VoTeR Center

UConn Voting Technology Research Center

PI : A. Shvartsman, Ph.D.
Co-PIs : A. Kiayias, Ph.D., L. Michel, Ph.D., A. Russell, Ph.D.
Staff: S. Davtyan, S. Kentros, N. Nicolaou, A. See, N. Shashidhar

Pre-Election Audit of Memory Cards for the November 2007 Connecticut Elections

Version 1.0, January 24, 2008

Summary

The UConn VoTeR Center performed an audit of the pre-election memory cards for the AccuVote Optical Scan tabulators that were to be used in the November 2007 Connecticut Elections. The cards were programmed by LHS Associates of Methuen, Massachusetts, and shipped to the towns in Connecticut. The towns were instructed to test the cards and to choose randomly one out of each four cards per district to be shipped for the audit.

The total of 522 cards were received and tested by the VoTeR Center, out of which 378 cards were received before the election. Out of the total number of cards, 18 cards, or 3.5% were found to contain "junk" data, that is, they were unreadable, which is easily detected by the tabulators as such, and could not have been used in the election. The rest of the cards, or 96.6%, were found to have been properly programmed for election. These cards contained valid ballot data and the executable code on these cards was the expected code, with no extraneous data or code on the cards.

About half of the cards were found to have been tested and set for election—the intended state of the cards following the prescribed testing procedure. Most of the remaining cards were tested by the towns but not set for election; while this is not a problem, this suggested that the relevant towns/districts either misunderstood the instructions or did not follow the instructions. One card was found in the state set for election but with non-zero counters, indicating that the district tested the card in election mode and did not reset the card. This is a potentially problematic, but detectable situation, since proper procedures require that the "zero counter" report is produced at the start of the election[1].

This document contains the description of the audit procedures, the (reverse) engineering that was performed by the VoTeR Center in order to enable memory car testing, the results of the audit, discussion, and recommendations.

The audit was performed on request of the Office of the Secretary of the State.

[1]For the town in question, the Secretary of the State subsequently received copies of the printout that contained a correct zero-count report, indicating that correct procedures were in fact followed on the Election Day.

Contents

1 Preface

The Voting Technology Research (VoTeR) Center at the University of Connecticut conducted pre-election audit of the memory cards to be used in the AccuVote Optical Scan (AV-OS) tabulators in the municipal elections of November 2007. The audit was performed on request of the Office of the Secretary of the State of the State of Connecticut.

The memory cards were originally programmed for the November 2007 election by LHS Associates of Methuen, Massachusetts, and provided by LHS to the districts in Connecticut. The audit was performed on the randomly selected memory cards (one out of four) that were selected and shipped by the individual districts to the VoTeR Center at the University of Connecticut in Storrs.

The memory cards were subject to several integrity tests and this report presents a comprehensive overview of these procedures taken by the VoTeR Center personnel in conducting the audit. In this report, we present the objectives of the pre-election audit, the audit process, and the audit results. The process included testing, comparison, and analysis of the data collected during the audit. We also outline 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.

We conclude the report with several observations based on what was learned during the pre-election audit process, and we offer recommendations aimed at enhancing the integrity of our elections. These include recommendations to poll workers and election officials regarding making and managing relevant policies, safely and efficiently handling memory cards, voting terminals, and other equipment associated with an election. We include comments on the importance of clear and unambiguous instructions in dealing with the electoral apparatus and following such directions diligently. We believe that pre-election audits are crucial in providing timely information and maintaining the integrity of the electoral process.

This report is a high-level, non-technical overview of the procedures taken by the VoTeR Center and to this end omits several technical details. We also note that we had no access to, and we did not use any vendor/manufacturer documentation regarding the specification, design and the internals of the AV-OS terminal or the memory cards.

Finally, on request of the Office of the Secretary of the State of the State of Connecticut, the VoTeR Center also performed a partial post-election audit of the memory cards used in the election. A companion report will be issued documenting the results.

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.

The 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 include strict physical custody policy, tamper-resistant protection of the equipment, and random post-election audits.

2 Introduction

We start by overviewing the AV-OS based election system used in Connecticut, the goals of the pre-election memory card audit, and a preview of the audit results.

2.1 Brief Description of the AV-OS

The AV-OS election system consists of two components: the AccuVote Optical Scan voting terminal (AV-OS terminal) and the ballot design and central tabulation system, GEMS, for Global Election Management System. See our report at URL http://voter.engr.uconn.edu/voter/Report-OS.html for details on this election system. We point out the following characteristics of these components:

- The AV-OS system currently in use in the State of Connecticut contains the firmware version 1.96.6. It is equipped with an optical scanner, a paper-tape dot-matrix printer, a LCD display, a serial communication port, and telephone jacks leading to a built-in modem.
- The GEMS software is installed on a conventional PC (or a laptop). It includes a ballot design system and a tabulation system.

  The GEMS system can be used for centralized tabulation of the election results. However, in Connecticut the results are reported at the precincts, and the overall tabulation does not involve GEMS, thus it is eliminated as a source of uncertainty in the tabulation.
- Once the election data is entered into the GEMS system, the specifications of the election are downloaded into a memory card via an AV-OS system connected to GEMS by a serial line cable.
- The memory cards are the 40-pin 128KB Epson cards. The memory card is installed into to the 40-pin card slot (J40 connector) of the AV-OS. It is worth mentioning that Epson has discontinued this memory card some time ago, and reader/writers for this memory card are not readily available.

For election deployment the system is secured within a ballot box so that no sensitive controls or connectors are exposed to the voter. Each memory card contains executable code that is used for printing the reports. The code is written in a proprietary symbolic language. Such executable files are identified as *.abo (AccuBasic Object) bytecode. The installation of the GEMS software on the PC contains several databases that include the data, ballot layout, and bytecode corresponding to the precincts of the State of Connecticut for use during elections.

2.2 Goals of the Pre-Election Memory Card Audit

VoTeR Center was asked by the CT SOTS Office to prepare for and implement memory card audits for the upcoming election. The primary goal of the pre-election audit was to perform an integrity check of the contents of the memory cards that were to be used in the elections.

The memory cards contain the data and the ballot layout for the elections. The memory cards used in the AV-OS terminals also store the tally of the ballots cast and report the results of the election. In this sense the memory cards are the electronic analogue of a physical ballot box.

The data, layout and the functionality on the memory cards are loaded on to the memory card using the AV-OS terminal from the GEMS database. The GEMS database to be used as the baseline for the election data was provided by LHS Associates prior to the election. Each district was given four identical memory cards containing the election information for that precinct. The precinct then shipped one of the cards chosen randomly to VoTeR Center for the audit. The contents of the cards were then extracted and compared with the intended contents using the GEMS database as the reference. The audit process was automated to the extent possible. Any discrepancies or deviations from the baseline were then logged and analyzed. Specifically, the memory cards were audited for any deviations in the ballot data/layout, bytecode, the state of the counters, and to some extent the audit logs on the memory card. The remainder of this report describes each of these steps in detail.

2.3 Preview of the Audit Results

The total of 522 cards were received and tested by the VoTeR Center, out of which 378 cards were received before the election, which represents more than one half of the precincts involved in the election. Out of the total number of cards, 18 cards, or 3.5% were found to contain "junk" data, that is, they were unreadable, which is easily detected by the tabulators as such, and could not have been used in the election. The rest of the cards, or 96.6%, were found to have been properly programmed for election. These cards contained valid ballot data and the executable code on these cards was the expected code, with no extraneous data or code on the cards.

About half of the cards were found to have been tested and set for election—the intended state of the cards following the prescribed testing procedure. Most of the remaining cards were tested by the towns but not set for election; while this is not a problem, this suggested that the relevant towns/districts either misunderstood the instructions or did not follow the instructions. One card was found in the state set for election but with non-zero counters, indicating that the district tested the card in election mode and did not reset the card. This is a potentially problematic, but detectable situation, since proper procedures require that the "zero counter" report is produced at the start of the election[2].

3 Audit Process

This section discusses the steps involved in the audit process in detail. We begin by summarizing the memory card handling procedures. Then we describe the challenge involved in obtaining a true extract of the contents of the 128 KB Epson memory card in the absence of a card reader. Since a card reader for the discontinued Epson card is not readily available in the market we re-engineered the software (firmware) in the AV-OS terminal so it could be used as the memory card reader. Having done this, we used one of the AV-OS terminals in our lab as a card reader/writer. We describe how we re-engineered the firmware of the AV-OS so it could be used as a reader/writer, and the motivation and necessity behind this task. We then describe the data collection tool running on a PC that captures the contents of the memory card extracted by the AV-OS with re-engineered firmware and saves its contents on the PC for comparison and analysis with the baseline data.

The reader primarily interested in the results of the pre-election audit can proceed to Section 4.

[2]For the town in question, the Secretary of the State subsequently received copies of the printout that contained a correct zero-count report, indicating that correct procedures were in fact followed on the Election Day.

3.1 Memory Card Handling – Reception to Storage

VoTeR Center made special accommodations to handle the memory cards received from the districts. Briefly the steps taken from the reception to the storage (including the testing) of a card are the following:

1. Reception of the card by the staff.
2. The staff logs the date and time of the reception and informs a VoTeR center's representative to collect the card.
3. Arrival of the card in the VoTeR lab. Date and time of arrival is logged in a book and the card is locked in a safe.
4. A *demo* memory card is programmed with the initial data that the *election* memory card received supposedly contains.
5. Baseline data are collected by extracting the contents of the *demo* memory card.
6. *Election* card received is taken out of the safe.
7. Audit data are collected by extracting the contents of the *election* memory card. The time and date of the extraction is logged in the book.
8. The *election* card is stored in the safe.
9. The audit data are compared with the baseline data.
10. If the comparison reveals uncertainties about the election card the steps 4 to 6 are repeated. If no uncertainties are detected, the *election* card remains stored and is not used further.

3.2 Data Collection

The data collection component consists of two distinct parts:

- Customized firmware running on the AV-OS and
- Data collection tool running on a PC.

3.2.1 Custom Firmware for Obtaining the Memory Card Contents

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*. Hence, the process of extracting the contents of the memory card is called "dumping" the memory card. The goal of dumping the memory card is to obtain and examine the contents of the card and this "dump" procedure is provided by the firmware installed on the AV-OS. However, there are several major issues in using the built-in dumping procedure of the AV-OS firmware:

1. 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 and unacceptable modification of the audit card.

2. The dump procedure of the AV-OS firmware selectively filters out some characters (hexadecimal 0x11 and 0x13) from the contents of the card and they are not reliably reproduced/extracted from the card. (This is for reasons beyond our understanding.)

3. 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.

4. The dumping of the card using the procedure takes relatively long time and is highly inefficient.

The above issues motivate the need for re-engineering the original firmware to suit our needs and eliminate the drawbacks. This step is imperative if we are to obtain an accurate image of the card, avoid audit card modification, and obtain a significant speed-up of the data collection process.

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 report contains only the high-level overview of these steps and omits the technical details. These details will be included in the extended, more technical version of this report that will be issued in the future.

The AV-OS firmware: We call *firmware* the executable code kept in the hardware of the AV-OS machine that is responsible for all the functions provided by the machine. The code is kept in an EPROM chip (M27C1001) that is electronically programmable and UV (ultra-violet) light erasable. To obtain and process the binary representation of the code 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 firmware code is binary (1's and 0's) and can be examined using a hex editor. The EPROM reader was used to obtain a copy of 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. To obtain a "human readable" representation of the firmware the hex code was processed using the IDA Pro disassembler. We obtained the assembly representation of the code by providing the processor chip architecture (80186) as the input to the IDA disassembler. Once a point of interest was located in the disassembled code we used the hex editor to perform any additions and/or modifications. To test the modified code, we uploaded the code onto one of the programmable EPROMs using the EPROM burner. Notice that both the EPROM versions were compatible with the AV-OS machine. The burned EPROM was then ready to be loaded onto the machine and tested. This formed the first step in our goal to re-engineer the firmware and obtain a custom firmware to transform an AV-OS into a memory card reader/writer.

Firmware Modification: We first identified the components and the procedures responsible for dumping the contents of the memory card. Armed with this knowledge we were able to modify each of these existing procedures to suit our needs and re-assemble them to build our own modified firmware. We then combined these functions and then programmed an EPROM with these functions. This formed the basis for our modified firmware. To hasten the data extraction process we implement

a very simple form of data compression algorithm called Run-length encoding (RLE) and used it to transfer the contents of the memory card through the wire. In this way, our modified firmware code transforms the AV-OS terminal into a true card reader that simply delivers the data from the memory card that can be read from the serial port without any undesirable side-effects of the original firmware as discussed earlier.

Clean Dump: Recall that the original firmware used by the AV-OS modified the data sent over the wire in unexplained ways – adding and/or subtracting specific characters to/from the memory card's byte stream. Some of the characters include the hexadecimal values 0x11 and 0x13. Clearly the need for an accurate comparison between baseline and audit cards led our attention to obtaining a clean dump of the memory cards.

Four main points were taken into account during the firmware modification procedure:

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

All the findings reported here were obtained by close examination and reverse engineering the firmware's binary file. At no point did VoTeR Center have access to internal documentation or source code for any of the components of the AV-OS voting system. This includes GEMS, AV-OS firmware, or other components.

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 place them in the appropriate location so that it could be read on the serial port. From a reference on the Intel-derived processor chip of the AV-OS, we identified the register responsible for the serial communication protocol. We then reverse-engineered the code responsible for dumping in the original firmware and identified the procedure responsible for transmitting bytes to the serial port. This revealed that extra bytes were indeed sent over the wire for some byte values (0x11, 0x13) as we suspected. (Although the values 0x11 and 0x13 are used with the XON/XOFF flow control in some communication protocols and it may be possible to strip these bytes by setting the parameters of the serial port, the reason and purpose for these extra bytes is not yet clear to us and is not discussed in this report.) We also identified the register responsible for access to the serial port communication in the same procedure. Setting the register to a specific value instructs the processor to pick a byte from a local buffer and transmit it through the serial port. Since the register, the sending buffer address, and the extraneous bytes were identified, we were able to modify the procedure to fit our needs. We removed the unnecessary bytes from the procedure and only define the byte to be sent, we store that to the sending buffer and then trigger the transmitting register. Hence, a clean transmission of the byte to the serial port was accomplished. We then tested the transmission on 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: Thus far we established the method to read and write a single byte from the memory card and to transmit a single byte through the serial line. We then

developed a procedure that loops through each byte of the memory card and transmits the byte to the serial port. A dedicated program waits on the other side of the wire and collects the data sent. That program saves the received bytes in a binary 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 we developed most of the parts of the dumping process we made sure that no logging is used in any of our steps. However, there was an initialization step of the AVOS hardware that we had no control over. To test and verify that this particular part of the code does not affect the log file on the card we further ran several tests. We ascertained that cards were not modified. Thus we obtained a clean extraction of the contents of the memory card without any alteration.

Since all the necessary points were addressed, we dependably used the re-engineered firmware to perform the data collection. The time needed for transmitting all the data through the wire however was prohibitively long. So, we next present a simple form of data compression algorithm that substantially speeds up the card dumping time.

Speeding up memory Card Dumping: Because of the low transmission rate of the serial port (9600bps = 1KB/s) of AV-OS, dumping the contents of the 128KB memory card takes a significant amount of time (> 2 *min*). Thus inspecting a large number of cards (i.e., hundreds of cards) would require substantial time. To solve the problem we implemented a data compression algorithm. The resulting memory card dumping time is about 20 *sec* per card

3.2.2 Data Collection Tool

The data collection tool serves three purposes:

1. Decoding the memory card dump that was sent using run length encoding algorithm
2. Managing the saved data for baseline and audit cards
3. Comparing the audit and baseline data to identify audit cards with potential problems.

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 allows to maintain the list of towns and districts that keeps track of the data collected for both baseline and audit cards, it records data sent from the AV-OS with a single button click, and compares all collected data, reporting any discrepancies. The comparison is done on the basis of our reverse-engineering the memory card layout by observing sample data and inspecting the firmware. 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 4 below. This allows quick assessment after data collection to identify potential problems.

3.3 Testing Procedure

Having extracted the data from the audit cards, our next task is to test and compare the audit data against the baseline obtained from the GEMS database. We first discuss the procedures outlined by the State in sampling the memory cards for the audit process, and some shortcomings in this sampling process. We then proceed to examine the contents of the memory card and offer a schematic

view of the contents of the memory card. We conclude the section with a brief discussion of the *.abo (AccuBasic Object) bytecode present in each memory card.

3.3.1 Audit Data

Audit data was collected for all the memory cards received prior to the elections. We also received a large number of memory cards after the elections. By the agreement with the State, we collected the audit data for such cards as well. We report the results for the memory cards received prior to the election, and separately for all cards received (before and after the election). The audit data was collected by using the modified firmware through the data collection tool created specifically for that purpose (for collecting audit and baseline data) as discussed in the previous sections.

Sampling of Memory Cards. Recall that each polling place received four programmed memory cards from LHS Associates. There are two AV-OS voting terminals in each polling place. 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 State election procedures, each precinct/district/polling place is supposed to have two AV-OS machines in "election mode" prior to the election. Only one of these machines is to be used during the election. The second machine is to be used only if the primary voting machine fails. Moreover, each district is also supplied with two backup cards (one per each machine). For example, the AV-OS machine may encounter a problems, display an error message, and fail (the meaning and symptoms of such failures are discussed in the Moderator handbook). In this case poll workers are required to shut down the faulty voting terminal and not attempt to fix or try to get the machine functioning again by any means. Once the faulty machine is shut down, the second machine is put into service. All the ballots from the first machine are supposed to be cast once again by using the second machine after the election ends.

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 randomly choose two out of the four cards in their possession, put them into the machine and run a test election. After testing these cards they need to place these cards in "election mode" and remove these cards from the AV-OS terminal. Then they apply the same procedure for the remaining two cards. However, this time, after placing the cards in "election mode" the poll workers need to seal the optical scan machines. Immediately after the testing is complete, they are required to randomly select one memory card per district and send these cards 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.

See Section 4.1 for some of our observations regarding the implementation of memory card sampling performed by the towns.

3.3.2 Baseline Data

We collected the baseline data in order to compare it against the audit data received from the towns. We received the database from LHS prior to elections and we used the same version of GEMS and AV-OS firmware to program the memory cards for collecting the baseline data. Again, as in the case of the audit data, after programming the cards we collected the baseline data by using the modified firmware and the same data collection tool that has an option of switching between the baseline and the audit data. After all corresponding data were collected, we run an appropriate comparison program to compare the baseline and the audit data. A detailed explanation of the comparison process is given in the next section.

3.3.3 Testing and Comparison

The data stored on the memory card falls into the following categories:

- **Status:** This indicates the current state of the memory card, such as blank, loaded with an election, set for election, running an election, or closed election.
- **Log:** This is the record of the history of the card after its initialization.
- **Ballot Data:** This includes the information about the ballot, including the district name, candidate names, and ballot layout.
- **Counters:** This contains all counters pertaining to the election, including the vote counts for each candidate, blank votes, and total ballots cast.

The actual status of a memory card being audited may vary from that of the baseline data, depending on the procedure followed by the poll workers prior to sending the card. Likewise for the log data. If the audit cards are properly set for election, then the counters should be zero. Otherwise, the counter section may differ from the baseline, which is always zeroed. The ballot data portion should never differ from the baseline.

3.4 Memory Card Format

In order to perform the memory card audit, it is imperative to understand the structure of the data on the memory card, so that the expected layout is established and that any deviations from the expected layout are identified.

We now describe the memory card format and overview the election data, bytecode, and race and candidate counters. Our findings are based on the examination of the firmware code of the AV-OS, and analysis of the data on memory cards. Although the analysis is performed without any technical documentation from the vendor, and in the absence of the source code, we are quite sure of our findings based on the systematic analysis of firmware binary code and by "eavesdropping" on the communication between GEMS and AV-OS. The analysis of the memory card content 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 information on the card and main description of the election. This segment includes:

- AV-OS version.
- Election Status.
- PIN number encoding.
- General Counters.
- References to Memory Addresses.
- District information.

Log: This segment of the memory card holds the actions performed by the users on the AV-OS machine. The log registers the action and the time that action was performed.

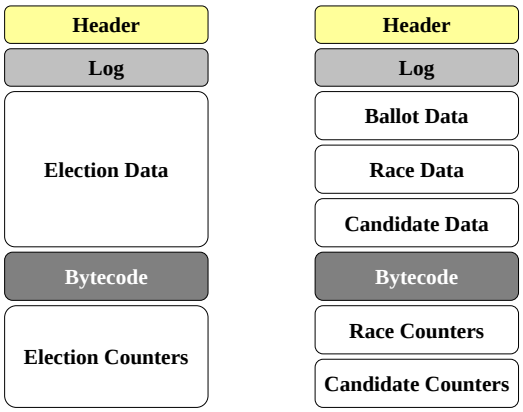

Figure 1: Left: General Memory Card Structure. Right: Further division of Election Data and Counters

Election Data: The election data segment consist of data in three categories:

1. **Ballot Data:** This segment contains information about the ballot layout used in the current district for the current election.
2. **Race Data:** This segment 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.
   - Number of candidates for the office.
3. **Candidate Data:** This segment of the memory card keeps 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 the executable code that is responsible for the reporting procedures associated with an election. For the scope of this audit, we did a manual decompilation of the Accu-Basic bytecode provided by LHS Associates for this election. Our goal was to verify that no extraneous (or malicious) functionality was present (injected) in the bytecode. The rules of translation from AB-bytecode syntax to Accu-Basic syntax used in the decompilation are described in detail in our earlier report[3]. The rules were derived by experimenting with the AccuBasic compiler available at the URL http://www.blackboxvoting.org. The source code for the 1.94 and 1.95 compilers is available at that site.

[3]Security Assessment of the Optical Scan Voting Technology from LHS Associates, UConn VoTeR Center, June 8, 2007.

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.

We defer detailed discussion of all technical aspects of the memory card format and related topics to our forthcoming extended technical report. The presentation of the audit results in the next section does not depend on these technical details.

4 Audit Results

We now present the results of the pre-election audit. As of December 25, 2007 we have received and examined 522 memory cards, out of which 378 cards were received prior to the election, and the rest were received in the following weeks. We present the results in two sets: one for the cards received prior to the election, the other for all cards received (before and after the election). The results of the audit are substantially similar for both sets. We start by discussing the issues that arose in the selection of the cards that we shipped to us.

4.1 Sampling Issues

We noticed a few discrepancies from the actual procedures taken by the poll workers and the required procedures as defined by the Office of Secretary of the State with regards to sampling the memory cards to be sent to VoTeR Center. This section details some of these discrepancies. The information in this section contains our observations and it is not to be considered as a critical remark regarding the procedures followed by the poll workers.

We observed that not all districts were able to follow the procedures discussed above. The primary and backup cards can be distinguished by the label on the card. The result is that a vast majority of the districts naturally chose to keep the "primary" cards and chose a "backup" card to be sent for the audit. Thus the cards were not chosen uniformly at random for the audit.

There is another issue that impacted the sampling process. Recall that each town was supposed to send the memory cards for each district to VoTeR Center. Unfortunately, some towns apparently misinterpreted the instructions and ended up selecting memory cards from (apparently) randomly chosen districts in the towns. In most cases, they sent the memory cards for half of the districts, however, in some cases we received only a single card for a town which has 24 districts. Only a handful of towns sent one memory card per each district as they were supposed to.

In the future it would make sense to define the audit explicitly 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 or distinguished in any way from the main cards[4]. Clearer instructions should help mitigate some of these discrepancies. Greater care should be taken to adhere to the instructions provided by the State.

4.2 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:

[4]This requirement was already communicated by the SOTS Office to LHS Associates for future elections.

(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", that is a few isolated bytes with unexpected values. (It is possible that these are errors that occurred during transmission.) The specks are not detected by AV-OS, and it does not appear that they interfere with normal AV-OS operation. Over 3% of cards contained "junk" data, that is the card format is unrecognizable and appears to contain random noise. Such cards are not readable by AV-OS and they are readily detected through pre-election testing by poll workers.

In the rest of the analysis the percentages are computed for the over 96% of the cards that were properly formatted and contained good data, i.e., the cards that did not contain junk data.

(b) Card Status: This refers to the current state of the memory card, such as blank (not programmed), loaded with an election, set for election, running an election, or closed election, and others.

No blank/unprogrammed but properly formatted cards were found. No cards with uploaded results were found. No cards with audit report printed were found. These are the expected results.

The plurality of the cards, over 46% were Set for Election, which is the desired memory card 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 vote were cast. This is problematic. This is most likely 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. Nonetheless, if poll workers are unaware of this policy then such a machine could result in incorrect election results. (It is worth reiterating that for the town in question, the Secretary of the State subsequently received copies of the printout that contained a correct zero-count report, indicating that correct procedures were in fact followed on the Election Day.)

(d) Election Count: This table shows the observed values of the election counter. Here 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.

	For cards received before election		For cards received after election	
	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: (Number of test elections)				
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: Memory card analysis summary: (a) card format, (b) card status, (c) counter status, (d) number of test elections performed.

4.3 Bytecode Analysis Result

We have decompliled the Accu-Basic bytecode that is loaded into each programmed memory card. After the analysis of the decompiled Accu-Basic bytecode we conclude that the bytecode provided by LHS Associates for the elections is safe to use. The bytecode performs the expected reporting functions. Note 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[5].

5 Discussion and Recommendations

Having performed and completed the audit, we believe that pre-election memory card audits are crucial in providing valuable and timely information necessary to ensure the integrity of our electoral system. This section contains the conclusions we draw from the pre-election audit process, and some recommendations on safe-use procedures.

1. Only one card was set for election with non-zero counters.

   Among all the cards that were subject to the pre-election audit process only one card was potentially dangerous in terms of compromising the election. The mentioned memory card was not only in a "set for election" status, but also had 19 votes cast. If such a card is carelessly used in an election, the results would reflect the 19 extra votes. However, this situation can be easily identified by a careful poll worker as the required zero report would not be printed in this case. Note that printing a zero total report prior the start of election is a requirement which cannot be ignored.

2. Several had non-zero counters, but were not set for election.

   Several cards had non-zero counters, which indicates that test elections were done by either LHS Associates or the corresponding district. However, the cards were not set for election. According to the procedures provided by the State this should not be the case. However, this situation is not potentially dangerous because once the cards are set for election all the counters would be automatically nullified and the zero total report printed. We should note that the set of counters used for pre-election testing and for the election itself is the same. However, AV-OS status bit identifies the state of the voting terminal. Consequently, if the counters are not zero but the machine is in pre-election mode, then this is treated as normal. Though, we should stress again that this is a violation of the procedures which poll workers should follow. All the cards should be in "election mode" and there should not be any non-zero counters.

3. Election mode was used for testing ballots in many precincts.

   Many precincts tested the ballots in election mode. However, after running the election they closed it. So the situation here is not the same as with non-zero counters in election mode. In this case, depending on what they did after closing the election, we encountered a few different scenarios. Some of them, after closing the election, set the cards back to "election mode". Thus, all the counters were nullified again. We could tell that they ran the election by looking at the status bit and noticing the corresponding changes in the log. Some of the precincts closed the election without setting the cards into "election mode". This situation is again not a potentially dangerous situation. However, this does indicate that poll workers did not follow the procedures described above.

[5]Security Assessment of the Optical Scan Voting Technology from LHS Associates, UConn VoTeR Center, June 8, 2007.

4. No detected ballot data or bytecode corruption.

   During the data analysis we have not noticed any corruption of the ballot data or the bytecode. The ballot layout of the audit cards were identical to the ballot layout of the corresponding baseline data.

5. Surprising number of "junk" cards

   By saying that the card is "junk" we understand that the card was not programmed correctly. When you put the card containing the "junk" data into the AV-OS terminal it issues a prompt requesting to format the card. We do not believe these cards were damaged in shipping. Consequently, it appears that these cards were never tested by LHS Associates. Some of these cards were tested by the districts, however: some of the cards had a note attached to it indicating that the card was bad. Given that we could see that not all the districts followed the outlined memory card testing procedures correctly, we recommend that all the programmed cards undergo the same testing procedures without any differentiation between backup and main memory cards. Among the audited cards we detected 3.5% of the cards containing junk data. This percentage is very big and this issue has to be resolved in the future.

6. Improving and making more explicit instructions for the districts.

   We found the memory cards to be in a variety of different states, with large percentages of cards not being in the prescribed states. It may be the case that the instructions to poll workers were unclear, or that the poll workers were unable to follow the instructions. If so, we recommend holding training sessions explaining to poll workers exactly what needs to be done to prevent this situation in the future.

[End]