SUPREME COURT OF THE STATE OF NEW YORK
COUNTY OF NASSAU

----------X

COUNTY OF NASSAU, NASSAU COUNTY BOARD OF ELECTIONS, JOHN A. DEGRACE, in his official capacity as Nassau County Republican Commissioner of Elections, and WILLIAM T. BIAMONTE, in his official capacity as Nassau County Democratic Commissioner of Elections,

Index No. _____

Petitioners-Plaintiffs,

- against -

STATE OF NEW YORK, NEW YORK STATE BOARD OF ELECTIONS, and JAMES A. WALSH, DOUGLAS A. KELLNER, EVELYN J. AQUILA, GREGORY P. PETERSON as Commissioners constituting the Board,

Respondents-Defendants.

----------X

EXPERT AFFIDAVIT OF ALEXANDER A. SHVARTSMAN IN SUPPORT OF PETITION-COMPLAINT

On the Security and Integrity Issues of Optical Scan Voting Systems

Alexander A. Shvartsman
aas@votingsecurity.com

Voting Systems Security, LLC
23 Moulton Road
Storrs, CT 06268

March 19, 2010

Alexander A. Shvartsman, being duly sworn, deposes and says:

Credentials

1. I am a Professor (full, tenured) and Associate Head of the Computer Science & Engineering Department at the University of Connecticut (UConn). I am also the Director of the UConn Voting Technology Research (VoTeR) Center.

2. I earned B.S. at Stevens Institute of Technology in 1979, with High Honor, M.S. at Cornell University in 1981, and Ph.D. at Brown University in 1992, all in Computer Science. I did my post-doctoral work at the Massachusetts Institute of Technology from 1995 to 1997.

3. I have been at UConn for over 10 years, and prior to that I worked for over 10 years in the industry as a member of the technical staff at AT&T Bell Labs and Digital Equipment Corporation.

4. My research broadly deals with dependable computing systems, distributed computing, fault-tolerance, information assurance, and responsible electronic voting systems. My research has been supported by several federal grants, including Air Force Office of Sponsored Research and National Science Foundation, and I am a past winner of the NSF CAREER Award.

5. I served as a chair and as a program committee member of numerous conferences in my areas of research. I am an author of over 125 scholarly articles and two books.

6. In the area of dependable electronic voting systems I made important contributions in discovering security and integrity vulnerabilities of electronic voting equipment and developing safe-use procedures and state-wide technological audits in Connecticut. I have been deeply involved in the selection, deployment and audits of electronic voting systems in Connecticut.

7. In 2005–2006 I served as a member of the Connecticut Voting Technology Standards Board, appointed by the Governor. Since 2006, I am the Director of the Voting Technology Research Center at the University of Connecticut.

8. I co-authored and published a number of reports documenting my research and findings, including the reports on voting system vulnerabilities and the results of the technological audits performed by the VoTeR Center in Connecticut.

Activities of the University of Connecticut Center for Voting Technology Research

9. The primary author, Alexander A. Shvartsman, and the three contributing authors — Dr. Aggelos Kiayias, Dr. Laurent Michel, and Dr. Alexander Russell — are the four principal investigators at the University of Connecticut Center for Voting Technology Research (VoTeR Center). The Center was established in 2006 with the help of State of Connecticut funding. The Center currently has four faculty members, an engineer, and several graduate students.The Center works with the Office of the Secretary of the State in ensuring technological integrity of the electoral processes.

10. In the past four years the VoTeR Center has been engaged by the Secretary of State's Office of the State of Connecticut to advise the State on electronic voting technology issues. The Center has been deeply involved in the selection and deployment of electronic voting systems in Connecticut, security and integrity evaluation of voting systems, recommendations for safe use of electronic voting equipment, and technological audits of voting equipment. In 2009 the principals of the Center were honored by the Secretary of the State with a *Public Service Award* for "invaluable contributions to assuring the success of our electoral process."

11. The Center has published numerous reports documenting our research and findings, including the reports on voting system vulnerabilities and the results of the technological audits performed by the VoTeR Center in Connecticut. The Center personnel made several presentations of their findings at key international conferences dealing with security and integrity of elections conducted with the help of electronic equipment. Copies of selected reports are available at `http://voter.engr.uconn.edu/voter/reports/`.

Summary: Electronic Voting Systems, Vulnerabilities, and their Potential Impact on Elections

12. An electronic voting systems is a complex distributed system comprised of several types of devices, including (i.) election management systems, (ii.) electronic voting terminals, such as optical scan terminals, direct entry electronic terminals, and/or enhanced-access terminals for people with disabilities, (iii.) voter-assist terminals, such as ballot marking devices, (iv.) removable memory devices, such as memory cards, universal serial bus drives, compact flash drives, etc., (v.) means of communication, including removable media, and telephone and data networks.

13. Electronic voting terminals are complex computing devices that include sophisticated hardware and software. The behavior of any given voting terminal depends on the software/firmware pre-installed on the terminal, software/firmware installed as an upgrade, and software and data installed for the purposes of an election via removable media. Any such installation, including the installation of election-specific software and data via removable media, can completely change the behavior of the terminal. In particular, incorrect, incomplete, or even arbitrary precinct election results can be reported by optical scan terminals due to errors or malicious interference.

14. Election management systems are used to configure elections, program removable media for optical scanner terminals, and to aggregate precinct-level results. These systems are complex, using general purpose computers, operating systems, and specific election management software. It is extremely difficult to guarantee correctness and tamper-freedom of such complex systems. Election management systems can contain faults and can be subject to malicious tampering. The result can be that such systems report election outcomes that do not accurately reflect the votes cast in an election.

15. Removable memory devices serve to provide election configuration to optical scan terminals and to convey the results to central tabulation. Such devices have proved to be a major source of vulnerabilities in electronic voting systems. The cards connect the election management system and the optical scan terminals into a large distributed system. Inadequate security measures (electro-mechanical, software, cryptographic, and physical custody) can allow errors, introduced inadvertently or as the result of deliberate tampering, to propagate through

the entire system. Such errors can create broad tampering risks and lead, in extreme cases, to massive failures. Every component of such distributed electronic system is susceptible to attacks, both external attacks and insider attacks.

16. Although vendors have improved their use of cryptography, the mere application of cryptographic mechanisms such as (i.) hash checking for software integrity, (ii.) encryption for confidentiality of election related data, and (iii.) digital signatures for integrity of election data, does not guarantee in itself that the desired properties are achieved. Use of good tools must go hand-in-hand with good use of tools. In particular, severe security deficiencies have been reported in optical scan voting terminals despite use of cryptographic tools.

17. The complexity and size of election systems and their dynamic nature due to the software they use, including vendor-specific software, software from third parties used by the vendors, and election-specific software and data, preclude any absolute guarantees of security, integrity, correctness, fault-tolerance, and performance. Testing and certification notwithstanding, the only current way to guarantee that the voter-verified paper ballots are correctly tabulated and that the results are correctly reported is to hand count the ballots.

18. The state-of-the-art in verifying correctness of complex software systems makes it unfeasible to provide formal correctness and security guarantees. Testing and certification, although able to increase one's belief in the integrity of electronic election systems, are in fact only able to prove the presence of errors and problems, and are unable to prove correctness of such systems. There exists no compelling evidence that any electronic election system has been certified or verified in any scientifically meaningful sense. All such systems that were seriously evaluated have been shown to have internal logic errors and/or vulnerabilities, calling into question any election results reported by such systems.

19. Being complex software-based systems, electronic election systems perform their activities in a way that cannot be observed. The inability to observe the inner workings of the system precludes external observers and officials from achieving their primary mission. Indeed, a compromised voting terminal may appear to look, act and operate exactly like a legitimate terminal. It is impossible for election officials to ascertain whether or not a system is operating correctly by observing its behavior and by running vendor-supplied tests. The election officials must rely on vendors, their representatives, and domain experts and, in effect, delegate to them some of their responsibilities.

20. All vulnerable systems are can be successfully attacked, and the literature is replete with evidence that attacks are quite feasible. The severity of attacks and the extent of the damage varies, ranging from a mere denial of service and escalating to state-wide election outcome alterations. Even in the absence of malicious intent, system failures can cause a voting system to misrepresent the will of the electorate. The use of election management systems to program removable media and to conduct automatic aggregation can significantly amplify system failures.

21. For these reasons it is necessary (in addition to any and all traditional policies and procedures, and strict chain-of-custody requirements) to have a broad technological oversight of the electronic election systems in order to safeguard the integrity of the electoral process. In particular, it is necessary to conduct routine comprehensive pre-election and post-election technological audits of the election management systems and a substantial percentage of optical scan tabulators. Such audits may be feasible for smaller states, provided the election technology is relatively simple. It may be infeasible for larger states when deploying highly complex electronic voting systems, such as those considered in New York State.

22. Optical scan voting technology offers a Voter Verified Audit Trail (VVAT) which currently presents a clear advantage over Direct Recording Electronic terminals (DRE). VVAT enables hand counted audits to be performed after the election. To yield meaningful results hand counted audits must cover a substantial percentage of precincts and/or optical scanners. Doing so on a broad scale implies a complete manual recount in audited precincts, which negatively impacts the benefits of electronic counting. On the other hand, performing a modest audit, such as New York's 3% audit can only detect with high probability widespread system failures or massive electronic fraud. In particular, a 3% audit cannot with high certainty detect localized failures or irregularities in

small number of districts. This is particularly significant for elections with small margins of victory, because a small number of incorrectly tabulated districts can lead to the circumvention of the will of the entire electorate.

23. A combination of comprehensive technological audits and hand counted audits can prevent electoral process failures and substantially increase confidence in the election outcome. However, (i.) technological audits are difficult and perhaps infeasible for complex electronic election systems, and (ii.) modest hand-counted audits, such as a 3% audit, provide protection principally against massive failure and fraud and are ineffective against localized instances of tampering and failure; such audits are statistically unable to instill confidence in close elections.

24. We also note that the New York Election Law requires the board of elections to be responsible for certain activities that the board is likely either not be able to perform or not be able to conclude that the activities have been successfully (or not) performed. For example, testing every voting machine "to insure that each such machine functions properly" (§7-206). The board(s) are not in the position to ensure this, and clearly cannot rely on vendor-supplied tests: such tests are designed by an interested side and have been historically incapable of detecting tampering. In some cases the law provides for "technicians" that are employees and that are directed by the board(s) "to insure that voting machines are in proper repair and working order" (§3-302). Given the complexity of the systems and the task, it is unlikely that the technicians without substantial and deep expertise in the relevant technologies can meaningfully guarantee such circumstances.

25. The state of practice in the domain of electronic voting systems can be generally described as premature deployment of immature technology. In order to use the currently available electronic voting systems in a responsible way, it is necessary to include and rely on the participation of domain experts (either vendors themselves or third parties) – the systems are simply not ready for unassisted end-user deployment, given the high demands for integrity in the electoral processes.

Optical Scan Election Systems, an Overview

26. Optical scan voting terminals are instruments for counting votes recorded on paper ballots. In typical current practice, ballots are either directly marked by voters or with the assistance of ballot marking devices in controlled circumstances; this physical record of an election is processed by the voting terminal to produce a tally. A strength of such a system and its clear advantage over the Direct Recording Electronic (DRE) systems (whether or not DRE systems produce a computer-printed paper record) is that the resulting paper trail is directly verified by voters and it can be used for various verification processes including, for example, independent recounts.

27. The underlying computational process carried out by such terminals is, in the abstract, very simple: it consists of identifying marked portions of the ballot, insuring that the markings correspond to a legal vote, and incrementing associated counters. In fact, even the simplest voting terminals are enormously complex, consisting of computing hardware comparable to that of general purpose computers. It is convenient to distinguish voting terminal hardware from the software it runs for a number of reasons: (i.) the bulk of the logic specific to the machine's function as a voting terminal is reflected in the software; hardware, in contrast, is typically more generic in function, (ii.) typical systems provide a means for replacing resident software (for the purpose of introducing new features or correcting deficiencies). We use the term "firmware" throughout to refer to all software running on a voting terminal.

28. In existing optical scan systems, the terminal described above is used in conjunction with a removable storage device, the principal vehicle for electronic communication with the terminal. (We remark that some systems provide other means of electronic communication, such as a modem.) In particular, removable storage is typically used to import election data, such as ballot layout, race characteristics, and candidate identities. Additionally, removable storage is typically a potential means for exporting vote tallies for the purposes of electronic tally aggregation.

29. In a typical jurisdiction, optical scan terminals deployment is complemented by an Election Management System, or EMS, that is used to define ballots for specific contests, to program the removal storage devices used by the optical scan terminals, and to aggregate election results from precincts after the close of polls by either reading in precinct results from the removable storage devices corresponding to the precincts where they were used in the precinct optical scanners, or by other means. EMS software is typically installed on a general purpose computer.

30. Prior to any election relying on such equipment, paper ballots must be prepared to match an electronic ballot description. In typical usage, as mentioned above, this electronic description is communicated to the terminal by removable storage. The infrastructure for pre-election preparation and post-election electronic vote aggregation is provided by Election Management Systems (EMS).

A More Detailed Description of Optical Scan Election Systems

31. **Firmware.** We define the body of programming responsible for carrying out the functions of the voting terminal as *firmware*. It may reside in a variety of storage media: (i.) firmware may reside in a read-only PROM (hardware chip) directly affixed to the terminal hardware; (ii.) firmware may reside in nonvolatile, but write-accessible, memory in the terminal (for example, flash memory or a hard drive); and (iii.) firmware may reside in a removable memory device. Typical terminals (like typical general purpose computers) adopt a mixture of these options. For example, in the the Premier's AccuVote Optical Scan (AVOS) system,[1] a hybrid approach is adopted where some firmware components reside in a read-only EPROM and some components are stored on removable and rewritable media.

32. Existing optical scan voting terminals provide a means for replacing firmware (for the purpose of upgrades). In cases where firmware resides in non-writable memory devices (e.g., PROMs), this requires physical replacement. When, instead, firmware resides in writable memory devices (e.g., flash memory) it is typically transferred to the terminal from a removable storage device.

33. **Removable storage.** All existing optical scan machines utilize some variety of removable, non-volatile, read-write storage. Removable storage is used to transmit election-specific data to the voting terminal: ballot layout, race characteristics, and candidate identities. Additionally, election results, including logs and vote tallies, are typically stored on removable storage. As mentioned above, removable storage is often used for firmware upgrades.

34. Ballot layout data provides the association between the location of markings in scanned ballot images with a digital model of the ballot and, hence, the rules for interpreting markings as votes. This digital model of the layout is specific to each election and is installed into the OS voting terminal via removable storage media. Similarly, election-specific validation rules accompany ballot information on removable media. These rules determine when a collection of markings on a ballot constitute a legal vote.

35. Additionally, the tallies produced by the OS terminal as it processes the ballots are saved in non-volatile rewritable and removable memory. Often, this is the same removable media used to communicate ballot data. Final tally data present on removable storage media can typically enable a digital tallying process to consolidate the results from several machines and polling places.

36. Thus, removable storage is typically in active use during three phases of the electoral process: (i.) prior to the election, to load the ballot definition (a digital model of its layout and integrity rules), (ii.) during the election to hold transient results as the terminal scans ballots as well as logs of its activity, (iii.) possibly after the election closes to serve as a vehicle for result aggregation across multiple machine and polling places. During initial programming and post-election aggregation processes, the memory card is typically *separated from the terminal and transported to other sites while it contains sensitive election data.*

[1] Seda Davtyan, Sotiris Kentros, Aggelos Kiayias, Laurent D. Michel, Nicolas C. Nicolaou, Alexander Russell, Andrew See, Narasimha Shashidhar, Alexander A. Shvartsman: Taking total control of voting systems: firmware manipulations on an optical scan voting terminal. 2009 ACM Symposium on Applied Computing: 2049-2053.

37. The integrity of this removable media is thus critical to maintaining correctness of the election results. Existing OS terminal vendors have settled on commodity, off-the-shelf solutions for removable memory. Current solutions range from compact-flash memory cards, to usb memory sticks or even vintage EPSON memory cards (precursors to PCMCIA cards) as in the AVOS terminal. The common traits in all solutions are (i.) non-volatility: the contents of the memory is persistent, not relying on an external power source, (ii.) rewritability: the content can be modified at will, and (iii.) portability.

38. **The Election Management System** (EMS). The election management system is a critical hardware and software component that plays a key role in the configuration and operation of the individual optical scan terminals. The hardware part of EMS is, generally, an off-the-shelf computer such as a PC running an off-the-shelf operating system (e.g., Microsoft Windows). The software part of the EMS is provided by the vendor of the optical scan terminals and it is used to configure the contests in a particular election, to set up the memory cards for elections, and for post-election tally aggregation either by loading the election data from memory cards or receiving the data through a telephone or other network.

39. The two optical scan election systems under consideration in New York State are the ES&S Unity 3.0 and Dominion Democracy Suite 3.0 voting systems are classical examples of the systems described above. Both optical scan voting terminal (The DS200 and the ImageCast) are based on the Linux Operating Systems (i.e., large and general purpose off-the-shelf operating systems). Both optical scan systems rely on removable memory cards, specifically, the DS200 uses standard off-the-shelf Universal Serial Bus (USB) memory sticks of large capacities, while the ImageCast relies on Compact Flash memory cards. The ImageCast also features a USB port (meant for a printer, but USB is a general purpose port). Both use election management systems (EMS) running on commodity hardware/software (Microsoft Windows Server/Microsoft Windows XP). Both systems offer the capabilities described above, namely: preparing ballot descriptions ahead of the election, memory card programming, processing ballots at the polling station and aggregation of precinct-level results through the EMS. Additionally there is an option of using a ballot marking device.

Vulnerabilities of Optical Scan Election Systems

Optical Scan Election Systems are Intrinsically Complex

40. The hardware used in an optical scan voting terminal is best described as general purpose computing equipment. The widespread use of commercial, off-the-shelf components contributes to this state of affairs. For illustration purposes, consider the following off-the-shelf components such as commodity Intel processors (e.g., found in Premier's Accu-Vote, ES&S DS200, Avante VoteTracker), universal-serial-bus (USB) interfaces (e.g., in ES&S DS200, Avante VoteTracker), serial and parallel ports (e.g., RS-232 found in DS200, Accu-Vote, VoteTracker), standard modems and ethernet ports (e.g., Accu-Vote, VoteTracker, DS200, Dominion). Some vendors go so far as to use a complete off-the-shelf personal computer (e.g., Avante).

41. We emphasize that such general purpose hardware can itself offer no guarantees as to the correctness of the vote processing carried out by the equipment: (i.) hardware itself can be faulty; even the hardware systems built under the most stringent quality control can be faulty, e.g., the infamous "Intel Pentium bug" that caused intermittent computation errors,[2] (ii.) alterations to the resident software can completely change the behavior of the machine regardless of the correctness of the hardware itself.

42. Additionally, most vendors also use off-the-shelf systems software (i.e., Operating Systems) for managing their off-the-shelf hardware. Some machines rely on Microsoft Windows operating systems, such as Windows CE or Linux as these are convenient software platforms for managing the complexity of the underlying hardware. General purpose operating systems are truly staggering in term of complexity. (For instance, Both Windows 2000 and Linux are estimated to be well over 50 millions line of code and Linux is written by thousands of volunteer developers worldwide).

[2] Tom R. Halfhill. "An error in a lookup table created the infamous bug in Intel's latest processor." BYTE. March 1995.

43. The immediate implication is that, despite a minimalistic interface presented to voters, an (optical scan) voting terminal is an extremely capable device rivaling, if not equaling, conventional personal computers. Optical scan voting terminals are also comparable to personal computers in term of complexity and are susceptible to similar weaknesses (e.g., viruses, malware, or any other type of software injection, and, of course, unintentional software errors).

44. Verifying that a computing device performs precisely the set of tasks for which it has been designed is a notoriously difficult problem in computer science. When this "verification problem" is formalized in a suitably general way, it can be mathematically proved to be impossible to solve. In principle, this kind of verification is possible for devices that are specially designed to permit verification. While the last two decades have seen progress in verification, the techniques are still limited. While in practice, it is possible to partially verify tiny systems, verifying large software remains as elusive as ever. Verifying a modest operating system has never been accomplished, let alone one with more than 50 millions line of code.

45. While it is tempting to view a voting terminal in isolation, it is critical to view the entire system formed by hundreds (or even thousands) of voting terminal (and ballot marking devices, if any) distributed over a large geographical area and ultimately interacting with a single central system, e.g., EMS, for the preparation of the election and the tabulation of the results. It is therefore a large, complex distributed system (even if it is only sporadically interconnected, e.g., by means of programmed removable media devices).

46. Attempting to verify and certify an optical scan terminal without at the same time verifying and certifying all involved systems, including EMS, provides a false sense of security. Where central aggregation of tallies is employed, showing that malicious exploits are impossible, and that computation and logic errors are not present, requires considering how the data from multiple voting terminals interacts with EMS; this is even more challenging.

47. Because an electronic voting system is in effect a complex distributed system, the "closed network" requirement, such as New York Election Law, Rules and Regulations §6210.11(G), does not by itself offer protection against external (attempts of) infiltration.

48. Two observations are critical in this respect: (i.) The safety and correctness of a large distributed system is only as good as its weakest link. Additionally, a single failure — whether benign or malicious — can ripple through and affect the entire system. (ii.) Procedural counter-measures can be used to mitigate the weaknesses of the system; yet, any procedure performed by a human operator has a — perhaps small — likelihood of failure. In a large system relying on many distributed procedural elements, the probability of a procedure failure can be extremely high, even if each individual procedure fails with small probability. For the purposes of illustration, suppose that drivers accidentally forget to lock their cars 1% of the time. In this case, a parking lot of even 500 cars is 99% likely to contain an unlocked car.

Use of Cryptography: Using Good Tools vs. Good Use of Tools

49. The cryptographic mechanisms used in conjunction with electronic voting systems include (i.) cryptographic hash functions, (ii.) cryptographic encryption, and (iii.) digital signatures. While these mechanisms are valuable tools, merely using them is not sufficient to ensure integrity of an electronic election system.

50. Cryptographic digital fingerprints (computed by so-called *hash functions*) are used to check the integrity of a software module. A digital fingerprint is a short sequence of binary digits and is included with the module. This fingerprint has the property that it is extremely difficult to construct another software module with an identical fingerprint. Thus checking the fingerprint of a software module against its known correct fingerprint enables one to confirm with high probability that the correct module is installed.

51. However, the mere employment of a digital fingerprint check does not necessarily guarantee that incorrect software module will be detected even if the used hash algorithm is standardized and believed to be secure,

such as the Secure Hash Standard (SHS).[3] To illustrate this point consider that a system running compromised software may deliberately try to misrepresent the hash value of its software image. If a successful attack of this type takes place it will enable rogue software to run undetected. To ensure that such attacks are thwarted it is imperative that the hash function calculation is guaranteed to be performed in a trustworthy fashion either through direct interaction with the target system's trusted hardware, or by using a trusted platform module (TPM) that can be relied on to perform the needed computation correctly.

52. Cryptographic encryption is a technique for hiding information: here the information is obscured by using encryption algorithms and keys in such a way that it is very difficult to recover the original information without the knowledge of the keys. They keys themselves are pieces of information (sequences of binary digits) that control the behavior of the encryption and decryption algorithms.

53. The mere employment of encryption does not necessarily guarantee confidentiality even if the encryption algorithm used is a standardized and believed to be secure algorithm, such as the Advanced Encryption Standard (AES).[4] To illustrate this point consider a setting where AES is used to encrypt individual records. AES, on its own, does not guarantee that encrypting two identical records results in two distinct ciphers. As a result, applying encryption to a series of records that belong to a small set of possible forms does not prevent analysis of the resulting encrypted data, such as the data found on a removable memory card. This type of attack was in fact illustrated in the context of electronic voting systems.[5]

54. Digital signatures are a mechanism for authenticating data records (such as messages, documents, database records). Digital signatures are analogous to hand-written signatures used for authenticating authorship. Specific algorithms using keys are used to produce signed digital data and subsequently to ascertain the authenticity of the data where it is to be used.

55. The mere employment of digital signatures does not necessarily guarantee integrity even if the signature algorithm is a standardized algorithm that is believed to be secure, such as the Digital Signature Algorithm (DSA).[6] To minimize the risks of tampering, it is crucial to ensure that the signed data is interpreted correctly and is used as intended. For example, consider a direct-recording electronic voting terminal, where the digital ballot is a list of pairs of digitally signed records. The first element of the pair represents the candidate name and associated counter. The second element of the pair tells the terminal how the candidate's information is displayed for the voter on the screen. Note that while the records are signed the pairings themselves are not signed and can be tampered with. A successful exploit of this is reported in a VoTeR Center technical report[7] where the attacker uses the absence of signature on the pairing to swap the graphical representations of two candidates on the display and therefore swaps their votes. This exploit does not tamper with any signed data, but rearranges order of data so that terminal does not operate correctly. Clearly, cryptography alone did not prevent tampering and its advertising without specific details can lead to a false sense of security.

56. Cryptographic techniques can mitigate the risks of attacks against removable media cards. The level of protection depends upon the strength of the cryptographic techniques, upon the safe keeping of the digital keys used to protect the cards, but also upon the safe-keeping of the voting terminal themselves. Indeed, the firmware of the voting terminal necessarily holds a copy of the digital keys used to protect the removable media. A successful attack against the terminal compromises those keys that an attacker can use to produce forged, compromised removable media cards. This situation is analogous to one where a person always hides a physical key under the doormat – knowing where the key is hidden defeats the purpose of having a lock. The trust in the whole

[3]SHS FIPS 180-3 (Federal Information Processing Standard), National Institute of Standards and Technology `http://www.nist.gov/cgi-bin/view_pub.cgi?pub_id=901372`

[4]AES FIPS-197, National Institute of Standards and Technology, `http://csrc.nist.gov/publications/PubsFIPS.html`

[5]Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach: Analysis of an Electronic Voting System. IEEE Symposium on Security and Privacy, pp 27-42, 2004.

[6]DSA FIPS 186-3, National Institute of Standards and Technology, `http://csrc.nist.gov/publications/PubsFIPS.html`

[7]Aggelos Kiayias, Laurent Michel, Alex Russell, Alexander A. Shvartsman, Integrity vulnerabilities in the Diebold TSX Voting Terminal, 2007. VoTeR Center, Technical Report. `http://voter.engr.uconn.edu/voter/2007/07/integrity-vulnerabilities-in-the-diebold-tsx-voting-terminal/`

system depends on the vendor diligence in its engineering practices to produce firmware that make extensive and complete use of cryptographic techniques, on the vendor's dedication at safe-keeping all the digital keys, and with election officials to secure the voting terminals between elections.

57. The above suggest that the evaluation of electronic voting systems is a sophisticated process that goes beyond the verification of employment of standardized cryptographic mechanisms or adherence to prescribed styles of using such mechanisms. Given that there are no standards that can ensure correct and sufficient application of cryptographic techniques, it is necessary to carry out the evaluation of such equipment by expert security researchers to ascertain the security and resiliency of electronic voting equipment against attacks. It is important that such security evaluation results in publicly disclosed reports that fully detail the research methodology employed. Furthermore such reports would preferably be vetted via academic peer reviewing procedures. The bottom line is that while cryptographic techniques are highly relevant and useful tools, it is equally important that the tools are used appropriately.

Specific Vulnerabilities Pertaining to Optical Scan Voting Terminals

58. The functions of the voting terminal are controlled by firmware, including ballot processing, vote tallying, and tally reporting. Therefore, correctness is of paramount importance in assuring integrity of an overall election.

59. Most voting terminals, as most software-based systems, are designed to be "upgradable" (in whole or in part) with new firmware versions through simple procedures where the new firmware is installed via a removable media. Any installation of new firmware results in essentially a new voting terminal whose functions may be completely different from the functions that existed prior to installation. Such installation must be viewed as completely invaliding any prior certification. Note that the existing firmware is responsible for validating the new firmware before installing it. This implies that the only entity in a position to certify that authorized firmware is installed is the vendor itself. If the validation itself is partial, or too weak, unauthorized firmware can slip through, be installed and take over the control of the entire machine (including every subsequent upgrade). Therefore, the trust in the whole system entirely rests on the vendor.

60. Vendors can use cryptographic techniques and digital keys to sign the new firmware. The old firmware is then responsible for checking the digital signature of the new firmware before installing it. These methods can minimize the risk of installing unauthorized firmware.

61. One Achilles' heel in using cryptographic techniques to protect against unauthorized firmware upgrade is that their effectiveness depends on the safe-guarding of the digital keys. If the vendor keys are exposed at any point, adversaries can impersonate the vendor and produce malicious firmware that appears legitimate. Once again, the trust in the whole system rests entirely on the vendor.

62. The removable media cards are used both for holding the description of the election (digital model of the ballot) and for holding the counters. Once a card is programmed on the election management system it is shipped to election officials to be inserted into the voting terminal where it stays for the duration of the election before being shipped back for aggregating the results (where central tabulation is used). The integrity of the card during the entire process is critical to the integrity of the election.

63. If the card can be tampered with while in transit to the precinct election officials, the entire system can be compromised. The election description can be made inconsistent with the paper ballot *leading to an incorrect interpretation* of the votes and therefore incorrect tallying. Malware can be copied onto the card and can be automatically installed when the media is inserted into the voting terminal. The malware can interfere with the firmware prior to and/or during the election to perturb the tallying. Worse, once the "infected" card returns to the election management system for aggregation, it can deliver its payload to EMS and compromise *all the media cards subsequently inserted* affecting the process on a much larger scale.[8]

[8] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine, September 13, 2006, http://citp.princeton.edu/pub/ts06full.pdf .

64. If the card can be tampered with while in transit after the election back to the election management system, the tallies it holds can be modified and malware can be injected as well leading to the same large scale impacts, in the extreme case causing incorrect election results to be reported. Thus it is imperative that any electronic voting system considered for deployment is evaluated by domain experts as a complete distributed system, and not only as a collection of standalone components.

65. The use of cryptographic techniques can increase the integrity of the electoral processes supported by electronic systems and make tampering more difficult. However inadequate, incomplete or incorrect uses of cryptography, and less-than-diligent or poorly designed management of cryptographic keys creates vulnerabilities and leads to a false sense of security.

66. Lastly, it is important to reiterate that it is critical and imperative to establish and enforce a suitable and secure chain of custody protocols to minimize the risks of attacks or interference that can range from a simple denial of service (e.g., benign voting terminal malfunction or card destruction) to an elaborate tampering scheme designed to compromise elections in multiple precincts. The chain of custody policy must consider, for example, whether it is permissible for the voting equipment and removable media to be transported by a common carrier, and how to properly store the equipment while it is not in use between elections.

Specific Election Management System (EMS) Vulnerabilities Enable Fraud and Error on a Massive Scale

67. New York State Election Law, Rules and Regulations §6209.1(l) defines Election Management Software (EMS), as "the software used by the voting system to describe ballot layout, collect and report election results, and maintain audit trails." The ballot layout definitions are transmitted to individual optical scan machines by means of removable media (e.g., memory cards).

68. The use of software-based voting systems unfortunately enables systematic exploits on a massive scale. As presented throughout this document, the electronic election system is comprised of an election management system (EMS) and programmable electronic voting terminals, it is possible for EMS to transmit, via removable media, malicious or erroneous programming to all voting terminals. In the extreme case, a single compromised voting terminal can be used to tamper with EMS and all voting terminals.

69. In general a precinct-count optical scan voting system, such as the type New York plans to use, consists of an Election Management System (EMS) contained in a central computer and a number of Optical Scan Voting Terminals, referred to herein as optical scanners or optical scan voting machines. The terminals are the optical scan computers on which voters cast their ballots at the poll site.

70. The EMS computer programs all the optical scanners by loading software into each voting computer before every election using a memory card that tells the scanner who is on the ballot and how to count the votes, thereby repeatedly exposing the election results to undetectable outcome-determinative exploits:

> "[F]unctionality — 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."[9]

71. While the election officials in New York may be responsible for the ballot programming of the EMS computer, the operation of the software inside the EMS computer is not observable to them. The database software where the votes are allocated to the candidates can be exploited to reallocate the votes or to cause the scanner to do so during the election.

[9] Harry Hursti, supra Security Alert: July 4, 2005, Critical Security Issues with Diebold Optical Scan Design, Black Box Voting. http://blackboxvoting.org/BBVreport.pdf.

72. A compromised or simply "broken" EMS computer could alter the programming of every optical scanner in a jurisdiction notwithstanding New York's "closed network." No transmission of data via the Internet, radio waves or other wireless means would be necessary to commit wide-scale fraud via the removable memory cards.

73. These observations were among the reasons why in the State of Connecticut a state-wide pre-election (as well as post-election) audit of removable memory cards is conducted for each major election on the request of the Office of the Secretary of the State. This audit, designed, implemented and performed by the UConn VoTeR Center mitigates the risks described herein and addresses some of the weaknesses introduced in elections by the adoption of software-based technology.

74. For the pre-election audit, each district (precinct) in Connecticut randomly chooses one out of the four removable cards in their possession and submits it to the VoTeR Center for audit. The contents of the cards are then faithfully extracted (without relying on any vendor-supplied audit tools) and compared with the intended contents; this portion of the audit process is semi-automated. Any discrepancies or deviations are then logged and analyzed. Specifically, the memory cards are audited for any irregularities in the ballot data/layout, any deviations in the executable code, the state of the counters, and the content of the audit logs. These audit logs contain significant events in the life of a card since the last time it was formatted. The report is then generated for the Secretary of the State.

75. We note that while it is feasible to perform such an audit for the state the size of Connecticut that uses relatively simple optical scan tabulators, performing such an audit in a substantially larger state that uses multiple, significantly more complicated optical scan tabulators may be impractical.

76. It is important to stress that the electronic voting machines chosen for deployment in the State of New York, i.e., the ES&S and Dominion systems, are substantially more complex than the Premier AccuVote system used in the State of Connecticut. Upon information and belief, the size of the software/firmware in both the ES&S and Dominion systems is measured in tens of millions of bytes. By comparison the corresponding size of Premier system is only 128 thousands of bytes, thus the software in the systems chosen for New York are about 100 times larger. While in Connecticut we have substantially analyzed the code through manual inspection, it will not be practical to perform the same examination for ES&S and Dominion systems. Additionally, the size of the removable media in the Premier system is also about 128 thousands of bytes, while the size of the removable media in the ES&S system is one thousand millions of bytes and the size of the removable media in the Dominion system is five hundred millions of bytes. All of this makes the analysis of data and executable code in the ES&S and Dominion systems, including the removable media, substantially more difficult or even unfeasible.

77. Conducting post-election hand counted audits is an additional remedy, however limited audits planned in New York State leave a window open to fraud and error in a small number of precincts whose effect on the outcome in a close election should not be underestimated.

Using Election Management Systems (EMS) for Central Aggregation Introduces Additional Vulnerabilities

78. The final and significant vulnerability associated with the use electronic voting systems is associated with using the Election Management System (EMS) in aggregating tallies from individual precincts. In the last stage of electronic canvassing the results from individual precincts are conveyed and entered into EMS by variety of means: reading the data from removable storage devices from electronic voting machines or transmitting the data from electronic machines via telephone lines or through a network. The precinct-level data is then aggregated to produce final tallies for the contests in specific jurisdictions.

79. The initial vulnerabilities in this context stem from the challenges associated with accurately and without loss conveying the data from the precinct electronic voting machines to EMS, whether it is done by physically moving the removable storage devices from precincts and connecting them to EMS for read-out, or by electronically transporting the data over communication lines to EMS. Strict chain-of-custody procedures must be in place to

mitigate the possibilities of fraud and errors when the precinct storage devices are physically conveyed to the EMS site. When the precinct level data is conveyed over telephone or data networks there are possibilities for denial-of-service attacks or outright malicious tampering with transmitted data.

80. The next significant vulnerability is associated with relying on EMS to perform central tabulation. Recall that EMS software is normally installed on general purpose computers and it is beyond the state-of-the-art to be able to reason about the correctness of the substantial amount of software in EMS system and its computing environment. As discussed earlier, certification, testing, self-testing, and self-audits can only create a false sense of security. For example, a Premier advisory note alerted EMS uses that precinct memory card data uploads can be flagged as successful when in fact upload of data failed (ironically, the vendor stated that this may in some cases be due to a conflict with anti-virus software running on the EMS computer).[10]

81. The use of EMS in aggregating precinct election results presents a single point of failure. A single tampered precinct removable storage device may taint the entire result and malicious software (viruses) may be injected into EMS from compromised removable storage. The same risks exist when using telephone or data networks to convey precinct data to EMS. Errors and malicious software can infect EMS, rendering any claimed (by EMS) election outcomes meaningless. Note also that a single individual may be able to tamper with EMS and consequently with the election results.

82. In closing the presentation of vulnerabilities in using EMS for tally aggregation I note that because of the associated risks the State of Connecticut does not use central tabulation of precinct-level results using EMS. We completely support this decision to avoid using EMS for aggregation. I realize that larger states will want to resort to central tabulation and assume the associated risks, however I advise strongly against doing so given that it is extremely difficult to guarantee that such systems contain no errors and are not prone to malicious interference.

Printed Ballots Enable Voter-Verified Audit Trail (VVAT) but also Introduce Vulnerabilities and Create the Possibility of not Recognizing Voter Intent

83. A very important criterion in assessing voting technology is the provision of the Voter Verified Audit Trail (VVAT), that is a physical copy, for example, a paper record, of the actual vote that the voter verified before it was cast. VVAT is sometimes referred to as the Voter Verified Paper Ballot (VVPB). For the optical scan terminals this is the actual ballot sheet and this is on obvious advantage of optical scan systems over the DRE (Direct Recording Electronic) systems, where no voter-marked ballot is produced (the DRE terminal may produce a printed record, but it is problematic to accept such records as voter-verified, moreover, the DRE terminal may mistakenly print incorrect ballots or multiple copies of ballots). However the optical scan election systems utilizing printed ballots are not without concerns.

84. Paper ballots must be printed very precisely to avoid possible issues during the election. The first is the geometry of the ballot that must satisfy the optical scanner's requirements for, e.g., dimensions, timing marks, positioning of the bubbles on the ballot, thickness and color of bubble outlines. Deviations from the requirements may yield unintentional over-votes and under-votes, and outright rejection of ballots.

85. Even if the ballots are printed according to the optical scan specifications, there is a very real problem of ensuring the match between the ballot definition produced using EMS and conveyed to the optical scan via removable media and the printed ballot itself. If, for example, two candidates' names are switched in a certain race – whether due to EMS programming error or the printed ballot error – the votes for the candidates will be switched. This can be remedied to some extent by running a specially designed deck of ballots during pre-election testing. However there is the possibility that erroneously programmed, or maliciously altered, removable storage device or optical scan programming would mask the problem until the actual election time.

[10] PREMIER ELECTION SOLUTIONS. Product Advisory Notice, GEMS versions 1.20.2 and earlier, Revision: 1.0 Date: 08-19-2008.

86. The accurate tabulation of the votes cast by the voters depends on voter education and correct marking of the ballots by the voters. Optical scan systems can only record the votes where the appropriate bubbles are substantially marked by the voters. Optical scanners will not record votes in the cases where the voter intent is clear, but not properly marked on the ballots, for example, circling a bubble or underlining candidate's name will not be recognized as votes.

Numerous Successful Attacks against Voting Terminals have been Documented

General Issues in Attacking Voting System Vulnerabilities

87. Vulnerabilities are latent opportunities for adversaries who desire to interfere with the electoral process and its results. The aforementioned vulnerabilties are not mere hypotheticals and many actual attacks exploiting these vulnerabilities have been demonstrated, documented, published and are discussed below.

88. Attacks against computerized systems are particularly devastating given that they are covert. To a casual observer, a compromised voting terminal looks and operates normally which renders all traditional monitoring and inspection methods completely useless.

89. Additionally, the compromised firmware can be programmed by its attacker to lay dormant for an extended period of time before delivering its payload (altering results of a specific election). Consequently, it is not sufficient to ensure the physical integrity of the voting terminal from the moment it is configured with an actual election, but instead, its integrity should be ensured from the moment the equipment is purchased. This was recognized by Wallach:[11]

> "At any point in a voting machines life, from the manufacturers shipping dock through intermediate storage to the day of the election, a voting machine could potentially be reprogrammed to report incorrect results."

The assurance of an unbroken chain of custody extends to a much longer time period when compared to mechanical device which can be inspected for tampering right before an election.

90. Perhaps even more worrisome, given that a computerized election process is a large distributed system, an attack against a single machine has the potential of compromising the central election management system (e.g., during the tabulation process) and therefore impact a large number of votes. This was recognized in the Source code review for the Diebold system in 2007 in a report to the California Secretary of State[12]

> "An attack could plausibly be accomplished by a single skilled individual with temporary access to a single voting machine. The damage could be extensive malicious code could spread to every voting machine in polling places and to county election servers."

91. Only a detailed, lengthly and costly forensic analysis carried out by experts in security and computer science can possibly expose the attack. Yet, it is critical to realize that these systems use rewritable memory and media, therefore malware (malicious software) infecting a machine has the ability to completely cover its track and remove itself from the compromised system after delivering its payload. In those cases, it is impossible to discover the true source of the attack and a manual and complete recount of the paper ballot is the sole option to recover the true outcome of the voting process.

[11] Dan S. Wallach, Testimony to National Institute of Standards and Technology and Election Assistance Commission Technical Guidelines Development Committee, September 20, 2004, `http://www.cs.rice.edu/~dwallach/pub/eac-tgdc-20sep2004.pdf`

[12] California Secretary of State, Source Code Review of the Diebold Voting System, July 20, 2007 `http://www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf`

Successful Attacks have been Developed

92. In the Blackbox report[13], computer scientist Harri Hursti demonstrates how the EMS could be easily subverted so as to

> "[M]odify the election results reports so that they do not match actual vote data .... produce false optical scan reports to facilitate checks and balances .... [and] mimic votes from many precincts at once while transmitting votes to the central tabulator."

This attack exploits the absence of cryptographic protection on the removable media card to stuff the initial tallies and bias the outcome. The attack also modifies the part of the firmware residing on the removable media to conceal the stuffing of the counters and subvert the zero-count report printing. The attack was carried out on a Diebold AccuVote terminal. It was filmed and featured by HBO as part of a documentary called *Hacking Democracy*.

93. Two studies published in 2006 and 2007[14, 15] successfully validated the Hursti attack and developed new attacks. The first report confirmed that the memory cards used in optical scanners contain executable code which can be manipulated to forge false reports showing that the counters *appear to be set to zero* prior to the start of an election. The first attack effectively exploited the removable media vulnerabilities of the AccuVote terminal *even without removing it from the terminal and only using the terminal serial port* to change the election description and the ballot layout. The attack is effectively capable of swapping the votes of two candidates, neutralizing votes or selectively shifting a subset of votes from one candidate to another.

94. The same report also demonstrates how to recover the "PIN" code which supposedly prevents unauthorized access to the sensitive administrative function of the terminal.

95. A subsequent report[16] strengthens the previous attacks by altering the firmware residing on the memory card to make the changes undetectable to pre-audit procedures thereby substantially increasing the seriousness of the attack.

96. In July 2007, a report commissioned by Florida's Secretary of State demonstrated how, with only a brief access to an optical scan tabulator, one individual can replace a memory card with one preprogrammed to read one candidate's votes as counting for another. "The attack can be carried out with a reasonably low probability of detection."[17] The study detailed how an optical scanner could be subverted to compromise election results without detection.

97. In December 2007, the EVEREST report[18] was delivered to the Ohio Secretary of the State. Two groups of teams contributed to the report which provides an analysis of systems (both Direct Recording systems and Optical Scan systems) from Premier (formely Diebold), ES&S and Hart Intercivic voting systems. The assessment conducted by MicroSolved, Inc. (an Ohio security firm) had access to the complete system and source code and was tasked with a penetration testing. They produced a "grade" for each system measuring their compliance with a baseline level of safety (a perfect grade is 12/12) covering physical integrity, networking integrity for the voting terminal, memory cards and EMS systems. The three vendors scored (respectively) 0/12, 1/12 and 0/12. They conclude

[13] Hursti, `http://www.blackboxvoting.org/BBVreport.pdf`

[14] Univ. of Connecticut Voting Technology Research Center, Security Assessment of the Diebold Optical Scan Voting Terminal, October 30, 2006 `http://voter.engr.uconn.edu/voter/Report-OS_files/uconn_report-os.pdf`

[15] KIAYIAS, A., MICHEL, L., RUSSELL, A., SHASHIDAR, N., SEE, A., AND SHVARTSMAN, A. An authentication and ballot layout attack against an optical scan voting terminal. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop (EVT'07)* (August 2007).

[16] KIAYIAS, A., MICHEL, L., RUSSELL, A., SHASHIDHAR, N., SEE, A., SHVARTSMAN, A. A., AND DAVTYAN, S. Tampering with special purpose trusted computing devices: A case study in optical scan e-voting. In *Proceedings of the 23rd Annual Computer Security Applications Conference (ACSAC 2007), December 10-14, 2007, Miami Beach, Florida, USA* (2007), pp. 30–39.

[17] Florida Dept. of State, Security and Assurance in Information Technology Laboratory (SAIT) Software Review and Security Analysis of the Diebold Voting Machine Software, July 27, 2007 available at `http://election.dos.state.fl.us/pdf/SAITreport.pdf`

[18] P. MCDANIEL, M. B., AND VIGNA, G. EVEREST: Evaluation and validation of election-related equipment, standards and testing, December 2007.

that all systems suffer from critical security failures. They highlight "pervasive mis-application of security technology," including failure to follow "standard and well-known practices for the use of cryptography, key and password management, and security hardware" as well as a "a visible lack of trustworthy auditing capability".

98. The EVEREST report corroborates the accepted idea that the vendors should not limit themselves to *use of good technology* but instead focus on *a good use of technology* starting with best practices in software engineering to prevent buffer overflows and low code quality. They also recommend the adoption of anti-virus and firewall software. Finally, the report insists on the importance for the vendor to

> "Undertake a systemic approach to mitigating the identified vulnerabilities in the system. [...] Each issue mitigated by the vendor greatly reduces the amount of risk management that must be transferred to the counties by policy and process control."

99. The same EVEREST report also offers an assessment by a "red-team" composed of University Research teams. Their extensive report (316 pages) ends with the following four critical failures in design and implementation of all three voting systems.

    1. Insufficient security where the voting systems uniformly failed to adequately address important threats against election data and processes.
    2. All the voting systems allow the "pervasive mis-application of security technology" and demonstrate an inability from all vendors to follow the best practices in cryptography and key and credentials management.
    3. None of the voting systems display a trustworthy auditing capability preventing auditors from discovering or recovering from security attacks
    4. The software maintenance procedures are deeply flawed in all cases and are leading to "fragile software in which exploitable crashes, lockups, and failures are common in normal use".

100. In 2008, A "red-team" (a team without access to the source code of the equipment or any support from the vendor) was comissioned by the California Secretary of the State to conduct an in-depth analysis of optical voting terminals[19] and the ES&S Unity 3.0.1.1 Voting System in particular. They designed several attacks carrying out ballot stuffing on the M100, election result modification on the M650, forging the audit logs after compromising the EMS, audio ballots modification for the AutoMARK to name just a few. Overall, the report provides more than a dozen attacks exploiting vulnerabilities in the cryptographic level, the removal media, the EMS or the voting terminal.

101. In 2006 a special transit bond election in Arizona's Pima County was conducted using electronic voting and EMS systems and it yielded controversial results[20]. Although as of this writing we are not aware of the final, if any, resolution, there is strong evidence that not all went right in that election. Rather than delving into the legal issues surrounding that election, we point out that from the technological standpoint, the alleged "rigging" of the election is entirely plausible, and without tremendous difficulty. We enumerate selected technical observations. (i.) An obscure device (Cropscan reader/writer) was obtained, whose only known purpose in conjunction with electronic election is to directly read and reprogram Premier's AccuVote Optical scan memory cards, bypassing the Election Management System (GEMS). (ii.) An unusually large number of optical scanner failed during the election, suggesting that programs on the memory cards were incorrectly changed. (iii.) Circumstantial evidence suggests that GEMS database was manipulated by means other than GEMS itself, i.e., by using direct access to the database that likely permits alterations. Our point here is not to deliberate whether or not election fraud was committed in Pima County, but to confirm in the positive that the alleged fraud is enabled by the (imperfect) technology provided by the election system vendor and by the technology in the public domain.

102. We also point out that "less-than-correct" software is not only vulnerable to malicious attacks, but also leads to outright failures of voting equipment. In 2009, in New York 23^{rd} congressional district, the repeated failures of

[19] JACOB D. STAUFFER, F. C. M. G. F. R. T. P. M. Red team testing of the ES&S unity 3.0.1.1 voting system. February 15 2008.

[20] William J. Risner, Esq., Letter to Arizona Attorney General Terry Goddard, February 18, 2009. `http://electiondefensealliance.org/Risner_Letter_to_Goddard`

voting terminal (amounting to a denial-of-service as the scanners were stalling/crashing) cast doubts about the results of the races and lead some observers to allege that the voting terminals had been infected by viruses. In reality, the machines were suffering from crashes resulting from buffer-overflows in the software controlling the scanner. The problem had been identified before hand, but the procedures deployed to upgrade the machines failed and several terminals were not upgraded. While this case does not result from actual foul-play, it highlights the dangers associated with the unobservable opeartion of voting equipment (observers could not assert whether something was amiss with the software buried inside the machine) and illustrates the mayhem that can ensue even under the mildest form of systemic failure.

The Limitations of Certification and Testing

103. New York State has attempted to deal with the lack of transparency and inherent risks of software-based systems by employing a more rigorous certification process than is required by the federal government.

104. However, certification of electronic voting systems can only provide a false sense of security. There does not exist a testing and certification process that, per New York Election Law §7-202(1.r), can "ensure the integrity and security of the voting machine or system by: (i) being capable of conducting both pre-election and post-election testing of the logic and accuracy of the machine or system that demonstrates an accurate tally when a known quantity of votes is entered into each machine; and (ii) providing a means by which a malfunctioning voting machine or system shall secure any votes already cast on such machine or system."

105. The fact is that for any non-trivial software system one cannot establish correctness and integrity through testing. Testing cannot be complete and it can only reveal the presence of errors or "bugs" – it cannot ascertain that the software system is correct and contains no flaws.

> "[R]egardless of whether the software [...] is improved to better resist attacks, bugs will always occur and the risk of tampering cannot be overcome. In particular [...] while 'logic-and-accuracy testing' can sometimes detect flaws, it will never be comprehensive; important flaws will always escape any amount of testing."[21]

106. Optical scan and EMS software consists of hundreds of thousands of lines of code (and this does not include substantial software in the underlying operating system). Software is tested by subjecting it to several possible scenarios. This means that when testing does not find errors in a necessarily limited set of scenarios, it does not prove that the system is correct.

107. This underlines one inherent flaw in the logic and accuracy testing typically used to test optical scan machines prior to an election. These tests only prove the absence of error or tampering during the pre-election test, and for specific set(s) of ballots that are run through the scanner. Such testing can not detect the presence of error and does not prove that there are no errors and it cannot demonstrate that the voting system will accurately count votes or that tampering, which could ensue at that conclusion of the passed tests or be programmed to avoid these tests, does not exist.

108. Another flaw in relying on the self-test features provided by any software system is that one can never trust software to test or audit itself (cf. relying on a corporate entity to perform self-audit). Independent testing and certification addresses only a part of this concern, for testing, as we are discussing, cannot guarantee correctness.

109. It is important to reiterate that in the current state-of-the-art in software verification it is unfeasible to prove correctness of any non-trivial software system, even upon a deep analysis by most qualified experts.

[21] Dan S. Wallach, Testimony to National Institute of Standards and Technology and Election Assistance Commission Technical Guidelines Development Committee, September 20, 2004, available at `http://www.cs.rice.edu/~dwallach/pub/eac-tgdc-20sep2004.pdf`.

110. In November 2006, scientists at the National Institute of Standards and Technology (NIST), the agency that writes the federal voting system standards to which New York adheres, and advises the United State Election Assistance Commission, found that unless a software system was built to be secure and reliable to begin with, "experience in testing software and systems has shown that testing to high degrees of security and reliability is from a practical perspective not possible"[22] and therefore testing of software-based voting systems cannot guarantee accurate and reliable election results.

111. A "certified" software-based voting machine can still be programmed to alter itself before, during, and after the election or can be subsequently manipulated with no ability for election officials or observers to perceive that the voting system has been compromised:

> "This is a classic computer security problem. Whoever gets into the machine first wins. So if the Trojan horse software is in there first, you ask it to test itself – it will always lie to you and tell you everything is fine. And no matter what testing code you try to add after the fact, it's too late."[23]

112. Malicious coding can evade certification testing; the testing cannot guarantee to reveal that the code has been compromised. A certified software-driven voting system can be programmed to give the false appearance that it is in proper working order, when in fact it has been compromised; the boards of elections and election officials responsible for ensuring the accuracy and integrity of the election results will have no way to know that the indicated totals do not correspond to the votes cast, thus no way to confirm the outcome of an election.

113. In February 2006, a report commissioned by Californias Secretary of State found that a certified compromised optical scanner would produce results that election officials and voters would not recognize as false:

> "There would be no way to know that any of these attacks occurred; the canvass procedure would not detect any anomalies, and would just produce incorrect results. The only way to detect and correct the problem would be by recount of the original paper ballots."[24]

114. Taking an example from our own work, we have performed security analysis of the Premier optical scan terminal that was previously tested by an independent agency. We have identified several security and integrity issues[25] [26] in this terminal that were not identified in the 266 page report[27] published by the agency.

115. It is important to stress that testing and certification approaches that may be successful with immutable, closed-system mechanical devices may not be effective with mutable, flexibly modifiable software systems. The pre-election testing and certification processes that can predict with a high degree of certainty the election-day operation of a static mechanical lever voting system, precisely because its functions are visible, immutable and finite, cannot be used to predict the operation of mutable software-driven voting systems:

> "The current certification process may have been appropriate when a 900 lb lever voting machine was deployed. The machine could be tested every which way, and if it met the criteria, it could be certified because it was not likely to change. But software is different. The software lifecycle is

---

[22] National Institute of Standards and Technology report on computerized voting systems, `http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf`.

[23] Dan Wallach, Rice University computer security expert has examined electronic voting systems since 2001. The quote is from *Peering through the chinks in the armor of high-tech elections*, May 27, 2007 `http://www.votersunite.org/info/PeeringThruChinks.asp`.

[24] California Voting Systems Technology Assessment Advisory Board (VSTAAB), Security Analysis of the Diebold AccuBasic Interpreter. February 14, 2006 available at `http://ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf` (confirming the findings of Hursti 2005, infra)

[25] KIAYIAS, A., MICHEL, L., RUSSELL, A., SHASHIDAR, N., SEE, A., AND SHVARTSMAN, A. An authentication and ballot layout attack against an optical scan voting terminal. In *Proceedings of the USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 07)* (August 2007).

[26] SEDA DAVTYAN, SOTIRIS KENTROS, AGGELOS KIAYIAS, LAURENT D. MICHEL, NICOLAS C. NICOLAOU, ALEXANDER RUSSELL, ANDREW SEE, NARASIMHA SHASHIDHAR, ALEXANDER A. SHVARTSMAN: Taking total control of voting systems: firmware manipulations on an optical scan voting terminal. 2009 ACM Symposium on Applied Computing (SAC), pp. 2049–2053, 2009.

[27] WYLE LABORATORIES, Hardware qualification testing of the Diebold Election Systems AccuVote Optical Scan Model D precinct ballot counter. Report No. 48619-09, 266 pages, August 4, 2005.

dynamic ... [Y]ou cannot certify an electronic voting machine the way you certify a lever machine ... [W]e absolutely expect that vulnerabilities will be discovered all the time..." [28]

116. Lastly, software systems are perpetually revised, extended and corrected. Each change, in principle, must trigger a complete new regression test, test of the changed or corrected functionality, and complete re-certification.

> "Software is designed to be upgraded, and patch management systems are the norm. A certification system that requires freezing a version in stone is doomed to failure because of the inherent nature of software."[29]

Hand-Counted Audits and Limitations

117. Acknowledging the risks associated with deployment of electronic voting systems in elections, several states mandate that post-election audits are to be performed, where a fraction of the total number of precincts is subject to an audit where the ballots marked by the voters are hand counted and these hand counts are then contrasted with the counts reported by electronic voting terminals. For example, in the State of Connecticut, there is a 10% audit, in which the Secretary of the State randomly draws 10% of the voting districts (precincts), where all ballots cast in the specified contests are hand counted (§9-320f of the General Statutes).

118. Conducting post-election hand counted audits is indeed a valuable remedy in the face of the risks of fraud and error associated with the use electronic voting systems. However, limited audits planned in New York State leave a window open to fraud and error in a small number of precincts whose effect on the outcome in a close election should not be underestimated.

119. A 3% audit rate (as suggested by the New York State Election Law. §9-211) can be expected to reveal massive inconsistencies: So long as the total population of voting machines is more than, say, 250, it is reasonable to expect a 3% audit rate to uncover massive inconsistencies. In particular, if $1/2$ of all voting terminals suffer from a detectable inconsistency, a 3% audit rate will reveal at least one problem with over 99% probability.

120. A 3% audit rate may leave undetected tampering or malfunction of a substantial percentage of voting equipment. For example, when a 3% audit is applied to a total of, say, 250 voting machines, the audit will be oblivious to security breaches in as many as 50 polling places with probability more than 18%. This suggests that 20% (50 out of 250) manipulation of election results is feasible in such setting with non-trivial (18%) probability of being undetected. In particular, given the low possibility of detection, a determined attacker may be successful every sixth election in affecting 20% of the machines (this is approximated by taking 18% and multiplying this times 6 to obtain high probability of success).

121. A 3% audit rate cannot be expected to reveal local inconsistencies: For a total number of, say, 250 voting machines, a 3% audit will overlook an inconsistency in a particular set of 3 voting machines with over 90% probability. As an example, if a precinct had a total of three voting terminals, each of which have been tampered with, this would go undetected 90% of the time (by a 3% audit). In such a case, systematic inconsistencies affecting every machine in a single precinct would go undetected.

122. A 3% audit may in fact in some cases confirm with high certainty election outcomes where the margin of victory is substantial, for example in federal elections with a margin over 10% and state election with a margin over 20%. However, for close election, e.g., where the margin of victory is 5% or lower, a 3% audit may confirm the outcome with only 30% or lower, in the sense "of finding at least one Election District containing miscounted votes if the winner of the contest were incorrectly reported" by an electronic voting system. [30]

---

[28] AVI RUBIN, (Professor of Computer Science at Johns Hopkins Univ.) Secretary Bowen's Clever Insight, August 7, 2007, http://avi-rubin.blogspot.com/2007/08/secretary-bowens-clever-insight.html

[29] Ibid.

[30] Howard Stanislevic. New Yorks 3% Post-Election Audit Will Not Provide Confidence in Election Outcomes Reported By Optical Scan Voting Systems, Feb. 16. 2010, http://e-voter.blogspot.com.

123. Therefore, a 3% hand-counted audit must be viewed as an important, but necessarily partial measure, in safe-guarding the integrity of the electoral process. While such an audit can increase one's confidence in that no massive fraud or failure occurred in an election, it has only a modest value in serving to endorse an election outcome.

New York State Election Law is Difficult to Enforce in a Meaningful Way

124. The New York State Election Law, and Rules and Regulations dealing with electronic voting systems contain several articles that are difficult to impossible to enforce or guarantee given the currently available electronic systems. In particular, it may become necessary for Board of Election officials to delegate some of their duties to equipment vendors, their technicians and representatives. We enumerate several important examples.

125. §7-206 provides for testing of voting and ballot counting machines: "The state board of elections shall test every voting machine [...] to insure that each such machine functions properly before such machines may be used in any election in this state." Given the state of the electronic voting technology, substantial expertise is required to perform such tests and to be reasonably convinced that a machine functions properly. In the absence of such expertise the Board of Elections may need to rely solely on the self-assurance tests provided by the vendors of the equipment. Accepting positive results of such self-tests in essence delegates the responsibility for testing to the vendor. Furthermore, given the critical nature of the application, accepting such test results is problematic as testing in good engineering practice is never performed by the developers of the system.

126. The testing that needs to be performed according to the law by board of elections personnel must include "a verification of the authenticity and integrity of the resident vote tabulation programming in open, encrypted, compiled, assembled, or any other form, in each voting machine of such types, by comparison of such resident vote tabulation programming with the programming which was in the machine of such type which was approved for use in this state." This formulation requires the board of elections to be responsible for testing that requires substantial specialized expertise. If the board resorts to equipment self-testing, the results are not necessarily trustworthy. In any case, the board would be delegating in essence such testing to the vendor(s). Also note that self-testing may or not be able reveal errors or malicious programming that is designed to be activated only on election day.

127. §7-207 defines the preparation of voting machines. In particular: "It shall be the duty of the board of elections [...] to examine all voting machines and all such electronic or computerized devices before they are sent out to the different polling places, to see that all the registering counters are set at zero..." In the absence of an in-depth technical pre-election examination of the machines in question, the board of elections must accept the display of a zero as the value of a counter as fact. At the same time erroneous or maliciously modified software may cause zero to be displayed or printed, which bears no impact on where machine counting is started and how the counting is performed on election day. Thus again, the board is charged with responsibility that it cannot carry out without delegating it to vendors or their software and hardware.

128. The examination required of the board of elections by §7-207 also deals with "any removable electronic or computerized device which operates such [voting] machine or records the vote thereon". Again, substantial specialized expertise is required to meaningfully assert the correctness of data on such removable devices and that the election counters stored on such devices are zero. The data on such removable devices is normally in vendor proprietary formats and often encoded or encrypted, in which case it is practically impossible for the board of elections to conclude anything about the true state of the counters. We reiterate that relying on vendor-supplied tools for this purpose is not advised.

129. §3-302 instructs the board of elections to direct "voting machine technicians" in supervising "the preparation of the voting machines." "Voting machine technicians may be full time employees of the board of elections and may also serve as voting machine custodians as hereinafter provided." The technicians "shall inspect voting

machines to insure that they are in proper repair and working order". This is problematic because insuring that the machines are functioning correctly requires substantial specialized expertise, and it is unlikely that board of elections will be able to hire suitably prepared technicians. Thus the technicians that may be available to perform such tasks will be able to carry out the required tasks only on a superficial level, again relying on the tools provided by the vendors. Given the critical nature of election systems, adhering to the law in this case is extremely difficult or even impossible on a broad scale.

130. Lastly we comment on a certain difficulty in certifying and testing electronic voting equipment. This difficulty has to do with the fact that an electronic voting machine is not a closed system with fixed and immutable behavior. The behavior of an electronic voting machine depends in part on the contents of the removable memory devices that are prepared before each election and inserted into the machine for each election. Given that removable storage devices used with election machines contain or can contain executable code, the behavior of the machine after the insertion of such devices may be radically different than what is desired. Certifying an electronic voting machine does not guarantee that the machine will operate correctly when faulty or maliciously altered removable memory device is inserted.

131. Consider New Your State Board of Elections Rules and Regulations §6209.4 dealing with application process for vendors of voting equipment. Paragraph 6209.4(h.3) requires vendors to affirm that "the submitted voting system's software does not contain any code, procedures or other material (including but not limited to 'viruses', 'worms', 'time bombs', and 'drop dead' devices that may cause the voting system to cease functioning at a future time), which may disable, damage, disarm or otherwise affect the proper operation of the voting system..." Affirming and verifying that this requirement is satisfied can only create a false sense of security. Even if a voting machine is free from such harmful software, there exists the possibility that malicious or erroneous software may be injected into the machine by means of removable memory devices. In fact such vulnerabilities were shown to exist in a number of research studies as we already discussed.

132. In summary, even under the most diligent application of New York Election Law, and Rules and Regulations, there will exist opportunities for errors in, and malicious tampering with elections that are created solely due to the premature deployment of immature technology.

Concluding Remarks

133. Electronic voting terminals are complex computing devices and optical scan voting terminals are not exceptions. They rely on sophisticated hardware (often off-the-shelf) as well as commodity operating systems and software. An electronic voting solution is not limited to a voting terminal but encompasses several artifacts ranging from an Election Management System to a voting terminal, removable media used for communication, and printed ballots whose content and form must match the digital template stored on the removable media.

134. These complex systems do not operate in a closed environment. Instead, they are used within a context where rules and procedures govern their operation as well as numerous interactions with a variety of actors/agents, including election officials, vendors, and voters. Every single component of this electronic system is susceptible to attacks, both external attacks and insider attacks.

135. First and foremost, the very complexity and size of the system precludes any absolute guarantees of security, integrity, correctness, fault-tolerance, and performance. Vendors themselves build upon large and complex systems (e.g., operating systems) built by third parties and with no formal guarantees.

136. Second, the inability to observe the inner workings of the system precludes external observers from achieving their primary mission: indeed, a compromised voting terminal may look, act and operate exactly like a legitimate terminal.

137. Third, voting systems are large, distributed systems, where a single compromised component (whether it is the EMS or a voting terminal) may affect the entire system.

138. Optical scan terminals offer a Voter Verified Audit Trail (VVAT) which, ultimately, is a true asset (and a clear advantage over DRE, Direct Recording Electronic terminals). Yet, consulting the paper trail (a full audit) implies a complete manual recount which defeats the purpose of electronic counting. Optical scan voting terminals, as DRE terminals, have a number of possible penetration points that an attacker may exploit; these include (i.) the end-user upgradeable firmware, (ii.) the removable media used for communicating the election description, communicating the election results, and upgrading the firmware, and (iii.) the election management system (EMS) responsible for configuring the election and digital ballots, conveying this information via removable media to voting terminals, and for the electronic tallying of election results.

139. Electronic voting systems are complex, and to date there is no compelling evidence that any of them have been certified or verified in any scientifically meaningful sense. The vendors are reluctant to release their systems to researchers for in-depth evaluation knowing that problems will be found, and perhaps protecting their intellectual property. (We note that both researchers and vendors need to do better in this regard – it is in constructive cooperation that better election systems will emerge.) Regrettably the fact is that all systems that were seriously evaluated have been shown to have vulnerabilities.

140. All vulnerable systems are susceptible to attacks.[31] The body of literature on the subject offers a pessimistic picture in which various groups (auditing firms and academics) have demonstrated successful attacks that exploit those vulnerabilities. The severity of attacks and the extent of the damage varies, ranging from a mere denial of service and escalating to state-wide election outcome alterations. Clearly, the results can be devastating, shattering the confidence in the system, and prompt drastic recovery measures (e.g., full manual recounts). The use of EMS to program removable media in the absence of technological audits and the employment of automatic aggregation through the EMS are particularly susceptible to exploitation for tampering on a large scale.

141. Technological audits and hand counted audits offer, in principle, a substantial degree of assurance, however, (i.) technological audits are increasingly difficult and costly for complex and distributed electronic election systems, and (ii.) modest hand-counted audits, such as a 3% audit, provide protection mainly against massive failure and fraud and are insufficiently effective against localized instances of tampering and failure.

142. The literature offers many documented cases of attacks conducted by independent groups tasked with testing security, integrity and reliability of electronic election systems from several vendors. All studies reach consistent conclusions. The industry is still in its infancy and offers "solutions" that perform poorly in light of these attacks. The users of the electronic voting technology find themselves in the position where they prematurely adopt immature technology.

143. The electronic voting technology industry as a whole does not seem, at the moment, to address the core issues and embrace the necessary practices that are mandated to deliver higher quality products. Just because a vendor incorporates relevant technology in their products does not guarantee a better product, e.g., mere adoption of cryptographic tools does not imply a secure product. It is far more critical to make good use of the technology *as a whole*.

144. The state of practice in the domain of electronic voting systems is such that the deployment of existing systems requires the participation of domain experts (either vendors themselves or third parties) – the systems are simply not ready for unassisted end-user deployment. This is in stark contrast with existing procedures and expectations in current use of electronic election systems. Consequently, it is extremely difficult (if not impossible) for board of elections officials to carry out their supervisory duties. Instead, the adoption of the current generation of electronic voting technology implicitly causes or explicitly effects the delegation of such duties to the private sector, equipment vendors and their technicians and representatives, and other domain experts.

[31] One occasionally hears about the success of electronic banking as a precedent for electronic voting: "We all use ATM's, right? Why not a voting machine?" Yet in North America the banking industry loses over $4 Billion dollars per year to electronic fraud, representing about 1.5% of relevant revenue. The banking industry accepts the losses as the cost of doing business. (Francois Paget, Financial Fraud and Internet Banking: Threats and Countermeasures. McAfee Avert Labs, 2009. `http://www.mcafee.com/us/local_content/reports/6168rpt_fraud_0409.pdf`)

Credentials of Supporting Authors

Aggelos Kiayias, Ph. D.

145. Aggelos Kiayias received his Ph. D. from the City U. of New York in 2002. He currently holds a position of Associate Professor in the Computer Science & Engineering department at the University of Connecticut.

146. He has authored or coauthored more than 50 archival conference and journal papers as well as book chapters in the area of cryptography and computer security with electronic voting one of the most frequent themes.

147. He is the recipient of an NSF CAREER Award on the topic of copyright protection techniques for digital content, and received Fulbright and Marie Curie fellowships for conducting research related to cryptography and security.

148. In 2010 he served as the co-program chair of the Real-Life Cryptographic protocols and standardization workshop. Currently he is serving as the program chair of the cryptographers' track in the RSA Conference 2011, which is one of the largest expos worldwide for data security and is managed by the RSA company.

149. He is one of the principal investigators in the Center for Voting Technology Research.

Laurent Michel, Ph. D.

150. Laurent Michel received his Ph. D. from Brown University in 1999. He currently holds a position of Associate Professor in the Computer Science & Engineering department at the University of Connecticut.

151. He worked in industry for two years in a major optimization company (Ilog, Inc. now an IBM divison) as project manager for OPLStudio, a leading product in optimization.

152. He has co-authored two books, over 25 book chapters and journal papers and more than 50 conference articles. He is also the recipient of an NSF CAREER Award on Combinatorial Optimization. He is also the lead author of several sophisticated industrial-grade software systems including, NUMERICA, OPL and COMET.

153. Laurent serves on the editorial board of three journals (Math Programming Computation, Constraints, Constraint Programming Letters), has served on many program committee of international conferences as well as evaluation committee for the National Science Foundation.

154. His research interests lie at the intersection between Operation Research, Programming Languages, Artificial Intelligence and Distributed Systems.

155. He is one of the principal investigators in the Center for Voting Technology Research.

Alexander Russell, Ph. D.

156. Alexander Russell received his Ph. D. from the Massachusetts Institute of Technology in 1996. He is currently an Associate Professor in the Department of Computer Science and Engineering at the University of Connecticut.

157. He has authored over 40 archival journal articles and over 50 conference papers, many on the topic of cryptography and security in voting systems. He is the recipient of an NSF CAREER Award on the topic of provably secure cryptography.

158. In 2009, he served on the US Election Assistance Commission's working group on technology in elections.

159. He is one of the principal investigators at the University of Connecticut Center for Voting Technology Research.

Further affiant sayeth naught.

Alexander A Shvartsman

[signature of affiant]

ALEXANDER A. SHVARTSMAN

[typed name of affiant]

23 MOULTON RD, STORRS, CT 06268

[address of affiant]

Subscribed and sworn to before me,
this 19 [day] day of March [month], 2010.

[Notary Seal:]

Melanie R Lovelace

[signature of Notary]

[typed name of Notary]

Melanie R Lovelace
Notary Public, Connecticut
My Commission Expires Jan. 31, 2012

NOTARY PUBLIC My commission expires: _____, 20____.