Pre-Election Testing and Post-Election Audit of Optical Scan Voting Terminal Memory Cards

Seda Davtyan *Sotiris Kentros* *Aggelos Kiayias* *Laurent Michel*
Nicolas Nicolaou *Alexander Russell* *Andrew See* *Narasimha Shashidhar*
Alexander A. Shvartsman
Voting Technology Research Center and Computer Science and Engineering Department
University of Connecticut, Storrs, CT 06269, USA
{seda,skentros,aggelos,ldm,nicolas}@cse.uconn.edu
{acr,andysee,karpoor,aas}@cse.uconn.edu

Abstract

Optical scan electronic voting machines employ software components that are customized for each specific election. Such software components are critical from a security and integrity point of view, as they define ballot layout and outcome reporting facilities. The possibility of these components to be tampered with presents a major concern as incorrect election results may be produced due to either malicious interference or accidental corruption. Erroneous results caused by tampering or corruptions can go unnoticed in the absence of testing and auditing, and the errors may not be detectable by election officials/poll workers using the pre-election testing procedures that rely on the machines themselves. This paper presents an actual auditing process for the AccuVote Optical Scan Voting Terminal (AV-OS) (manufactured by Premier Election Solutions) and the ensuing results from a recent statewide audit, showing that thorough auditing of a large sample of voting hardware, specifically the memory cards that contain custom software components, is both practical and informative. We argue that memory card audits are crucial in providing timely information and maintaining the integrity of the electoral process. To substantiate this claim, we present as part of our results hard evidence of inadequate reliability of certain hardware components used with the voting terminals, and indications of marginal procedural compliance on the part of the poll workers. These audits were performed without any access to the manufacturer's source code or the documentation regarding the design or the internal workings of the AV-OS terminal. We conclude the paper with several observations based on what was learned during the memory card audit process and offer recommendations aimed at enhancing the integrity of elections.

The audits presented in this paper were performed on request of the Office of the Secretary of the State of Connecticut.

1 Introduction

Post election audits are essential to ensure voter confidence in election outcomes. Traditionally, audits (or recounts) are triggered when the vote counts for candidates are very close (one half of one percent in Connecticut) and consist of a manual hand count of ballots. More recently, it has been recommended that audits be performed randomly regardless of any close or disputed elections [15]. In light of the Help America Vote Act (HAVA) [4] requiring the adoption of electronic voting machines, and research indicating security concerns regarding such technologies (e.g., [3, 2, 9, 10, 11, 5, 13, 12, 14, 7, 8]), this paper argues for an audit of the voting machines themselves, specifically the loadable software components, both before and after an election.

We present the process used by the University of Connecticut VoTeR Center (Voting Technology Research Center) to perform the pre-election testing and post-election audits of memory cards for the Accu-Vote Optical Scan (AV-OS) tabulators that were used in the November 2007 Municipal Elections in Connecticut. While the tabulator hardware is identical in all districts using AV-OS systems, custom programming for each district is provided by means of removable memory cards. The process presented in this report includes testing, comparison, and analysis of the data collected during the audit. This paper also briefly outlines the safekeeping steps taken in dealing with the memory cards after receiving them from the districts. These include a strict chain of custody policy with regard to handling the cards, maintaining a log of all transactions and activities, and safekeeping (both physical and electro-magnetic) of the memory cards. In order to enable the audit process, new firmware was developed to speed up the data collection phase, and new (outboard) software was developed to perform analysis and to identify discrepancies in the collected data.

It is important to note that speed is essential for both pre- and post-election audits. Ballots may change up to just a few days before the election, leaving little time to audit the memory cards and address any discovered problems. For post election auditing, speed is also essential as lengthy disputes can directly interfere with governmental continuity.

The paper concludes with several observations based on what was learned during the memory card audit process and offers recommendations aimed at enhancing the integrity of elections. We believe that memory card audits are crucial in providing timely information and maintaining the integrity of the electoral process.

The entire audit, tool development, and re-engineering was conducted by the VoTeR Center without any access to internal vendor documentation for the AV-OS systems, source code, or assistance of any kind.

1.1 Goals of the Memory Card Audit

The VoTeR Center was asked by the Connecticut Secretary of the State (CT SOTS) Office to prepare for and implement memory card audits for the municipal election. We performed both pre-election and post-election audits of memory cards. The primary goal of the pre-election audit was to perform an integrity check of the contents of the memory cards which were to be used in the elections. The goal of the post-election audit was to ensure that the memory cards were in the proper state ("Election Closed" with results printed) in addition to the integrity check (same as used for the pre-election audit) to verify that the memory card programming corresponds to the intended pre-election programming.

The memory cards contain the election data, ballot layout, and bytecode (for custom reporting) for the elections. They also store the tally of ballots cast. In this sense, the memory cards are the electronic analogue of a physical ballot box. In this work, we focus on auditing the AV-OS terminal and therefore make the assumption that all state information is kept on the memory cards. For other machines which contain internal storage there would obviously be a larger class of potential problems and attacks that would require additional steps to audit.

Vendor-supplied election management systems, in our case the system called GEMS, are used to produce custom election software and data for the memory cards. For the State of Connecticut, LHS Associates of Methuen, MA were responsible for programming the memory cards. The data, layout and bytecode are contained in the GEMS database and are loaded onto the memory card using an AV-OS terminal connected to a conventional PC running GEMS. A copy of the GEMS database used to program the cards was provided by LHS Associates prior to the election. Each district received four identical memory cards containing the election information. After testing the cards, each district was directed by the Secretary of the State's Office to randomly select and ship one of the cards to VoTeR Center for the audit procedure.

The audit of a card involves the extraction of the card's image and its comparison against a reference image that the VoTeR Center produced independently from the GEMS database, using GEMS itself and its own auditing tools. Any discrepancy or deviation is logged and analyzed. Specifically, the comparison focuses on deviations in the ballot data and layout, bytecode, the state of the counters, and to some extent the audit logs present on the card. The audit process is automated to the greatest extent feasible. The remainder of the paper describes each of these steps in detail.

2 The AV-OS Election System

The overall election system that is the subject of this report consists of two major components [6]: the AccuVote Optical Scan voting terminal (AV-OS) and Global Election Management System (GEMS).

The AV-OS terminal is a computing device responsible for accepting ballots and recording the results of the election. The functionality of the terminal is determined by its firmware which is loaded on an Erasable Programmable Read Only Memory (EPROM). The terminals currently in use in the State of Connecticut contain the firmware version 1.96.6. The major hardware components include an optical scanner, paper-tape dot-matrix printer, LCD display, serial communication port, and built-in modem. Finally, the AV-OS supports a removable 40 pin EPSON memory card that maintains the information regarding the candidates, the results of the elections, and executable code used for reporting. Extensive analysis and discussion of the contents of the memory card appear below.

GEMS is the ballot design and central tabulation system. It is installed and operated from a conventional PC. GEMS consists of several databases that include the data, ballot layout, and bytecode corresponding to the precincts participating in the election. This data is transferred via the serial communication port to (and from) the memory card kept in the AV-OS terminal. (We note that in Connecticut, central tabulation feature of GEMS is not used.)

2.1 AV-OS Software Components

The behavior of each AV-OS terminal is determined by two software components: (i) the firmware and (ii) the memory card's contents.

2.1.1 Firmware

The main software component of the AV-OS is the *firmware*, that is, executable code kept in an EPROM chip (M27C1001) and responsible for all the functions provided by the machine. The EPROM is electronically programmable and UV (ultra-violet) light erasable. To obtain and process the binary representation of the code of the firmware, we used the following tools:

- *EPROM reader/burner*: Batronix - Bagero BX40
- *EPROM Eraser*: BK Precision - 850 EPROM eraser
- *Programmable and UV light erasable EPROMS*: M27C1001, TMS27C010A
- *Hex Editor*: Batronix - Prog-Express v.1.2.5
- *Disassembler*: IDA Pro freeware v.4.3

The EPROM reader was used to read the original firmware from the machine's EPROM and save it on the PC as a binary (hex code) file. This code was processed using a hex editor to gain some understanding of the firmware. The binary image of the firmware was examined as a friendlier human-readable representation with the IDA Pro tool based on the assumption that the code was meant for a 80186 processor[1]. Note that no decompilation of the code was attempted or performed. All new code needed to perform the audits was developed directly on the firmware image with the help of a simple hexadecimal editor. Deploying the needed audit firmware boiled down to burning a new image onto a programmable EPROM[2] and installing the new EPROM into the AV-OS.

2.1.2 Memory Card

The memory card inserted and kept in each of the AV-OS terminals is a 40-pin 128KB Epson card. It is installed into the 40-pin card slot (J40 connector) of the AV-OS. It is worth mentioning that Epson discontinued the production of this memory card, and reader/writers for this memory card are not readily available.

The data on the card includes status information, an audit log, ballot description, and counters, described in more detail below. Note that the analysis is performed without any technical documentation from the vendor and in the absence of the firmware source code. Therefore the validity of our findings is based on the systematic analysis of the firmware binary code and by "eavesdropping" on the communication between GEMS and AV-OS. Our analysis revealed the formatting depicted in Figure 1. Here we summarize briefly the data found in each part of the memory card.

Header: The header of the card contains useful information about the organization of the contents of the card and main description of the election. The headers are all of a fixed length, totaling 576 bytes. This segment includes:

- AV-OS version.
- Election Status, indicating the current state of the card (e.g., blank,, set for election, closed election).
- PIN number encoding.
- General Counters, including the total ballots cast and total elections run.
- Pointers to data segments on the memory card.
- District information.

Log: This segment of the memory card is a fixed-size "circular" buffer in which the firmware logs certain actions and the time they were performed. It can hold at most 512 entries—any log additions beyond this limit overwrite entries in an earliest-first fashion.

Election Data: The content of the election data segment has a variable length and can be classified into three subsections:

1. **Ballot Data:** This section contains information about the ballot layout used in the current district for the current election.
2. **Race Data:** This section contains information about the offices available in a race for the district in the current election. Key parts of this data include: Office ID, Name of the office, and Number of candidates for the office.
3. **Candidate Data:** This section of the memory card maintains information about the candidates. For each candidate it includes: Office ID the candidate belongs to, Candidate ID, Candidate Name, Location of the candidate on the ballot sheet.

Bytecode: This section of the card contains the bytecode.

The AccuBasic (AB) bytecode present in the programmed memory cards is responsible for the reporting

[1] The actual processor in the AV-OS (part number NEC D70320L-8) emulates an Intel 80186 processor.

[2] Both EPROM versions mentioned above are compatible with the AV-OS.

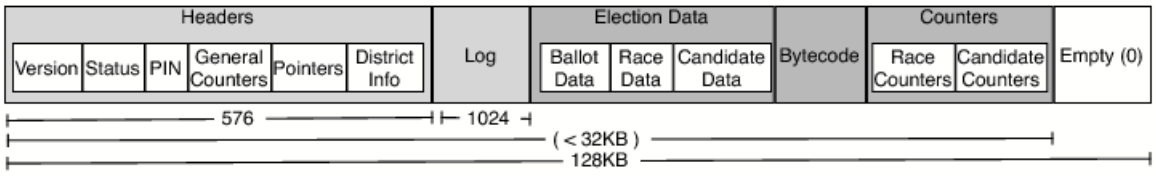

Figure 1: Format of the Memory Card.

procedures associated with an election. The code is written in a proprietary symbolic language; though the language explicitly lacks the ability to write to the memory card, it supports traditional control-flow, arithmetic, read-write *local* variables and procedure calls. AccuBasic programs are compiled to produce bytecode (externally) stored in `.abo` files. The bytecode provided by LHS Associates for this election was manually analyzed to verify that no extraneous (or malicious) functionality was present. This analysis was performed in part with the help of experiments conducted using the AccuBasic compilers (1.94 and 1.95) publicly available at [1].

Election Counters: The election counters are located below the bytecode on the memory card as illustrated in the schematic. Here all the election results and statistics are stored. This section can be divided into two broad subsections:

1. **Race Counters:** Statistics and counters for each office are kept in this section of the card.

2. **Candidate Counters:** This section contains the counters for each individual candidate.

3 Auditing Process

The auditing process consists of two phases: (i) analysis of the AV-OS firmware and bytecode, and (ii) analysis of data collected from memory cards.

In the static analysis phase we describe how to obtain a true image of the contents of the memory cards used in AV-OS terminals. A major obstacle is the absence of readily available card readers in the market, due to the discontinuation of such memory cards. We developed new firmware for the AV-OS terminal in order to use the terminal as a card reader. Having done so, we used one of the AV-OS terminals, equipped with our new firmware, as a card reader/writer and captured the contents of the card with the help of data collection software running on a connected PC. This software was designed to communicate with the modified firmware and save the contents of the cards on the PC for further testing. Below we provide a high level description of the new custom firmware and the data collection software.

Once the data collection tools are described, we go on to describe the testing phase and, in particular, the exact data collected for card evaluation. The data is classified into three categories: (a) Baseline data, (b) Pre-Election Data, (c) Post-Election Data. We discuss below the role and the selection process for each category. Overall the testing phase aims to collect adequate data to ensure the integrity of the memory cards used in the elections and the discovery of any data inconsistencies.

3.1 Static Analysis

The static analysis phase consists of three parts: analysis and customization of the AV-OS firmware, developing a data collection and comparison tool, and analyzing the bytecode that is used in all districts.

3.1.1 Custom Firmware

The AV-OS terminal can be used to obtain the contents of the memory card installed in its 40-pin card slot. This is done by using the diagnostic mode of the terminal under the option *Dump Contents of Memory Card*. Although this "dump" procedure is provided by the stock firmware installed on the AV-OS, there are several major issues in using the built-in dumping procedure of the AV-OS firmware:

1. Relying on the AV-OS dumping procedure is questionable, since there is no way to tell whether AV-OS faithfully dumps the contents of the card.

2. Since the dumping procedure is a part of the original firmware of the AV-OS over which we have no control, the use of this procedure may be registered and logged on to the audit logs of the memory card. This would result in an undesirable modification of the audited card.

3. The dump procedure of the AV-OS firmware selectively filters out some characters (specifically

hexadecimal 11 hex and 13 hex) from the contents of the card and they are not reliably reproduced/extracted from the card. (There is no apparent reason for this behavior except perhaps historical uses of these hex values as flow control characters.)

4. The dumping of the card using the procedure takes a relatively long time, and is prohibitively inefficient for an auditing process involving hundreds or even thousands of cards).

The above issues motivate the need for analyzing the firmware and developing new firmware to eliminate the drawbacks.

Thus our objective here was to transform the AV-OS voting terminal into a simple card reader that would reliably deliver the data from the card so it could be read from the serial port with no side-effects. We emphasize here that this paper contains only the high-level overview of these steps and omits the technical details.

Custom Firmware Development: As mentioned in Section 2 the AV-OS terminal's processor is based on an Intel 80186, 16 bit architecture. As a consequence, the firmware stored in the 128K 32 pin EPROM consists of two segments, with the first segment at the beginning of the EPROM's memory space. "Far" calls, which reveal the starting address of the second segment, are employed to facilitate the interaction between the two segments. The firmware contains hardware initialization (boot code) and the AV-OS program. In our work we used the original hardware initialization code. To confirm that this code does not alter memory card contents, we performed multiple experiments using cards with known content. The fact that no content alteration was observed, and that the initialization of the terminal does not required the card to be inserted provided evidence that we could safely use the initialization in our auditing procedure.

Our goal was the following: (i) identify the components and the procedures responsible for dumping the contents of the memory card and, (ii) develop new procedures to suit our needs and to produce new firmware to be used in the audit. To hasten the data extraction process we implemented a very simple form of data compression based on *run-length encoding (RLE)* and used it to transfer the contents of the memory card through the serial line. In this way, our new firmware code transforms the AV-OS terminal into a true card reader that simply delivers the data from the memory card to the serial port without any of the undesirable side-effects seen with the original firmware.

Four main points were taken into account during the production of new firmware:

1. Memory Card Access
2. Serial Port Access
3. Delivery of the Memory Card data
4. Avoid any logging on the memory cards

Again, the findings reported here were obtained by close examination and analysis the firmware's binary file and without any assistance or technical documentation from the vendor.

Memory Card Access: The first challenge is to directly access the data stored in the memory card. For that purpose we identified the memory addresses of different segments on the memory card. With experimentation and tests we verified our ability to read and write from predefined locations of the card. As a result the exact value of each particular byte kept on the card could be obtained.

Serial Port Access: The second objective was to extract the bytes obtained from the card and faithfully place them in the appropriate location so that it could be read on the serial port. We determined that the original firmware was indeed inadequate in performing the audit. We analyzed the code responsible for dumping in the original firmware and (with the help of [16]) identified the procedure responsible for transmitting bytes to the serial port. Our analysis of the code revealed that byte values 11 hex and 13 hex were indeed treated differently and not sent correctly over the wire. Our new firmware transmits the data faithfully, without any filtering. The firmware was tested on the transmission of known contents of the memory card to confirm and verify that no additional bytes were transmitted and that the functionality was as required.

Delivery of the Memory Card data: To dump the entire card, it is sufficient to write a simple routine that transfers all the bytes of the card to the serial port, one at a time. A dedicated program waits on the other side of the wire and collects the data sent. That program saves the received bytes in a file that is used later for evaluation and audit analysis.

Avoid logging on the memory cards: The final task was to ensure that no logging information is added to the memory card during the dumping process – such changes would be unacceptable in a pre-election audit setting. Since our firmware implements the dumping process and controls the execution from the beginning of the boot, we can guarantee that no logging occurs. Thorough testing verified that the unmodified initialization code in the firmware also does not alter the log nor any other portion of the memory card. Thus the entire procedure gets an image of the card and does not alter the card.

Speeding up memory Card Dumping: Because of the low transmission rate of the serial port (9600bps $\approx$ 1KB/s) of AV-OS, dumping the contents of the 128KB memory card takes a significant amount of time ($>$ 2 *min*). Inspecting a large number of cards (hundreds or even thousands) would require substantial time. To solve this problem and to optimize the dumping procedure, we implemented Run Length encoding to compress the bytestream sent over the wire, and decompress it on the receiving end. This simple improvement reduces the dump time to 20*sec*. (Simple run-length encoding works well here because several large parts of the memory card are populated with sequences of identical values.)

3.1.2 Data Collection Tool

The data collection/comparison tool serves two purposes:

1. Collecting the memory card dump sent using run length encoding.
2. Auditing the collected data by comparing baseline and audit data and analyzing the differences.

The challenge in auditing the memory cards is in managing the large number of data files and automating the tasks. The tool we developed includes a graphical user interface (GUI) to simplify the process. The tool maintains the list of towns and districts, keeping track of the data collected for both baseline and audit cards. It also records data sent from the AV-OS with a single button click, and compares all collected data, reporting any discrepancy. The comparison is done on the basis of our analysis of the memory card layout. The comparison identifies any differences, ignoring those that are not significant (such as timestamps, log entries, and sequence numbers). The tool also generates a table listing all districts with the various memory card states, discussed in Section 3.2.2 below. This allows quick assessment after data collection to identify potential problems.

3.1.3 Bytecode Analysis

The Accu-Basic bytecode that is loaded into each programmed memory card manually analyzed to ensure the absence of undesirable behaviors. The analysis determined that the bytecode performs the expected reporting functions. The bytecode analysis was performed with the assumptions based on the reviews done by the source code review team as part of a "Top-to-Bottom" review of electronic voting systems certified for use in the State of California [17] and the security analysis of the Diebold Accu-Basic interpreter [18]. Although these reports bring to light multiple vulnerabilities in the Accu-Basic interpreter, it was not claimed that it interprets the bytecode incorrectly. Recall that it is not possible to overwrite the contents of the card with the Accu-Basic bytecode, as was pointed out in our earlier report [6].

3.2 Testing Methodology

Having the methodology to extract the data from the memory cards, our next task is to test for potential data inconsistencies and integrity problems of the memory cards used in the elections. To perform this task we need to collect three types of data: (a) Baseline data, (b) Pre-Election Data, and (c) Post-Election Data.

Baseline Data: Before the elections the VoTeR Center used an unmodified AV-OS, GEMS and database that LHS Associates used to program the memory cards for the elections. Using these resources we programmed our own memory cards. After programming those cards we collected and saved their data using our data collection methodology. This gives us the *baseline data*.

Pre-Election Data: Prior to the elections the precincts were instructed to send a randomly selected subset of their memory cards for testing. We collected images for each of these memory cards using our own tools. This forms the *pre-election data*.

Post-Election Data: Similar to the pre-election data, some of the precincts were instructed to send us a subset of their cards after the completion of the elections. We refer to the data collected from those cards as *post-election data*.

3.2.1 Testing Procedure

A focal point of the audit was the validity of the data collected and the integrity and reliability of the memory cards as a storage medium. The latter can be tested partially during the data collection as our data collection tool identifies cards containing "junk" (i.e., an apparently arbitrary sequence of data values) or no programmed data. Validity of card data is checked automatically with the data collection tool. Below we present the steps taken for testing the pre- and post- election cards. This section only presents the methodology used for testing. The results and detailed description of the testing appears in Section 4.

Pre-Election Audit: The goal of the pre-election audit is to identify invalid or maliciously altered memory cards before the execution of the elections and additionally check that the towns followed the correct testing procedures.

The first concern was to collect a sufficient amount of memory cards in order to create a representative sample for our findings. Each polling center received four programmed memory cards from LHS Associates. There are two AV-OS voting terminals in each polling center. Consequently, two out of the four cards from each precinct were the "primary" cards, i.e., the cards that would be used in the election, and the remaining two cards were the "backup" or "secondary" cards. According to the instructions set up by the Office of Secretary of the State, after receiving four programmed memory cards, poll workers of each district are supposed to put any two out of four cards in the available machines and run a test election on each of them. Once tested the cards should be placed in "election mode" and removed from the AV-OS machine. Putting the cards in "election mode" resets the counters to zero. Then, the remaining two cards should be tested and placed in "election mode". The AV-OS machine should now be sealed and stored in a secure location. Immediately after the testing is complete, they are required to *randomly* select one memory card per district and send this card to the University of Connecticut VoTeR Center for pre-election audit testing. This card should be chosen from the memory card(s) that are not already sealed in an optical scan voting machine. The procedure for random selection of the memory card(s) described above applies only to precinct based tabulators and does not include central counting absentee ballot tabulators. Given the above procedures, each memory card received for pre-election auditing should be in "election mode" with counters set to zero and should have evidence of a pre-election test.

After collecting the necessary cards from the districts we tested the validity of the cards by performing a semantic comparison between the pre-election and the baseline data. The potential problems we are testing for include incorrect ballot data or bytecode, non-zero counters, and incorrect states. Such problems could arise from either malicous attacks, accidents, or failure to follow procedures. By comparing all data on the audited card with baseline data we can detect any such discrepancies.

Post-Election Audit: The post-election audit employs a similar procedure as the pre-election audit to establish the validity of the cards. The main goal however of the post-election audit is to check the validity of the cards after the elections are closed. As a result in this testing phase we get to test memory cards that were used on the election day. Again to test the validity of a card, we compare the post-election data of a district with the corresponding baseline data for that district. Reports regarding the status of each post election card, and information about the counters in the card were extracted from the comparison tool and examined. The integrity and the reliability of the hardware of the memory cards was tested in this phase as well. Detailed results appear in the next section.

3.2.2 States of the Memory Card

There are four aspects of interest with respect to the format of a memory card and the state it can be in when audited: *(a) Card Format*, *(b) Card Status*, *(c) Counter Status*, and *(d) Election Count*.

(a) Card Format: Most of the pre and post-election cards we received, were either properly formatted and contained good data or contained "junk" data. Cards with "junk" data cannot be read and recognized by the AV-OS. Such cards are readily detected through pre-election testing by poll workers and cannot be used for an election. We also observed some cards that although properly formatted, useable and with good data, also contained a few "specks", that is a few isolated bytes with unexpected values. These occurred in an area beyond the area that is used for election data, typically filled with zeros. (It is possible that these are errors that occurred during transmission.) The "specks" are not detected by AV-OS, and it appears that they do not interfere with normal AV-OS operation. To sum up the card format can be one of the following three: *Good Data, Clean Card; Good Data, Some Specks* and *Junk Data*.

(b) Card Status: This refers to the current state of the memory card indicated by a status flag in the header data. We identified the following states of the memory card: *Not Programmed (Blank); Not Set for Election, Set for Election, Results Print Aborted, Election Closed, Results Sent/Uploaded; Audit Report Pinted*.

(c) Counter Status: The Counter Status can be one of the following: *Zero Counters, Non Zero Counters, Non Zero and Set for Election*. Depending on the audit phase (pre-election or post-election) we can consider a counter status being good/bad depending on the situation. Pre-election cards are expected to have zero counters. If a card has non-zero counters, but is not set for election, the counters will be zeroed when the card is set for election. Post-election cards, used in an election are expected to have non-zero counters and a status of closed.

(d) Election Count: The Election Count is a numeric value which equals to 1 at the beginning, meaning that the card was never reset. This is only examined in pre-election cards and refers to the observed values of the election counter. Higher values indicate

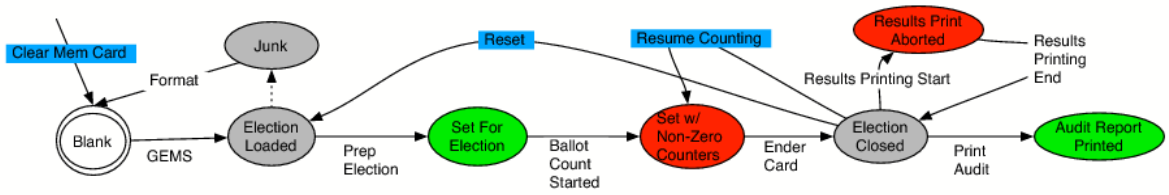

Figure 2: State Machine describing the state of the AV-OS while being used.

that the machine was used for a (test) election and then reset, in some cases more than once (several test runs).

Figure 2 shows the states of the AV-OS (ovals) and the actions (arrows) that move the machine from one state to another. The states in red, Set for Election with Non-Zero Counters and Results Print Aborted, are "dangerous" states for an audited pre or post election card, respectively. States shown in Green, Set For Election and Audit Report Printed, are the ideal states for pre and post election cards, respectively. Gray states, Election Loaded and Election Closed, are safe, though reflect a failure to follow strict procedures. Junk cards are also safe, though it is unclear how they get into this state. Actions in blue are restricted to poll workers with the PIN number.

To summarize: pre-election cards should at least be in the Election Loaded state, and ideally in the Set for Election state, but never Set for Election with non-zero counters. Post election cards should ideally be in the Election Closed state, and ideally with the audit log printed, but never with the Results Aborted or with the election not yet closed. When the election is closed, the results printing is begun automatically and the aborted state is only reached if the printing is cancelled, or if a duplicate copy is begun and aborted. The Audit Report Printed thus indicates that the results and the audit log were both printed. In Section 4 we see that post election cards were never in the audited state since auditing was not yet part of the standard procedures. Because of this, the Election Closed state is the expected state in our analysis.

4 Results and Observations

We present the results of the pre and post-election audits. The pre-election audit was performed in 522 memory cards, covering over 75% of all districts, received during the weeks before and after the election. The post-election audit was performed in 100 memory cards, that covered the 5% of the cards used in the election.

4.1 Pre-election

378 out of 522 memory cards were received prior to the election. The rest were received in weeks following the election. We present the results in two sets: one for the cards received prior to the election, the other for all cards received (both before and after the election). The results of the audit are generally similar for both sets. We start by discussing the issues that arose in the selection of the cards that were shipped to us.

4.1.1 Sampling

We noticed a few differences between the actual procedures followed by the poll workers and the procedures defined by the Office of Secretary of the State, regarding the sampling of the memory cards to be sent to VoTeR Center. Some of those were:

- The cards were not chosen uniformly at random for the audit. The primary and backup cards could be distinguished by the label on the card. As a result, the majority of the districts kept the "primary" cards and chose one of the "backup" cards (at random) to send for the audit.

- Although each town had to send a randomly chosen memory card for each district to VoTeR Center, some towns randomly selected districts from which to send memory cards. In most cases, they sent the memory cards for half of the districts. There were cases, where we received a single card per town, although the town had more than one district. Only a few towns sent one memory card per district as they were supposed to.

Clearly a better definition of the audit procedure is needed, so that the memory cards are selected from all districts per town. Moreover, we suggest sampling the memory cards uniformly at random and not choosing the backup cards as the ones to send. This would require that all the cards "look and feel" the same and the backup cards are not marked differently from the main cards. Greater care should be taken to adhere to the instructions provided by the State. It is important to emphasize that

the backup cards were programmed and handled the exact same way as the primary cards during the pre-election procedure from the LHS Associates. Thus the fact that some districts sent us their backup cards does not greatly affect the significance of our statistical results. We expect that future audits would reflect higher reliability and improve statistical strength. The changes in the audit procedures are already being implemented by the CT SOTS Office for future elections.

4.1.2 Memory Card Data Audit Results

Table 1 shows the frequency of various states observed on the audited memory cards. The data is presented in four parts:

(a) Card Format: About 95% of the cards were properly formatted and contained good data. Under 2% of the cards were properly formatted, contained good data, but also contained a few "specks". Over 3% of cards contained "junk" data.

In the rest of the analysis the percentages are computed for almost 97% of the cards that were properly formatted and contained contained good data, i.e., the cards that did not contain junk data.

(b) Card Status: The plurality of the cards, over 46% were Set for Election, which is the desired memory card state. No cards were found in the unprogrammed, newly uploaded, or audited state.

Over 8% of the cards were found to be in the Election Closed state, suggesting that the poll workers performed AV-OS testing in the election mode, and this is not the intended procedure. However, for AV-OS machines with such cards to be used on the election day, the cards would need to be reset.

(c) Counter Status: Over 56% of the cards had zero counters. This is the intended state.

About 43% of the cards had non-zero counters, but were not set for election. This is not the intended state of the counters, however the counters will be zeroed when the machine is going to be set for election.

One card (0.2%) was found in the state where it was set for election with non-zero counters, specifically recording that 19 votes were cast. This is problematic and is due to incorrect pre-election testing procedures. The Poll Workers Guide specifies that when the machine is turned on the day of the election, it should print an election zero report which the poll workers should verify. Any machine that is set for election with zero counters should print such a report when it is turned on. However, if the counters are non-zero, it will not print anything and will instead resume (continue) counting. Therefore, attentive poll workers should be able to detect a card that is in this state by the lack of a zero report (in fact it was confirmed that in Connecticut all districts documented printing the zero report). Nonetheless, if poll workers are unaware of this policy then such a machine could result in incorrect election results.

(d) Election Count: A value of 1 means that the card was never reset. Higher values indicate that the machine was used for a (test) election and then reset, in some cases more than once (several test runs).

These observations indicate that proper pre-election testing procedures are either not uniform, or are not communicated effectively.

4.2 Post-election

We now present the results of the post-election audit. We have received and examined 100 memory cards from several districts. Most of the cards used in the election were shipped to LHS for reprogramming, and the VoTeR Center received the remaining cards that were still in the possession of the districts. Thus these cards do not represent a random sample of the cards used in the election. In spite of this fact we could make post-election audit possible as 36 cards out of 100 were used during the election and we could analyze the data stored on those memory cards. The post-election audit covered more than 5% of all cards actually used in the election.

Table 2 shows the frequency of various states observed on the audited memory cards.

Recall that each district received 4 memory cards. Most of the districts sent one of the cards to the VoTeR Center for pre-election audit, leaving 3 cards in the possession of each district. Among these, it is expected that one card was used in the election. Thus about 33.3% of the cards should have been used in the election. Among the post-election cards we examined, 36% of the cards (36 cards) were used, which is close to what was anticipated. (Some of the audited cards turned out to be unusable (they contained "junk" data), so among the usable cards 39.6% were used.)

We present the rest of the results in three parts:

(a) Card Format: Among the 100 cards, 92% of the cards were properly formatted and were found to contain consistent data. The remaining 8% of cards (8 cards) contained "junk" data. No cards with "specks" where found.

In the rest of the analysis the percentages are computed for the 92% of the cards that were properly

	For cards received before election		For all pre-election cards received	
	Number	% Total	Number	% Total
(a) Card Format				
Good Data, Clean Card	362	96.2%	495	94.8%
Good Data, Some Specks	6	1.1%	9	1.7%
Junk Data	10	2.6%	18	3.4%
Totals:	378	100%	522	100%
(b) Card Status				
Not Programmed (Blank)	0	0.0%	0	0.0%
Not Set for Election	167	45.4%	218	43.3%
Set for Election	181	49.2%	233	46.2%
Results Print Aborted	7	1.9%	11	2.2%
Election Closed	13	3.5%	42	8.3%
Results Sent/Uploaded	0	0.0%	0	0.0%
Audit Report Printed	0	0.0%	0	0.0%
Totals:	368	100%	504	100%
(c) Counter Status				
Zero Counters	209	56.8%	285	56.5%
Non Zero Counters	158	42.9%	218	43.3%
Non Zero and Set for Election	1	0.3%	1	0.2%
Totals:	368	100%	504	100%
(d) Election Count				
1	361	98.1%	485	96.2%
2	6	1.6%	16	3.2%
3	0	0.0%	2	0.4%
4	1	0.3%	1	0.2%
Totals:	368	100%	504	100%

Table 1: Pre-election memory card analysis summary: (a) card format, (b) card status, (c) counter status, (d) number of elections count.

formatted, i.e., the cards that did not contain junk data.

(b) Card Status: One blank/unprogrammed but properly formatted card was found. This means, most probably, that LHS Associates did not program the card, and they shipped it without testing.

No cards with uploaded results were found. No cards with audit report printed were found. These are the expected results.

Of the usable cards, 12% were not set for election. These cards were not used in the election, but they should have been set for election, suggesting that some pre-election protocols were not followed properly.

Over 47% of the cards were Set for Election, which is the desired memory card state for cards that were not used in the election.

Almost 35% of the usable cards (32 cards) were found to be in the Election Closed state. These are the cards that were used in the election.

Another 4.3% (4 cards) were used in the election, but indicate that the printing of the results was aborted. This suggests that the machine was turned off before the complete paper tape was printed. (Perhaps poll workers waited just for the counters to be printed, then turned off the machine. Alternatively, it is possible that the printing of a duplicate tape was aborted.)

(c) Counter Status: Over 12% of the usable cards were not set for election, and had non-zero counters. Such cards indicate that they were tested by poll workers prior to the election, but not set for election. These were not used in the election.

Over 47% of the cards were set for election and had

	Number of Cards	% Total Cards
(a) Card Format (all cards)		
Good Data, Clean Card	92	92.0%
Good Data, Some "Specks"	0	0.0%
Junk Data	8	8.0%
Total:	100	100%
(b) Card Status (well-formatted cards)		
Not Programmed (Blank)	1	1.1%
Not Set for Election	11	12.0%
Set for Election	44	47.8%
Results Print Aborted	4	4.3%
Election Closed	32	34.8%
Results Sent/Uploaded	0	0.0%
Audit Report Printed	0	0.0%
Totals:	92	100%
(c) Counter Status (usable cards)		
Not Set for Election, Non Zero Counters	11	12.1%
Set for Election, Zero Counters	43	47.3%
Set for Election, Non Zero Counters	1	1.1%
Election Closed, Non Zero Counters	32	35.2%
Print Aborted, Non Zero Counters	4	4.4%
Totals:	91	100%
Total number of cards used in the election:	36	39.6%

Table 2: Post-election memory card analysis summary: (a) card format for all cards, (b) card status for well-formatted cards, (c) counter status for usable cards.

zero counters. This is the intended state of the cards that were not used in the election.

About 35% of the cards (32 cards) indicated that election was closed and had non-zero counters. These cards were used in the election.

Over 4% of the cards (4 cards) had non-zero counters and indicated that the printing of the results was aborted (see above). These cards were used in the election.

One card (1.1%) was found in the state where it was set for election with non-zero counters. The counters must be 0 for such a card. This situation is detectable upon the attempt to print the "zero count" report on the election day.

5 Conclusions

Having performed and completed the audit, we believe that both pre-election and post-election tests and audits of memory cards (and similar components of voting equipment of various makes) are crucial in providing valuable and timely information necessary to ensure the integrity of our electoral system. Such audits can reveal not only incorrect (or malicious) programming of the customizable software components, but also mistakes or oversights that can occur in preparing voting machines for elections and running the elections using the machines.

For example, one memory card was found to be set for election with non-zero counters. If such a card is carelessly used in an election, the results would reflect the extra votes already on the card. This would have been detected by the failure to produce a zero total report on election day. Additionally, several cards were in states that, although not dangerous, were contrary to the proper state. For example, the pre-election cards tested with in Election Mode or not set for election, or post-election cards with aborted report printing. This serves to highlight the importance of having clear and precise instructions, and poll workers trained to follow them.

There were also a surprising number of "junk" cards (3.5% in pre-election audit and 8% in post-election audit). Whether or not these cards were the results of soft-

ware or hardware failures, or lack of testing at the vendor site, such rates of failure are clearly inadequate for modern electronic systems. Note that such cards will not work in the AV-OS. Indeed, some arrived with messages indicating that they were tested by poll workers and found to be "broken". We do not believe these cards were damaged in shipping. Consequently, it appears that these cards were either not tested prior to shipping them to districts, or the results of hardware failures of cards themselves or of the voting terminals used to program them. Thus testing the voting equipment before the elections will help avoid problems on election day.

Finally, our examination of the memory cards revealed no incorrect ballot data or bytecode.

About the UConn VoTeR Center

Following our participation in the Connecticut Voting technology Standards Board in 2005, the Voting Technology Research (VoTeR) Center was established in 2006 to advise state government in the use of voting technologies, to research, investigate and evaluate voting technology and voting equipment, and to develop and recommend safe use procedures for the computerized voting technology in elections. The personnel of the Center includes several faculty members, graduate students, and staff of the Computer Science and Engineering department at the University Of Connecticut.

The work of VoTeR Center in the State of Connecticut is funded by the Office of the Connecticut Secretary of the State (SOTS), and we function in close contact with the SOTS Office personnel. We offer the State an independent, objective analysis of the voting technologies offered by several vendors, we advise the State on selecting and administering the voting equipment for its election needs, and we are not associated with any of the voting technology vendors. The evaluations of the voting technology are performed at the VoTeR Center Lab at the University of Connecticut. These include hands-on evaluations, exploration of possible attack vectors, physical integrity checks of the terminals and memory cards, and mitigation strategies. It is worth pointing out that the VoTeR center is not involved in the State's policies for choosing a vendor to procure the voting technology, but limited to evaluating these technologies before deployment and use by the State. In this sense the VoTeR center is a third party independent technical consulting resource for the State of Connecticut.

VoTeR Center personnel assisted the State in developing safe use procedures for the Optical Scan terminals for this election. The procedures in place for the election includes strict physical custody policy, tamper-resistant protection of the equipment, and random post-election audits.

References

[1] Black Box Voting http://blackboxvoting.org.

[2] Jonathan Bannet, David W. Price, Algis Rudys, Justin Singer, Dan S. Wallach: Hack-a-Vote: Security Issues with Electronic Voting Systems. IEEE Security & Privacy 2(1): 32-37 (2004)

[3] Brennen Center Task Force on Voting System Security. *The machinery of democracy: Protecting elections in an electronic world, 2005.* Lawrence Norden, Chair. Brennen Center for Justice, NYU School of Law. http://www.brennancenter.org

[4] Help America Vote Act (HAVA), http://www.fec.gov/hava/law_ext.txt

[5] H. Hursti, Critical Security Issues with Diebold Optical Scan Design, Black Box Voting Project, July 4, 2005. http://www.blackboxvoting.org/BBVreport.pdf

[6] A. Kiayias, L. Mchel, A. Russell, A.A. Shvartsman, M. Korman, A. See, N. Shashidhar and D. Walluck, Security Assessment of the Diebold Optical Scan Voting Terminal, http://voter.engr.uconn.edu/voter/Report-OS.html

[7] A. Kiayias, L. Michel, A. Russell, N. Sashidar, A. See, and A. Shvartsman, An Authentication and Ballot Layout Attack Against an Optical Scan Voting Terminal. 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT 07), Augist, 2007, Boston, MA.

[8] A. Kiayias, L. Michel, A. Russel, N. Sashidar, A. See, A. Shvartsman, S. Davtyan. Tampering with Special Purpose Trusted Computing Devices: A Case Study in Optical Scan E-Voting. Twenty-Third Annual Computer Security Applications Conference (ACSAC), December, 2007, Miami Beach, Fl.

[9] T. Kohno, A. Stubblefield, A. D. Rubin and D. S. Wallach, Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy 2004.

[10] Poorvi L. Vora, Ben Adida, Ren Bucholz, David Chaum, David L. Dill, David Jefferson, Douglas W. Jones, William Lattin, Aviel D. Rubin, Michael I. Shamos, Moti Yung: Evaluation of voting systems. Commun. ACM 47(11): 144 (2004)

[11] RABA Innovative Solution Cell. Trusted agent report Diebold AccuVote-TS voting system, January 2004.

[12] David Wagner, David Jefferson and Matt Bishop, Security Analysis of the Diebold AccuBasic Interpreter, Voting Systems Technology Assessment Advisory Board, University of California, Berkeley, February 14, 2006.

[13] Harri Hursti, Diebold TSx Evaluation, Black Box Voting Project, May 11, 2006 http://www.blackboxvoting.org/BBVtsxstudy.pdf

[14] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, Security Analysis of the Diebold AccuVote-TS Voting Machine, September 13, 2006 http://itpolicy.princeton.edu/voting

[15] Pamela Smith, President, VerifiedVoting.org Written Testimony Before the Committee on House Administration, Subcommittee on Elections U.S. House of Representatives March 20, 2007. http://electionaudits.org/files/PamelaSmithTestimonyFinal_2007mar20.pdf

[16] V25+ and V35+ User's Manual, NEC Corporation, December, 1992.

[17] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, William P. Zeller, Source Code Review of the Diebold Voting System, July 20, 2007
www.sos.ca.gov/elections/voting_systems/ttbr/diebold-source-public-jul29.pdf

[18] David Wagner, David Jefferson, Matt Bishop, Security Analysis of the Diebold AccuBasic Interpreter, February 14, 2006
www.sos.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf