



Pre-Election Audit of Memory Cards for the November 2009 Elections

Version 1.2, April 20, 2010

Summary

The Voting Technology Research (VoTeR) Center at the University of Connecticut performed a pre-election audit of the memory cards for the Accu-Vote Optical Scan tabulators that were to be used in the November 2009 Elections. The cards were programmed by LHS Associates of Methuen, Massachusetts, and shipped to Connecticut districts for use in the elections. The VoTeR Center received in total 491 memory cards from 481 districts before the elections. This document reports on the findings obtained during the audit. The 491 cards represent over 80.6% of all districts, thus the audit is broad enough to draw meaningful conclusions.

Among the 491 cards representing those intended for use in the elections, 87% were properly programmed. 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. Concerning the remaining cards, 42 or 9% were found to contain “junk” data, that is, they were unreadable, which is easily detected by the tabulators; had a card contained junk data at the time of the election, it could not have been used. It was determined that weak batteries is the primary cause of this and a separate report will document our findings.

Two additional cards did not match the pre-election baseline: one card had a different candidate name due to late replacement, another had a different district number (1 vs. 2), otherwise being properly programmed. There are 76 cards that, although not presenting an immediate security concern, were found in unexpected states or contained unexpected timing of events. For example, 23 card duplication events were found prior to the election. We note that the adherence to the election procedures by the districts is improving, however analysis of the audit logs indicates that the established procedures are not always followed; it would be helpful if reasons for these extra-procedural actions were documented and communicated to the SOTS office. One card contained a few unexpected data characters beyond the range of memory known to be used by the tabulators.

In summary, (a) 87% of the cards representing those intended for use in the election were properly programmed, (b) cards with junk data continue to be a problem; we believe we know the reason and are finalizing the findings, (c) a number of cards show that the pre-election procedures are not followed uniformly and that cards continue to be duplicated; we recommend that in addition to the prohibition of duplication of cards, that whenever there is a perceived necessity to duplicate a card, the reason be documented and furnished to the SOTS office. The audit was performed at the request of the Office of the Secretary of the State.

1 Preface

The Voting Technology Research (VoTeR) Center at the University of Connecticut conducted a pre-election audit of the memory cards used in the Accu-Vote Optical Scan (AV-OS) tabulators in the November 2009 elections in the State of Connecticut. The audit was performed at the request of the Office of the Secretary of the State of Connecticut.

The memory cards were programmed by LHS Associates of Methuen, Massachusetts, and provided by LHS to the districts in Connecticut. The audit was performed on a set of memory cards that were delivered to the VoTeR Center from the towns, where the cards were randomly chosen for pre-election testing.

The cards are tested as they arrive, but the complete audit cannot be completed before the election. The majority of the pre-election cards arrived at the Center during November, 2009, with about 90% of the cards arriving before Thanksgiving. If noteworthy irregularities that might affect integrity or security are detected, they are reported to the SOTS office without delay. Complete preliminary results were reported to the SOTS office on December 12, 2009. The report was subsequently revised to address outstanding issues and to improve the presentation.

The memory cards were subject to several integrity tests. A comprehensive overview of the procedures followed by the VoTeR Center personnel in conducting such audits is presented in prior reports¹. We do not repeat here the description of the engineering that was performed to enable the audit, including the log analysis, and the technical setup used in the tests.

In this report, we present the objectives of the pre-election audit and the audit results. The audit process included testing, comparison, and analysis of the data collected during the audit. The procedures followed in this audit 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. Audits provide feedback, in quantitative measurements, about the quality with which the electronic voting system supports the electoral process. These quantitative measurements characterize the effectiveness of the electronic voting system support. If, for example, a performance requirement existed upon the vendor for percentage of functioning memory cards, the quantitative measures of performance could be compared with the contractual requirement. Similarly, quantitative measures facilitate the selection of targets for process improvement.

This report is a high-level, non-technical presentation of the audit results and it omits technical details. We also note that we did not use any vendor documentation regarding the design and the internals of the AV-OS terminal.

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.

¹ Pre-Election Audit of Memory Cards for the November 2007 Connecticut Elections. UConn VoTeR Center, Version 1.0, January 24, 2008. Available online at <http://voter.engr.uconn.edu/voter/Reports.html>. Automating Voting Terminal Event Log Analysis. UConn VoTeR Center, EVT09, Montréal, Québec, Canada, August 2009, available at <http://voter.engr.uconn.edu/voter/wp-content/uploads/evt09.pdf>.

The work of VoTeR Center at the University of Connecticut is funded by the Secretary of the State (SOTS) for the state of Connecticut, and we function in close contact with the personnel at the office of the SOTS. 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 laboratory 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. The VoTeR Center is not involved in establishing the state's policies for procuring the voting technology, but limited to providing technical expertise on, and evaluations of these technologies before deployment and during the 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 continue to assist the state in developing safe use procedures for the Optical Scan terminals. The procedures in place for the election include strict physical custody policy, tamper-resistant protection of the equipment, and audits. The Center provides ongoing recommendations to improve the security of elections based upon our findings in evaluating the voting equipment and conducting pre- and post-election technological audits.

2 Introduction

We start by surveying 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 Accu-Vote 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 systems currently in use in the state of Connecticut contain the firmware version 1.96.6. This model 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.
- 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. In the state of Connecticut, GEMS is not used for central tabulation of election results.
- The memory cards are 40-pin, nominally 128KB cards. The memory card is installed into to the 40-pin card slot of the AV-OS. It is worth mentioning that recent (summer 2009) instances of this card were a custom product of Smart Modular Technologies produced for Premier Election Systems, Inc., and that commercial-off-the-shelf readers and writers for this card have not been found.

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, called bytecode, is written in a proprietary symbolic language. Such executable files are identified by means of the suffix .abo (AccuBasicObject). The installation

of the GEMS software on the PC contains several databases that include the data and ballot layout corresponding to the districts of the state of Connecticut, as well as the bytecode for AV-OS.

2.2 Goals of the Pre-Election Memory Card Audit

The VoTeR Center prepares for and implements memory card audits at the request of the SOTS. The primary goal of the pre-election audit is to obtain quantitative measures of the integrity of the contents of the memory cards.

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 onto each 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.

For the pre-election audit the VoTeR Center examined 491 cards received as of April 20, 2010. These cards correspond to 481 distinct districts in Connecticut. These memory cards were delivered to the Center by the towns, where the cards were randomly chosen for pre-election testing. Preliminary audit results were communicated to the SOTS Office on December 12, 2009.

The contents of the cards were then extracted and compared with the intended contents using the GEMS database as the reference; this portion of the audit process is semi-automated. 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, any deviations in the bytecode, the state of the counters and the content of the audit logs. These audit logs contain significant events in the life of a card since the last time it was formatted.

2.3 Overview of the Audit Results

2.3.1 Properly Programmed

The total of 491 cards were received and tested by the VoTeR Center. Among these 491 cards, 425 cards (87%) were found to have been properly programmed for election through direct load from the GEMS database. 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. Correspondingly, 13% of the cards were found to not be in the expected state (as we explain later, this percentage consists of twenty-three (23) cards that are properly programmed, but with audit log indicating duplication events, one (1) card that contained no election data, and forty two (42) cards that contained “junk” data.)

2.3.2 Usable for Election (Properly Programmed Cards and Duplicated Cards)

Usable cards are those properly programmed, including the twenty-three (23) cards whose audit log contains duplication events. Among the 491 cards, 448 cards (91%) were found to have been usable for election. These cards contained valid ballot data and the executable code on these cards was the expected code; for those which had been duplicated, certain bytes not matching the baseline can be used to determine that a duplication event occurred.

2.3.3 Unusable Cards (Cards with Junk Data or Blank)

The audit identified forty two (42) cards, or 9%, that contained “junk” data; these cards are unreadable by the tabulators, and easily detected as such. This is a high percentage of faulty/unusable cards. We note that this is consistent with the percentage reported for the pre-election audit of November 2008 elections. The percentage is lower than detected in the post-election audit for the August 2008

primary (15%), but higher than detected in the pre-election audit for the August 2008 primary (5%), post-election audit for the February 2008 primary (5%), post-election audit for the November 2007 elections (8%), and pre-election audit for the November 2007 elections (4%).

We have determined that weak batteries are the primary cause of this and we will document our findings in a separate report.

Additionally one card was found to be blank. It was formatted, but not programmed for election. Such cards are identified by the tabulator and cannot be used in the election, thus not presenting a security concern.

2.3.4 Cards with Duplication Events

The audit identified twenty-three (23) cards where the audit log indicates card duplication events. Card duplication is not authorized per SOTS Office instructions. Otherwise the cards were properly programmed for elections.

2.3.5 Candidate Name Differences

One card (0.2%) contained a different candidate name. This was due to a very late replacement of a candidate.

2.3.6 Race Definition Differences

Five cards from Guilford contained single byte (character) differences from the baseline. This difference appears in the Board of Education race. It was determined that this was due to a correction: “vote for 5” was corrected to be “vote for 4”. Thus the cards were correct, and the error was in the original database.

2.3.7 Minor Differences

Here we describe cards that contained minor differences detected by the audit that did not present security concerns. These differences did not affect the cards’ usability.

One card (0.2%), that for Hartford District 1, contained a single letter difference in the district designation (Hartford District 1 vs. 2). Comparison of the card content with the baseline reveals that this card, despite being designated District 1, maintains the data corresponding to District 2. Follow up with SOTS office personnel determined that this is due to the different naming of otherwise identical cards for a specific district.

This card’s audit log also shows duplication events, thus raising the concern that card duplication may introduce mismatched programming.

2.3.8 Extraneous Data in the Unused Part of the Card

0.2% of the cards (one card) was properly programmed, but contained a few bytes of noise (or “specks”) that are located in the unused part of the cards. It does not appear that these differences have any impact on the proper functioning of the cards. (Given the rarity of such differences it is difficult to establish their cause.)

2.3.9 Small Capacity Cards

The audit identified two cards of non-standard capacity (32KB instead of 128KB). The tabulator uses only the first 32KB of the memory cards, so this is not a security concern, however all cards purchased for use in Connecticut are 128KB, which means that these two cards either came from a

different state or were erroneously chosen for use in Connecticut. Subsequent follow up with LHS confirmed that these cards were sent to Connecticut by mistake; LHS will address this for future elections.

2.3.10 Additional Observations

There are 76 cards (15%) that were properly programmed, but were found in unexpected states or contained unexpected timing of events. This does not necessarily present an immediate security concern, however the findings indicate that the established procedures are not strictly followed in some cases. It would be helpful in improving the measures of quality of protection of the electoral process, if electoral officials could document the reasons for any exceptions they feel it has been necessary to take, and communicate this to the SOTS office.

We detail these finding in the next section. One contributor to the cards being flagged during the audit is the short time interval prior to an election when the cards were programmed. Part of the establishment of quantitative measures of the electoral process, described later in this report under recommendations, would include a determination of this minimum time interval.

3 Audit Results

We now present the results of the pre-election audit in more detail. For the November 2009 elections we received and examined 491 cards. These cards were programmed by LHS. The cards were shipped by the districts to the VoTeR Center for the purposes of the pre-election audit. The high level breakdown of the received cards is as follows:

- 491 were received for audit
- 42 were unreadable, that is, they contained junk data
- One card was not programmed (full of zeros)
- Three cards were in “Election Closed” status
- 272 were set to be used in the elections
- 173 were not set to be used in the elections (in effect serving as back-up cards)

3.1 Memory Card Data Audit Results

Table 1 shows the frequency of various states observed on the audited memory cards for the 448 cards that were readable, and also for all cards received by the VoTeR Center. The data is presented in three parts, corresponding to items in three categories:

(a) **Card Initial State:** 425 cards were properly formatted and contained good data.

One card (0.2%) contained a different candidate name. This was due to a very late replacement of a candidate.

One card (0.2%) contained a single letter difference in the district designation (Hartford District 1 vs. 2). This discrepancy has been explained: It is due to different naming of otherwise identical cards when multiple cards are programmed for the same district.

One card (0.2%) contained data that was satisfactorily explained, but also included a few “specks”, that is a few isolated bytes with unexpected values. Such specks might not, on the

	Cards Usable in the Election		All Cards	
	Number	% Total	Number	% Total
(a) Prior to Use by District				
Good Data, Clean Card	446	99.3%	446	91%
Different Candidate Name also had specks	1	0.2%	1	0.2%
Different District Number	1	0.2%	1	0.2%
"Junk" data	0	0%	42	9%
Not Programmed	0	0%	1	0.2%
Totals:	448	100%	491	100%
(b) Phases of Use				
Not Programmed	0	0%	1	0.2%
Not Set for Election	173	39%	173	35%
Set for Election	272	61%	272	56%
Election Closed	3	0.6%	3	0.6%
Results Print Aborted	0	0%	0	0%
Results Sent/Uploaded	0	0%	0	0%
Audit Report Printed	0	0%	0	0%
Preparation Warning	74	16.6%	74	15%
Duplication Events	23	5.1%	23	4.7%
Session Starts	9	2.0%	9	1.8%
Test Election Warning	76	17%	76	15%
(c) Card & Counter Status				
Election Closed, Non-Zero Counters	3	0.6%	3	0.6%
Election Closed, Zero Counters	0	0%	0	0%
Results Print Aborted, Non-Zero Counters	0	0%	0	0%

Table 1: Memory card analysis summary: (a) Card Initialization, (b) Card Record of Electoral Procedure, (c) Counter Status.

basis of being beyond the memory address range necessary to support an election, interfere with electoral process. These cards were otherwise properly programmed. A more thorough examination of the phenomenon of “specks” is in order.

- (b) **Card Record Of Electoral Procedure:** As electoral procedures are carried out, a record of certain events is made in the log section of the memory card. From this record it is possible to construe the process step in which the memory card was found, such as blank (not programmed), loaded with an election, set for election, running an election, or closed election, and others.

Two hundred and seventy two cards (61%) were found having “Set for Election” status. This is the intended status for pre-election cards that went through pre-election testing at the districts.

173 cards or 39% had “Not Set for Election” status. These cards did not undergo the complete pre-election testing procedure at the towns, indicating incomplete adherence to the established procedures, however this is not a security risk. If such a card was used on the election day, the election officials would set the tabulator into election mode before opening the polls — this resets the counters of the card to zero and changes the status of the card to “Set For Election”.

One card was found to be blank/unprogrammed but properly formatted. From the log of the card we conclude that it was formatted at its district. This could have happened either by accident, or if the card contained junk data and the election personnel decided to format it.

Audit Log Analysis Results

The AV-OS software records various events of significance in the audit log of its memory card. The automated audit log analysis reads this information and examines the reported sequence of events. Rules for the appropriate timing of events, such as when, relative to election day, the races and candidates should have been established on the memory card are readily expressed. The dates reported in the log can be checked against the rules. Here we report on the findings based on the audit log analysis. (We are continuously refining the log analysis procedure so it can be tuned to focus on the significant events and not issue warning for events that are considered to be routine or benign.)

- (1) 9 cards (2%) had more than 10 “session start“ events. This refers to machine restarts. If the election personnel considers it necessary to restart the machine for any reason, this should be documented.
- (2) 23 cards (5.1%) contained duplication events in their logs, with 2 cards indicating more than one duplication. There should be no reason to duplicate the cards. One possibility is that duplication was performed when cards containing junk data were discovered during testing. It is strongly recommended that duplication not be performed at districts and that all improperly programmed cards are reported to the SOTS office as soon as this is discovered. In the event someone decides it is necessary to duplicate a card, that person should document the reason and circumstances and should ensure this information is supplied to the SOTS office.
- (3) 24 cards (5.4%) had a “Zero Totals Report” printed before the date of the election. This can happen if one starts a machine before the date of the election after setting it for elections.
- (4) 60 cards (13%) had activity deserving a warning about initialization. These warnings are responses to unexpected dates — either too early or too late — for the initialization activities. (These dates are common sense and they are set arbitrarily for log analysis.)

- (c) **Counters on Card:** Three cards (0.6%) had “Election Closed” status; none of these had Non-Zero counters. Had any had non-zero counters, they would have been in the intended status for memory cards that had been used in the election. It appears that these cards were used for pre-election testing, but instead of running a test election the towns put the cards through an election.

It appears, from the duplication events and the zero totals reports, that proper procedures are not followed uniformly.

3.2 Bytecode Analysis Result on the Readable Cards

We have analyzed the AccuBasic bytecode that is loaded into each programmed memory card. Based on the analysis 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 AccuBasic bytecode.

As a new version of code for the AV-OS itself is expected, the AccuBasic bytecode analysis support might need to be updated to correspond.

3.3 Additional Observations and Details

Here we give additional information obtained from the audit log analysis. The audit log on each card contains reports of events. These records can be interpreted to obtain some information about the process steps undergone by the memory card. The details of the electoral procedure steps reported above are determined in part by the log analysis.

- Preparation for elections: Among the cards submitted for pre-election audit there are still many cards (about 39%) that are not set for election. All cards need to undergo pre-election testing and be set for election by the election day.

It is possible that test elections were performed, however, the cards were not set for election by the districts. In any case, this indicates that pre-election procedures were not followed. All cards not used in the election should have “Set For Election” status with zero counters.

- Card duplication: The SOTS office instructed the municipalities not to duplicate cards. If there is any perceived reason for cards to be duplicated, the SOTS office must be promptly informed. Duplicating cards creates cards that have not been directly produced from the election database (GEMS at LHS), and should not be allowed to be used in the elections until proper procedures are developed. It is recommended that the SOTS office offer training through ROVAC to reinforce that stated no-duplication policy.
- Additional details for observations documented earlier in this report.

1. A card with data corresponding to a different district, also duplicated:

HARTFORD-DISTRICT_1-0003152

This card contains data for District 2. The card is also duplicated. No other differences are observed.

2. Late replacement of a candidate resulted in a difference between memory card and baseline database.

NORWALK-DISTRICT_A2_OFFS-0004003

Candidate Replaced: Office: 1st Tax Commissioner Kenneth J. Slapin -> Frank N Zullo

3. All five cards from Guilford contained single byte (character) differences from the baseline. This difference appears in the Board of Education race. It was determined that this was due to a correction: "vote for 5" was corrected to be "vote for 4".

GUILFORD-DISTRICT_1-0004484

GUILFORD-DISTRICT_2-0005623

GUILFORD-DISTRICT_3-0004492

GUILFORD-DISTRICT_4-0004497

GUILFORD-DISTRICT_5-0004501

Thus the cards were correct, and the error was in the original database.

4. Two non-standard cards of 32KB size. These cards are usable, but they are not the 128KB cards procured by Connecticut.

NEWINGTON-DISTRICT_4-0002764

SIMSBURY-DISTRICT_2-000580

These cards were used by LHS for Connecticut elections by mistake; LHS will address this for future elections.

The audit indicates that we have still a large number (66, or 13%) of cards not in the expected state. While it may be the case that the instructions to poll workers were unclear, it might also be that the poll workers had reasons for not following instructions; in this latter event, for the purposes of improvement in the support by the electronic component of the election process, it would be helpful if the poll workers would document why these steps were taken counter to the expected procedures.

4 Recommendations

The current level of unusable (junk) cards, approximately 10%, is high. We have determined that weak batteries are the primary cause of this. A forthcoming report will explain this and provide the technical detail. Our recommendation is that the batteries in all cards are replaced prior to programming them for the next election.

It appears from the available data that established pre-election testing procedures are not consistently followed. The itemized list of recommendations follows.

- It might be helpful if the SOTS office would re-issue procedures and offer training.
- It is important to reiterate that cards must never be duplicated by individuals local to the election. It would be helpful if such individuals desiring to duplicate cards would note their reasoning in the moderators' logs.
- It is important for the individuals local to the election to report pre-election testing results (and any card problems) to the SOTS office as soon as possible upon completion of tests.
- It is important for the individuals local to the election to report any unexpected behavior of machines that seemed to necessitate a restart or a memory card reset to the SOTS office. It would be helpful if moderators' logs contained records of machine restarts, perceived causes, and reasoning for the restart or reset.

[End]