAITreport.pdf

The two primary systems analyzed consist of the Diebold Optical Scan, firmware version 1.96.8, and Touch Screen, firmware version 4.6.5. We also examined the Diebold Touch Screen bootloader version 1.3.6 as well as GEMS server software version 1.18.25.

We considered flaws in previous versions of the software for all parts of the system, including those found in the AccuBasic interpreters.

Our analysis focuses on two attacker categories… voters and poll workers. Attacks by elections officials and voting system vendors are largely outside the scope of this review. We did ***not*** conduct penetration or red team testing for these systems.

Our analysis examined only those flaws previously reported in the cited literature.

Flaws in the Optical Scan software enable an unofficial memory card to be inserted into an active terminal. Such a card can be preprogrammed to swap the electronically tabulated votes for two candidates, reroute all of a candidate's votes to a different candidate, or tabulate votes for several candidates of choice toward a different candidate.

Data on optical scan memory cards is neither encrypted nor authenticated, leading to many potential attacks that could manipulate vote counts on a memory card prior to or during the voting day.

Unsupervised access allows an attacker to place the Optical Scan terminal into diagnostics mode and obtain all or most of the data on the memory card, or to reset the machine clock.

The hand-coded RSA signature verification is insecure and can be forged. This applies to both the optical scan and touch screen systems. With technical knowledge and unsupervised access, an attacker can copy or dump the memory card contents by connecting a laptop or modem to the optical scanner.

The system uses the same cryptographic key for multiple purposes and is tied to publicly-known machine serial numbers. Its value is never changed after being created. The security key cards are insecurely protected, the same as all other smart cards, which allows anyone to read all data from them.

The public key is hard-coded into the source code. Such key-reuse is discouraged by the cryptographic community since such reuse introduces vulnerability. Supervisor PIN is not cryptographically protected.

System configuration information is unprotected. The protected counter is stored in a mutable file, and the ballot definition file is unprotected. Since stored votes are only associated with a candidate number and not a name, the ability to create custom ballot definition files allows one to alter or switch candidate names without any record in the vote counts or electronically stored ballots.

In the Touch Screen software, flaws allow an adversary to prepare official, activated voter smart cards that would enable voters to cast multiple ballots in a ballot-stuffing attack. Once an adversary obtained the necessary information, smart cards could be created and used in any precinct through a county. Even if detected, this attack is not correctable: the malicious ballots, either in electronic or paper form, are essentially unidentifiable and thus cannot be removed.

Memory card update file is unprotected. The file assure.ini remains unencrypted and unauthenticated and is subject to malicious manipulation. Removal of a memory card allows an attacker to create valid voter cards.

If the authentication key necessary to validate voter cards is the same across precincts, as we understand to be common practice in Florida, these cards could easily be modified to be used at any other precinct within a county.

Data and smart card passwords can now be set by election workers. The authentication protocol is not secure, allowing an attacker to create counterfeit, validating smart cards, including voter cards.

There is no integrity protection of stored electronic ballots and ballots are stored sequentially. This defeats voter privacy by allowing a voter's selections to be tied to a voter's name.

Audit logs are not cryptographically protected and data transmitted over communication lines is neither authenticated nor encrypted.

A custom, malicious bootloader is possible if the terminal is delivered to a polling place in debug mode. If not in debug mode, an attacker can open the case and move a hardware switch to enable this attack.   An attacker can hide preloaded votes on a forged memory card that the terminal will recognize.

Gainey, David, Michael Gerke, and Alec Yasinsac. Software Review and Security Analysis of the Diebold Voting Machine Software Supplemental Report, Security and Assurance in Information Technology Laboratory Florida State University, August 10, 2007. Accessed December 11, 2007.
http://election.dos.state.fl.us/pdf/DieboldSupplementalReportFinalSubmission.pdf

This report reflects the narrow investigative scope requested by FLDoS (Florida Department of State). These results are not comprehensive in any sense, nor is this report an endorsement of the system's overall security. We examined only a small subset of the flaws from the SAIT Diebold Report.

All other flaws identified in that report remain in the code base, including vulnerability to a sleepover attack that may allow an intruder to manipulate vote computation or worse.

Significant, critical vulnerability remains in this code base independent of repairs documented in this report.

Until voting systems are developed for high assurance, election officials face an unnecessarily high risk and must exercise significantly expanded election security procedures to mitigate known and unknown software vulnerability.

The signature flaw was fixed. This makes it much more difficult for preloaded votes to be hidden.

(Note: Other flaws reported to have been fixed were not detailed above. ~ RA)

Gonggrijp, Rop, and Willem-Jan Hengeveld. Studying the Nedap/Groenendaal ES3B Voting Computer: A Computer Security Perspective. Presented August 6, 2007 at the USENIX/ACCURATE Electronic Voting Technology Workshop, Boston, USA. (Marketed as Liberty DRE in the U.S.) Accessed December 11, 2007. http://www.wijvertrouwenstemcomputersniet.nl/images/c/ce/ES3B_EVT07.pdf

Ninety percent of the votes in The Netherlands are cast on the Nedap/Groenendaal ES3B voting computer. With very minor modifications, the same computer is also being used in parts of Germany and France.

The Nedap ES3B electronic voting computer is a touch screen system that only records votes in memory. The system requires ultimate trust, since it produces an election outcome that cannot be independently verified.

Anyone with brief access to the device at any time before an election can gain complete and virtually undetectable control over election results.

Radio emanations from an unmodified Nedap can be received at several meters distance and be used to tell who votes what.

The over-all security design relies almost solely on the near-universally deprecated concept of 'security by obscurity.' Since the problems we found stem from the very design, we see no quick fixes that could make this device sufficiently secure.

We conclude that the Nedap ES3B is unsuitable for use in elections, that the Dutch regulatory framework surrounding electronic voting insufficiently addresses security, and we pose that not enough thought has been given to the trust relationships and verifiability issues inherent in DRE class voting systems.

Given the fact that technical specifications and source code to most electronic voting systems are not publicly available, we see grave danger to our democracy by the use of secret voting technology.

Password stored in the code and quickly found, allowing attacks to read and modify election results.

Software code could be inserted, and in response to Nedap's challenge, **this team programmed the machine to play chess**. (Emphasis added. ~RA)

Software could be manipulated to steal a certain percentage of votes, for a given party. In this way, elections could be predetermined without knowing candidate names.

Parallel testing is ineffective, and only tests for outside threats - not insider attacks. The Brennan Center (2006) reached the same conclusion:

Even under the best of circumstances, Parallel Testing is an imperfect security measure. The testing creates an 'arms race' between the testers and the attacker, but the race is one in which the testers can never be certain that they have prevailed.

In the case of voting systems, the only meaningful security against insider attacks is to have a voting mechanism of which all the details are published and that a substantial portion of the general public is capable of comprehending in-depth.

By adding extra security measures against the over-emphasized threat posed by outsiders, one can actually ***increase*** the risk posed by insiders.

For example, today's mobile phones often combine a processor, execution memory and tamper-resistant key storage to make sure only the manufacturer (who has the cryptographic signing keys) can update the software. These mechanisms can sometimes still be circumvented, but at least they offer a layer of security that is completely absent in the Nedap ES3B. But by adding 'security' in this way, the device could also resist any attempts to independent inspectors to see what code it is actually running.

Goodwin-Gill, Guy S. Free & Fair Elections, International Parliamentary Union, 2006. Accessed December 11, 2007. http://www.ipu.org/PDF/publications/Free&Fair06-e.pdf

Page 157 presents a summary of the theory behind an observable vote count, and describes the benefits of a parallel election. http://www.ipu.org/PDF/publications/Free&Fair06-e.pdf

> Finally, there is the *count* and, in appropriate cases, the *transfer of power* to the successful party in the election. Complementary to the principle of secret ballot is the integrity of the count, which looks both to ensure that the expressed wish of the elector is taken into account, and that the result declared corresponds with the totality of the votes cast.
>
> Sometimes, the ballots will be counted on the spot, and at others, the ballot boxes are transported to central or regional counting stations. In either case, transparency of process is as valuable as accuracy in counting.
>
> Transportation of ballot boxes commonly gives rise to fear of substitution… Confidence in the process can be enhanced by the presence of party representatives both at the count and during any interim period of transport.

As to citizen-run parallel elections, the International Parliamentary Union explains:

> *Parallel voting tabulation* has also proven its value as a means of independently verifying the results reported by electoral authorities. In this process, monitors record results obtained from selected polling sites, and compare them with the official results: The monitoring of vote counts as part of an overall election-observation effort
>
> - Can boost the confidence of voters suspicious of possible fraud;
> - Permit results to be projected more quickly than the official results;
> - Allow for the identification of actual winners; and
> - Allow for the consequent exposure of any attempted manipulations.

Hertzberg, Steven. DRE Analysis for May 2006 Primary Cuyahoga County, Ohio, Election Science Institute, August 2006. Accessed December 11, 2007. http://bocc.cuyahogacounty.us/GSC/pdf/esi_cuyahoga_final.pdf

Steve Hertzberg of Election Science Institute (ESI) reported serious problems with Cuyahoga's May 2006 primary to Cuyahoga County Commissioners:

"I believe it is important to say directly to you … that the election system, in its entirety, exhibits shortcomings with extremely serious consequences, especially in the event of a close election. These shortcomings merit your urgent attention." (Emphasis in original)

One table in the ESI report on Cuyahoga County's May 06 primary election reports missing election assets (p.107):

- 13 VVPAT Summaries (voter verifiable paper audit trails)
- 86 VVPAT Cartridges
- 29 DREs (touch screen voting machines; one was later found)
- 24 DRE Election Archives (the archives displayed no data)
- 3 DRE memory cards.

The current election system contains significant threats to inventory control of mission critical election assets, error-free vote tabulation, and tabulation transparency.

The machines' four sources of vote totals – VVPAT individual ballots, VVPAT summary, election archive, and memory cards – did not agree with one another.

Due to limits in the data, software computational abnormality contributing to the count inaccuracies cannot be ruled out. Computational abnormality could be the result of a failure to adequately test the voting equipment before the election or to manage the various databases appropriately.

A lack of inventory controls and gaps in the chain of custody of mission critical assets, such as DRE memory cards, DRE units, and VVPAT cartridges, resulted in a significant amount of missing data. Because of the missing data, ESI is unable to give a definitive opinion of the accuracy of the Diebold TSX system.

In multi-precinct polling places, voters could vote on machines located in other precincts. Accordingly, ballots from a number of precincts appeared on the same VVPAT tape. VVPAT ballots, however, lack a header identifying the precinct. Without this information, it is not possible to conduct a precinct-level tally of the VVPAT ballots.

Consider that each machine has a printer and potentially multiple rolls of paper. Paper records of votes (the official records) may be lost without voters' awareness because of paper jams, paper not being loaded properly, ink issues, and other problems.

Lack of a standardized proven manual count process is likely to result in recount error and inefficiency.

ESI founder Steve Hertzberg spoke with wired.com's Kim Zetter in October, 2006.
http://www.wired.com/news/technology/0,71999-0.html?tw=wn_politics_evote_5
Zetter writes:

"Out of 467 touch-screen machines assigned to 145 precincts that ESI audited, officials could not locate 29 machines after the election, despite days of searching. And 24 machines that were found had no data on them. 'All their paperwork says (the machines) were deployed to polling locations but we can't figure out why there's no election data on them,' says ESI founder Steve Hertzberg. Cuyahoga County Board of Elections Director Michael Vu provided no explanation for the missing machines."

Hoke, Candice. California Top-To-Bottom Review ('TTBR') of Voting Technology.
Cleveland State University Center for Election Integrity, 2007. Accessed December 11, 2007
http://urban.csuohio.edu/cei/TTBR_Summary-Voting_Tech.pdf

In a personal email, Dr. Hoke wrote:

"Full disclosure: I was the team leader for the TTBR Diebold Documentation assessment. The TTBR study's lead scientists provided suggestions for this short summary but it is ultimately my work.

"To reduce over 500 pages to two pages, *at least a few* important findings -- especially about design flaws not relating to security issues -- had to be sidestepped."

Two-Page Summary of California's Top-To-Bottom Review:

Background

Initiated by the California Secretary of State (SOS), Debra Bowen, whose office contracted with the University of California system. Technical assessment research teams (focusing on security, accuracy and reliability issues) were led and staffed by some of the most respected computer scientists in the nation, from California and elsewhere. Documentation assessment teams involved both regulatory specialists and technically trained experts (software engineers or information systems). The Accessibility team focused on physical disability-related issues and involved two noted specialists.

Three California voting systems (VS) were comprehensively assessed: the election management/tabulation software plus the voting devices (optical scanning and DRE touchscreens), from Diebold, Hart, and Sequoia. With minor differences, all of these systems are in use in other States. ES&S systems were not evaluated.

Researchers had unprecedented access to the voting devices, software source code, testing lab and regulatory system certification reports, and other technical information.

When focusing on security and accuracy, teams considered activities that might be conducted by insiders as well as external intruders; they also considered protection of voting data from operator/election official mistakes.

Summary or Exemplar Findings

Overview: The most troubling security flaws are at the level of baseline, elementary computer security, i.e., they are not concerned with sophisticated or contested security principles on which scientists might disagree.

Election management/tabulation software

For all VS, the system architecture depends on a commercial operating system known to have security vulnerabilities. All vendors failed to secure this system properly. System architecture had not been designed with either basic or sophisticated security protections. All systems failed to follow standard security design principles.

All systems were susceptible to viruses that could be introduced from a number of vectors, including from voting device memory cards. (Viruses and other rogue programming can, e.g., flip votes among candidates, scramble tabulation data, delete voting data, and cause system programming to fail.)

Viruses could infect the central computer and then be spread to all the voting devices when their memory cards are prepared for the next election.

System logs of operator activity (audit logs) could be overwritten or erased, meaning that insider attackers could manipulate voting data and results, and then erase the logging inventories that would show the access and activity; or, could be used to frame a different employee.

Systems permitted relatively easy bypassing of passwords, thus permitting broader access than authorized.

In each VS, many other security holes exist that could compromise the system's ability to report accurate election results -- or any results.

Voting Devices

All systems failed to follow standard security design principles, and lacked even basic security protections. All systems' devices (DREs and precinct-based optical scanners) were subject to easy, undetectable attacks that could occur during the normal time that a voter would be at a voting machine casting a ballot.

Some devices permitted the researchers to introduce malicious code onto a voting machine in under a minute, while appearing to be in the process of voting.

All DRE touchscreen voting units permit a voter to generate and cast multiple ballots during a normal time voting could occur, in ways that would be largely undetectable to poll workers unless they were specially trained and closely supervising the voter's activity at the unit (voter privacy might still be compromised).

Some DRE devices permitted the researchers to damage the Voter-Verified Paper Audit Trail (VVPAT) covertly, so the voters could verify that their votes were printed correctly, but after the election the VVPAT could not be read.

Other DRE devices could be modified to store votes incorrectly, but print them on the VVPAT correctly (for example, a voter's choice of John Adams results in the VVPAT printing John Adams but the DRE stores the vote as a vote for Thomas Jefferson).

Documentation Review

The NASED qualification (certification) of all systems was based on testing lab (ITA) studies that were seriously flawed. While the ITA reports varied significantly, generally it was not possible to ascertain whether the lab had conducted the independent tests needed to determine VS satisfaction of FEC 2002 standards. Often the ITA would test a device but not the voting system as a whole, despite the guidelines' requirements for system testing to determine whether the various components worked accurately and reliably in concert.

Documentation was uniformly seriously deficient in alerting officials to security vulnerabilities and the management and training strategies so that election officials could protect the voting systems and accuracy of results.

The VS vendors varied significantly in the adequacy of the documentation they provided to local election officials. Some documentation was clear and well-written for support; other manuals were vague, contradictory and confusing.

Poor quality in a vendor's documentation for election officials can lead to a series of expensive technical services contracts with the vendors, so that a jurisdiction can run the systems.

Accessibility

Although some voting systems could be used by some voters with certain disabilities, each of the tested systems has accessibility design limitations that will not allow independent voting by voters with other disabilities.

Support stands for all the voting systems impeded physical access by most voters in wheelchairs.

The VVPAT paper trail printouts of the tested systems cannot be directly read and verified by blind voters, and were also found to be difficult or impossible to read and verify for many other voters with disabilities.

Impact

The California SOS decertified all VS that were reviewed and recertified them with special system-specific requirements. DRE units can be used only for accessibility, and a 100% hand-count audit of the votes.

The Secretaries of State in several other states have convened experts and election officials to respond to the TTBR findings relevant to their states' VS and to develop operational plans for protecting the integrity of the vote.

In other states, such as in Kentucky, the Attorney General initiated action: he convened an expert study to review VS reports with an expedited review of Kentucky's VS. Link to the report is below.

New concerns have arisen over the VS regulatory system for it did not weed out seriously flawed systems. Despite regulatory changes, these studies have raised concerns about the new regulatory system/standards.

Harry Hursti, <u>Critical Security Issues with Diebold Optical Scan Design</u>, The Black Box Report Security Alert: July 4, 2005. Accessed December 11, 2007. http://www.blackboxvoting.org/BBVreport.pdf

With this design, the functionality – the critical element to be certified during the certification process -- can be modified every time an election is prepared. Functionality is downloaded separately into each and every machine, via memory card, for every election. With this design, there is no way to verify that the certified or even standard functionality is maintained from one voting machine to the next.

Paper trail falsification – Ability to modify the election results reports so that they do not match the actual vote data 1.1) Production of false optical scan reports to facilitate checks and balances (matching the optical scan report to the central tabulator report), in order to conceal attacks like redistribution of the votes or Trojan horse scripts such as those designed by Dr. Herbert Thompson.(19)

Removal of information about pre-loaded votes 2.1) Ability to hide pre-loaded votes 2.2) Ability to hide a pre-arranged integer overflow

The exploits demonstrated in the false optical scan machine reports (poll tapes) shown on page 16 do not change the votes, only the report of the votes. When combined with the Trojan horse attack demonstrated by Dr. Thompson, this attack vector maintains an illusion of integrity by producing false reports to match the contaminated central tabulator report. The exploit demonstrated in the poll tape with a true report containing false votes, example pre-stuffs the ballot box in such a way as to produce an integer overflow.

In this exploit, a small number of votes is loaded for one candidate, offset by a large number of votes for the opposing candidate such that the sum of the numbers, because of the overflow, will be zero. The large number is designed to trigger an integer overflow such that after a certain number of votes is received it will flip the vote counter over to begin counting from zero for that candidate.

Kiayias, A., L. Michel, A. Russell, and A. A. Shvartsman, with the assistance of M. Korman, A. See, N. Shashidhar, and D. Walluck. Security Assessment of the Diebold Optical Scan Voting Terminal, UConn VoTeR Center and Department of Computer Science and Engineering, University of Connecticut, October 30, 2006. Accessed December 11, 2007. http://voter.engr.uconn.edu/voter/Report-OS_files/uconn_report-os.pdf

We identify a number of new vulnerabilities of this system which, if exploited maliciously, can invalidate the results of an election process utilizing the terminal.

An Accu-Vote Optical Scan can be compromised with off-the-shelf equipment in a matter of minutes even if the machine has its removable memory card sealed in place. The basic attack can be applied to effect a variety of results, including entirely neutralizing one candidate so that their votes are not counted, swapping the votes of two candidates, or biasing the results by shifting some votes from one candidate to another.

Such vote tabulation corruptions can lay dormant until Election Day, thus avoiding detection through pre-election tests.

The candidate names that are printed for the voter verified paper trail are based on the same RTF file that is displayed to the voter. However, the name printed for the final results is based on data from the .edb file. Because of this, **voters could be unaware of any discrepancies between their cast votes and the internally recorded votes.** Such a problem can only be detected by performing a manual count of the ballots from the VVPAT and comparing with the printed final counts. (However) [t]here is also no global check to ensure the entire election data is correct. For example, **the RTF files for candidates could be swapped … along with their integrity check.**

[emphasis added for clarity ~ RA]

Kiayias, A., L. Michel, A. Russell, and A. A. Shvartsman, with the assistance of S. Davtyan, A. See, and N. Shashidhar. Security Assessment of the Diebold TSx Voting Terminal, UConn VoTeR Center and Department of Computer Science and Engineering, University of Connecticut, July 16, 2007. Accessed December 11, 2007. http://voter.engr.uconn.edu/voter/Report-TSX_files/TSXVoting_Terminal_Report.pdf

The attacks presented in this report were discovered through direct experimentation with the voting terminal and without access to any internal documentation or the source code from the manufacturer.

We present two attacks based on these vulnerabilities: one attack swap the votes of two candidates and another erases the name of one candidate from the slate.

These attacks do not require the modification of the operating system of the voting terminal, and can be launched in a matter of minutes, requiring only a computer with the capability to mount a PCMCIA card file system (a default capability in current operating systems).

Security problems are present in the system despite the fact that a cryptographic integrity check appears to be employed in the voting system's memory card.

Mercuri, Rebecca. Affidavit filed in *Squire v. Geer*, Franklin County (Ohio) Court of Appeals, 06APD-12-1285.

Dr. Rebecca Mercuri has been studying electronic vote tabulation since 1989, and has published over 40 scientific papers on electronic voting technology. She observed the partial recount of Frankin County, Ohio's November 7, 2006 election. She also oversaw the Signature Audit of 25% of Franklin County's records. Her report found systemic problems, concluding there cannot be full confidence in the results of these (35) problematic precincts.

She describes Franklin County's recount process as constituting a breach of procedure that thwarts any meaningfully appropriate and independent recount of the election from the RTALs (real time audit logs that serve as the ballot of record in Ohio, often referred to as Voter Verified Paper Audit Trail, or VVPAT.)

The recount methodology used by Franklin County did not conform, and in fact significantly varied from the method prescribed by Ohio Secretary of State's Directive No. 2006.50 in many respects.

Dr. Mercuri concludes:

In summary, there are numerous reasons why there cannot be confidence in the election process, the recount, and the vote totals for the Franklin County, Ohio November 7, 2006 election. These reasons include:

a) the denial of an appropriate recount from the VVPAT/RTAL materials for the requested precincts;
b) significant evidence that parts of original RTALs and end tally reports were missing;
c) evidence the voting system was inappropriately configured and improperly used during the election;
d) indication that election procedures were violated, including the possibility of password overrides during setup, and use of the machines to cast ballots after RTAL paper supplies has run out;
e) evidence of inappropriate impounding and handling of election materials at the County warehouse following the election, including improper exposure of the VVPAT/RTALs;
f) unexplained disparities between the public counters of ballots cast and the number of voters who signed the poll books in many precincts; and
g) misleading information provided to voters, and not properly followed up by the County, regarding the safety and examination of the voting machines and system.

Norden, Lawrence, Chair, Brennan Center Task Force on Voting System Security. The Machinery of Democracy: Protecting Elections in an Electronic World, Brennan Center for Justice at New York School of Law, June 27, 2006. Accessed December 11, 2007. http://www.brennancenter.org/dynamic/subpages/download_file_39288.pdf

Studied 3 voting systems by type: DRE, DRE w/VVPAT, and Optical Scan. Brennan identified 120 vulnerability points.

Report is limited to identifying the least difficult way to alter results on a statewide basis. It is also limited to studying attacks that cannot be prevented by physical security and accounting measures taken by election officials. The analysis further assumed that certain fundamental physical security and accounting procedures were already in place.

Concluded that it would take only one person, with a sophisticated technical knowledge and timely access to the software that runs the voting machines, to change the outcome.

All three voting systems have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections.

The most troubling vulnerabilities of each system can be substantially remedied if proper countermeasures are implemented at the state and local level.

Few jurisdictions have implemented any of the key countermeasures that could make the least difficult attacks against voting systems much more difficult to execute successfully.

For *all three* types of voting systems:

1. When the goal is to change the outcome of a close statewide election, attacks that involve the insertion of Software Attack Programs or other corrupt software are the least difficult attacks.

2. Voting machines that have wireless components are significantly more vulnerable to a wide array of attacks.

DREs without voter-verified paper trails do not have available to them a powerful countermeasure to software attacks: post-election Automatic Routine Audits that compare paper records to electronic records.

For DREs w/VVPT and PCOS:

1. The voter-verified paper record, *by itself*, is of questionable security value. The paper record has significant value only if an Automatic Routine Audit is performed (and a well-designed chain of custody and physical security procedures is followed).

2. Even if jurisdictions routinely conduct audits of voter-verified paper records, DREs w/VVPT and PCOS are vulnerable to certain software attacks or errors.

Organization for Security and Co-operation in Europe, Office of Democratic Institutions and Human Rights. Election Observation Manual, 2005. Accessed December 11, 2007. http://www.osce.org/publications/odihr/2005/04/14004_240_en.pdf

Seventeen Criteria for a Fair Vote Count (p. 62) precludes machine tabulation:

1. Is the count performed by polling-station officials, or are other persons involved?

2. Do election officials appear to understand and adhere to the required procedures?

3. Are ballots counted in an orderly and secure manner?

4. Is the count conducted in a transparent environment, with adequate arrangements for domestic observers?

5. Does the number of registered voters recorded as having voted correspond with the number of ballots cast?

6. Are unused ballots secured, cancelled, or destroyed after being counted?

7. Are invalid ballots properly identified in a uniform manner? Are invalid ballots appropriately segregated and preserved for review?

8. Do the ballots contain any unusual markings intended to violate the secrecy of the vote?

9. Does the number of invalid ballots seem inordinately high?

10. Does the counting adhere to the principle that the ballot is deemed valid if the will of the voter is clear?

11. Are ballots for each party or candidate separated correctly and counted individually?

12. Are any disputes or complaints resolved in a satisfactory manner?

13. Are official counting records correctly completed at the end of the count and signed by all authorized persons?

14. Are domestic observers and poll watchers from political parties able to obtain official copies of the protocol for the polling station?

15. Are the results publicly posted at the polling station?

16. Are there inappropriate activities by police and/or security forces, such as taking notes and reporting figures or results by telephone?

17. Did polling-station officials agree on the vote-count procedures and results, and, if not, what action was taken in case of disagreement?

Ryan, Thomas P., and Candace Hoke. GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards, 2007. Accessed November 25, 2007. http://www.usenix.org/events/evt07/tech/full_papers/ryan/ryan.pdf

Abstract: This paper analyzes the Diebold Election Systems, Inc. election management software (GEMS) using publicly accessible postings of GEMS election databases.

It finds that the GEMS architecture fails to conform to fundamental database design principles and software industry standards for ensuring accurate data. Thus, in election tabulations, aspects of the GEMS design can lead to, or fail to protect against, erroneous reporting of election results. Further, GEMS' dependence on Microsoft's JET technology introduces additional risks to data accuracy and security.

Despite these technical and systemic deficiencies, GEMS received approval as complying with Federal Voting System 2002 standards. Questions then arise concerning the adequacy of the 2002 and 2005 regulatory standards.

The paper concludes that the standards structurally encourage and reward election system vendors for using less exacting database design standards.

U.S. Commission on Federal Election Reform. Building Confidence in U.S. Elections. September 2005. Accessed December 11, 2007.
http://www.american.edu/ia/cfer/report/full_report.pdf

Former Secretary of State James A. Baker III and former President Jimmy Carter, who were co-chairmen of the bipartisan Commission on Federal Election Reform, warned in their 2005 final report that (fraud) could happen.

"Software can be modified maliciously before being installed into individual voting machines. There is no reason to trust insiders in the election industry any more than in other industries."

U.S. Government Accountability Office. Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, But Key Activities Need to Be Completed, September 2005. Accessed December 11, 2007.
http://www.gao.gov/new.items/d05956.pdf

Voting system vulnerabilities and problems found include:

- Cast ballots, ballot definition files, and audit logs could be modified;
- Supervisor functions were protected with weak or easily guessed passwords;
- Systems had easily picked locks and power switches that were exposed and unprotected;
- Local jurisdictions misconfigured their electronic voting systems, leading to election day problems;
- Voting systems experienced operational failures during elections;
- Vendors installed uncertified software;
- Some electronic voting systems did not encrypt cast ballots or system audit logs, and it was possible to alter both without being detected;
- It was possible to alter the files that define how a ballot looks and works so that the votes for one candidate could be recorded for a different candidate.

Wagner, David. Written Testimony before the Committee on Science and Committee on House Administration U.S. House of Representatives, July 19, 2006.

The federal qualification process is not working. Federal standards call for voting machines to be tested by Independent Testing Authorities (ITAs) before the machines are approved for use, but ITA-approved machines have:

* Lost thousands of votes across the country, and have reported thousands more votes than voters;

* Failed to catch numerous security defects found by academics, industry consultants and interested outsiders.

The 2005 VVSG standards contain significant shortcomings regarding the security, reliability, and auditability of electronic voting:

* ITAs are paid by the vendors whose systems they are evaluating, raising conflicts of interest between the voting public and client-vendors;

* The process lacks transparency, rendering effective public oversight difficult or impossible;

* Technical information about voting systems is often considered proprietary and secret by vendors, and voting system source code is generally not available to independent experts. In the rare cases where independent experts have been able to gain access to source code, they have discovered reliability and security problems;

* Testing is too lax to ensure the machines are secure, reliable, and trustworthy.

* Many standards in the requirements appear to be ignored during ITA testing;

* If serious flaws are discovered in a voting system after it has been approved, there is no mechanism to decertify the flawed system.

Wertheimer, Michael A. Trusted Agent Report: Diebold AccuVote-TS Voting System (report prepared under cover of RABA Innovative Solution Cell on behalf of Maryland General Assembly Department of Legislative Services, Annapolis, Md.) January 2004. Accessed December 11, 2007. http://www.raba.com/press/TA_Report_AccuVote.pdf

The general lack of security awareness, as reflected in the Diebold code, is a valid and troubling revelation. In addition, it is not evident that widely accepted standards of software development were followed.

Knowing the password, a smart card can be replicated, and the voter can vote multiple times. RABA was able to guess the passwords quickly, and access each card's contents (Supervisor Card, Voter Card, and Security Key Card). Given access to the cards' contents it became an easy matter to duplicate them, to change a voter card to a supervisor card (and vice versa) and to reinitialize a voter card so that it could be used to vote multiple times.

The use of hardcoded passwords is surprising both as an inferior design principle and in light of them being published openly in the Hopkins report. It must be assumed these passwords are well known.

The contents of these cards are neither encrypted nor digitally signed. Thus, for example, the PIN associated with a Supervisor Card23 can be read directly from the card – provided the password is known. This means creating Supervisor Cards is a simple task: a perpetrator could program his card with an arbitrary PIN that the AccuVote-TS would readily accept.

It is reasonable to assume that a working key to the AccuVote hardware is available to an attacker. The hardware consists of a touch-screen voting terminal with two locked bays.

Maryland has ordered approximately 16,000 AccuVote-TS terminals each equipped with two locking bays and supplied with two keys accounting for 32,000 locks and keys. Surprisingly, *each lock is identical and can be opened by any one of the 32,000 keys.* Furthermore*,* team members were able to have duplicates made at local hardware stores.

One team member picked the lock in approximately 10 seconds. Individuals with no experience (in picking locks) were able to pick the lock in approximately 1 minute.

A sampling of the vulnerabilities found as a result of poor physical security coupled with software that fails to use robust encryption and authentication include six methods of attack. (Not reproduced herein.)

The GEMS server lacks several critical security updates from Microsoft. The team was able to *remotely* upload, download and execute files with full system administrator privileges.

The server enables the autorun feature. Given physical access to the server, one can insert a CD that will automatically upload malicious software, modify or delete elections, or reorder ballot definitions.

The back panel of the GEMS server is not protected. Given physical access to a running device it is possible to insert a USB flash drive and upload malicious software onto the server.

The database files that contain the election definition (and results) are neither encrypted nor authentication protected. By removing the front panel of the server (this is held in place by a small keyed lock), one can insert a CD, power up the server, and have it boot its operating system off the CD. A sophisticated user can automate this procedure requiring only a few minutes access to the server.

Because both the database password and audit logs are stored within the database itself, it is possible to modify the contents without detection. Furthermore, system auditing is not configured to detect access to the database. Given either physical or remote access it is possible to modify the GEMS database.

The procedure by which precincts upload votes to their LBE is vulnerable to a man-in-the-middle attack.

The team identified fifteen additional Microsoft patches that have not been installed on the servers. In addition, the servers lack additional measures (all considered best practice) for defense such as the use of firewall antivirus programs as well as the application of least privilege, i.e. turning off the services that are unused or not needed. Each of these represents a potential attack vector for the determined adversary.

####