Determining the Causes of AccuVote Optical Scan Voting Terminal Memory Card Failures*

Tigran Antonyan Nicolas Nicolaou Alexander A. Shvartsman Therese Smith
Computer Science & Engineering, University of Connecticut, Storrs, CT 06269, USA
{tigran,nicolas,aas,tms08012}@engr.uconn.edu

Abstract

Optical scan (OS) voting systems play an increasing role in the United States elections, with over 40 states deploying such systems. The AccuVote optical scanners (AV-OS) manufactured by ES&S account for over 20% of all OS systems. OS systems typically use removable media (cards) to provide election-specific programming to the scanners and to convey precinct election results for central tabulation. Several reports document occurrences of AV-OS memory card failures, with up to 15% of all cards failing in some cases.

This paper reports on determining the causes of memory card failures that lead to complete loss of data from the card. An initial experimental analysis identified the *battery discharge* as a significant part of the problem. This finding led to the question of the dependability of the built-in function of the AccuVote OS system that issues a warning when the memory card contains a low-voltage battery. We identified the components used to implement this function in one type of AccuVote memory card. Using the specifications of the commodity batteries that are used in these cards, we determined the time interval from the instant when a battery warning is issued by the AccuVote to the point when the battery does not have enough voltage to retain data on the memory card. We show that such interval is about 2 weeks. Thus timely warnings cannot be provided to protect against battery discharge and loss of data during the election process. The factors contributing to the short warning interval are likely to apply to other battery-backed RAM cards, such as those used in the ES&S Model 100. Recommendations for mitigating the problem are made in light of the expected behavior of the warning system.

*Research funded by the Secretary of the State of Connecticut and performed at the Center for Voting Technology Research at the University of Connecticut.

1 Introduction

A number of reports in recent years documented security and integrity vulnerabilities associated with electronic election systems (e.g., [24, 3, 19, 32, 34, 13, 14, 33, 10, 16, 17, 7, 8]). While it is extremely important to understand and mitigate the risks of misuse and tampering with electronic voting systems, it is also important to ensure that the systems are reliable, and when this is not the case, to analyze the problems and develop solutions leading to more dependable election systems.

Over 55% of the counties nationwide across more than 40 states incorporated OS election systems for the November 2008 Presidential Elections, with over 20% of those counties deploying the AccuVote Optical Scan (AV-OS) tabulators from ES&S (formerly Premier Election Systems, formerly Diebold) [30]. These systems normally use removable memory cards to provide election-specific programming to the tabulators, and to convey election results to the election management systems (EMS) for aggregation. It has been widely reported that the AV-OS memory cards have been malfunctioning at an unacceptably high rate.

Background and motivation. This work is motivated by the experience of using AV-OS systems in the State of Connecticut, and our own work on audits in the state. We study AV-OS memory card malfunctions that cause the cards to lose their data (e.g., see the informal compendium at VotersUnite.org). This is typically detected when a programmed card is inserted into the OS tabulator prior to an election. In other cases this is detected when attempting to load election results from a memory card to EMS for aggregation, for example, one report from Washtenaw County, Michigan describes some cards that “were wiped clean" of their data following an election [23]. There were also reports of memory card failures during the elections. Such failures may be catastrophic for DRE systems, however they are more benign for OS systems (possibly constituting denial-of-service) due to the ease of detection and the existence of voter-verifiable paper ballots. In any case, the magnitude of reported failures is a serious concern. E.g., 4.4% of cards in Volusia County, Florida, November 2006, over 9% card failures in two other (unnamed) counties in the same election in Florida. Other reports claim even higher failure rates. Unfortunately, while identifying a perceived problem with memory cards, these reports do not contain any technical data that can shed light on the causes of the problem and do not provide direct evidence that data is indeed lost in malfunctioning cards.

The first specific data on the AV-OS memory card failures appears in recent reports on technical audits in the State of Connecticut [29, 28]. The reports indicate that anywhere from 3.5% to 15% of the memory cards examined in audits are found to be faulty. The tabulators are not able to read such cards, but using special instrumentation it is possible to extract the contents of such cards. When any such card is read, it is revealed that it contains a sequence of arbitrary byte values without any apparent structure or format. In particular, these cards are distinct from properly formatted, but not programmed cards.

Frequent occurrence of such card failures for OS may lead to the following denial of service situations:
1) Loss of card data before or during an election makes it impossible to conduct the election, unless a replacement is secured or is available in a timely manner. This incurs substantial overheads associated with preparing redundant cards before elections, and card failures result in delays and interruptions on the election day.
2) Loss of card data after an election results in the complete loss of the electronic election results for the corresponding precincts. This makes it impossible to perform central aggregation of election results using an EMS (in the jurisdictions where such aggregation is used, e.g., in Connecticut this is not done).
3) Loss of card data after an election makes it impossible to audit the (lost) data on such cards. In particular, audit logs stored on the cards are also lost.

This report documents the results of the technical investigation whose goal is to identify the main causes leading to the loss of data on AV-OS memory cards. We are able to present strong evidence that the major cause of this loss of data is the depletion of the battery contained in the memory card. We also provide an explanation for why the function implemented in the AV-OS system to warn of the depleted battery condition is ineffective and cannot be relied on to assess predictably the condition of the on-board battery.

Summary of the results. For the purpose of this study, 105 memory cards for the AccuVote Optical Scan (AV-OS) system were retained from the November 2008 elections in Connecticut. 55 of these cards were identified as the cards that lost their data. The remaining 50 cards formed the control group consisting of cards that did not fail during the same election.

The AV-OS memory cards, marketed by ES&S, are the 40-pin 128 KB cards that essentially comply with the Seiko Epson specification [27]. The cards employ RAM that is volatile. Each card contains a coin-sized 3V battery (2016 type) required by the card to maintain its memory. The AV-OS system incorporates a function that issues a “low battery" warning. When so indicated, it is prudent to replace the battery before using the card. Ideally, when no such indication is issued by the system, the battery has sufficient charge to enable the card to maintain its memory (for a certain period of time).

The goal of this work is to explore the conjecture that the depletion of the on-board battery on these cards is a major factor causing the loss of data. If weak batteries are indeed the cause of the memory loss and given that the good use procedures demand that the battery is replaced upon the low battery warning before the card is programmed, we also consider the adequacy of the implementation of the AV-OS low battery warning system.

To this end, we conduct a case study of the most common memory cards used with the AV-OS terminals (there are two known types of cards in use in Connecticut). The contributions of this work are as follows.

1. We conducted tests on 55 memory cards that lost their data in the November 2008 elections. We programmed these cards with valid data, and we observed the state of these cards over time (at least four weeks). For those cards that failed to retain data, we replaced their batteries and we repeated the test. We contrasted the results for these cards with the results obtained from a test on a control set of 50 cards. Our findings present strong evidence that battery depletion was the cause of the data loss.

2. The memory card provides two quantities relevant to the conversion of the battery behavior to the lifetime of the memory card data: (i) the amount of energy discharged from the battery as a function of time, and (ii) the voltage level that triggers the AV-OS low battery warning. Given these parameters we computed the time from the appearance of the low-battery indicator until the data are lost due to battery discharge. We call this time period the warning time, and we estimate this time to be about 2 weeks for these memory cards. In light of this time being so short, the frequency with which memory cards lose their data is explicable, and a change is warranted.

3. For the typical election process in Connecticut, we identify the time when fresh batteries can be installed and the intervals during which the memory card depends upon battery power. We claim that, for memory cards whose components behave within their respective specifications, the warning time provided by AV-OS is inadequate to guarantee the retention of data for the duration of the electoral process. As a corollary, data retention cannot be guaranteed for any duration beyond the elections, as may be required by some jurisdictions.
4. Where battery-backed memory cards are employed, we recommend supplementing the vendor instructions for battery handling. In particular, we recommend that for each election, consideration be given to the age of the batteries used with the cards. If the time of the most recent battery replacement is more than a threshold amount of time for the specific battery (discussed later in this paper) in the past, such batteries should be replaced before the election to mitigate the frequent occurrences of data loss. Given that not all batteries are created equal, some lasting substantially longer than others, it is prudent to obtain and examine battery datasheets from the respective manufacturers to obtain the best value. Lastly, in the longer term, we recommend designing and using cards with intrinsically non-volatile memory.

Broader considerations. Our study focuses on one particular optical scan system that employs battery powered memory cards, the ES&S AccuVote Optical Scan (AV-OS), as used in Connecticut and several other states. We believe our results are applicable to other election systems that use battery powered removable media. This merits future study, however, as of this writing we have only access to the election systems in Connecticut. Other electronic voting systems with battery-backed memory cards (cartridges) include the ES&S Model 100 [26], corresponding to 36% of all counties using OS systems, and the Optech III P Eagle [18], corresponding to 11% of all counties. The Sequoia AVC Advantage DRE (Direct Recording Electronic) is another example of an electronic voting system using battery backed RAM [31]. While there are no formal reports of memory card malfunctions in these machines, it is prudent to conduct investigation of memory card dependability in these and similar systems.

Our recommended solution to replacing the batteries before every election is simple, but it comes at a cost. A state using AV-OS (or another similar system) will have many thousands of cards, and while batteries can be bought in bulk at less than $1 per battery, there are likely to be substantial labor costs, and costs associated with disposing a large number of batteries. It will be important to assess these costs and to examine alternatives, such as keeping track of the age of each battery and replacing only those that are at a higher risk of failing. A pilot test should also be conducted to to assess these costs and the effectiveness of the proposed solution. Another alternative is to develop plug-compatible memory cards that use non-volatile memory. This may be particularly important for those jurisdictions that require that all election data, including electronic, must be retained for at least 22 months.

Related work. A similarly critical problem of detecting when a battery needs to be replaced or recharged has been faced in the setting of pacemaker batteries [6, 25, 22, 20, 11, 12]. In the time before the availability of transcutaneous recharging of pacemaker batteries, a surgical procedure was scheduled to replace the battery. As not all patients' batteries discharged within the same time interval, some method of assessing when to replace the battery was desired. Some pacemakers paced at a reduced rate when the battery life remaining was short. Whatever the observable signal is, the amount (in time) of warning given by the signal corresponds to the time interval from when the warning signal is detectable to the time the performance of the battery-supplied system becomes unacceptable.

Paper outline. In Section 2 we present historical observations about the loss of data in cards that were examined during the technical audits. In Section 3 we present the details of our experiments. In Section 4, we present our analysis leading to the determination of the causes of memory loss, and we provide an estimation on the warning time for battery-backed cards. In Section 5 we give recommendations for mitigating the short warning time problem. Section 6 contains conclusions from our investigation and general recommendations on how to decrease the occurrence of card failures.

2 The Setting

The State of Connecticut introduced the AccuVote Optical Scan (AV-OS) election systems in 2006, together with implementing audits to mitigate the risks associated with security and integrity issues in using electronic election systems. The audits include post-election hand counted ballot audits covering 10% of the voting districts and technical audits of the AV-OS memory cards, performed before and after each state-wide election.

The AV-OS tabulators use removable, battery powered memory cards that are programmed prior to an election with the information pertaining to the specific contest configuration in each voting district. The memory card used in Connecticut is a 40-pin 128KB card, in many respects compatible with the Seiko-Epson datasheet [27]. In additional to the contest configuration, each memory card also stores the counters representing the number of votes cast for the candidates and propositions and the audit log (as well as additional data) [1].

There were over 1,000 polling places (inclusive of absentee) in the November 2008 elections in the State of Connecticut. Each polling location has four memory cards. One of the four cards is randomly selected for the pre-election audit. One of the remaining is normally used in the election, while the balance of two cards serve as backups. In total, there are about 4,000 memory cards in Connecticut. Note that for physical security, identification, and sealing purposes, the memory cards in Connecticut have tamper-evident, self-adhesive label that also covers the battery compartment.

The technical audits determined that a non-trivial percentage of the memory cards lost their data at some point after being programmed for election. The examination of the cards that lost data revealed that the contents of such cards appeared as an arbitrary, near random sequence of bytes (characters). The AV-OS systems cannot use such cards, recognizing them as invalid (and offering to format these cards). Thus this does not present an immediate security issue, however the substantial percentage of such cards observed in each election raises the concern of a non-malicious denial-of-service problem.

Table 1 presents the percentage of cards that lost their data, as discovered during the audits of five different elections. The pre-election audits are generally performed by randomly drawing one of four cards from each district before the election, and the post-election audit examines cards used in the elections for the voting districts subject to the 10% hand-counted ballot audit. The actual number of cards that lose their data could even be higher, given that in some cases cards are reprogrammed before the election when cards with lost data are encountered during the logic and accuracy tests.

Several hypotheses explaining the causes of data loss on memory cards were tested, but did not yield even a remotely significant statistical difference with respect to control group. For example, it was hypothesized that memory cards might be damaged in some electromagnetic way during transport, however no differences in the occurrence of data loss were observed for the cards that were transported using a common carrier vs. the cards that were transported using a dedicated courier. Another test revealed no differences in the occurrence of lost data for the cards that were "cold booted" where the cards are inserted prior to starting the tabulator and for the cards that were "hot booted" where the cards are inserted after starting the tabulator.

However, and not surprisingly, it was determined that the removal of the battery from the memory card results in loss of data. Replacing the battery reinitializes the memory to some apparently random, arbitrary data. Given that the state of the card after the replacement of the battery (e.g., random looking data) was essentially the same as the state of the card that lost its data with battery in place, the conjecture was made that depleted batteries caused loss of data. What was somewhat surprising is that the AV-OS function designed to alert the user that the battery is low did not do so consistently for the cards that lost their data. This led to the investigation that encompassed both the experimentation with the cards that lost their data and the assessment of the low battery function of the AV-OS itself.

We report our findings in the next two sections. We describe how much warning time can be provided by the AV-OS battery warning indicator; the report also draws important distinctions between failure modes occurring in cards used in elections. Using a case study, we also provide the warning time for the most common type of memory cards used in the AV-OS. Because the achievable warning time is short, a recommendation about battery replacement is provided.

3 The Symptoms

As shown in Table 1, the percentage of cards that lost their data ranged from the low 3.4% in the audit of November 2007 elections to the high 15.4% in the audit of August 2008 elections. The failure rates fluctuate and there does not seem to be a recognizable pattern in these observations (one important variable is not captured in these statistics, and that is whether or not, and when, the batteries were replaced, and in what cards).

This section presents an experimental investigation to determine whether the batteries that power the memory cards may be responsible for the loss of data. In addition we observe the physical condition of the memory cards and the function of the AV-OS tabulator that informs the users that the card battery is depleted.

3.1 Experimental Setup

We conducted experimental tests on 55 memory cards that lost their data in the November 2008 elections. We programmed these cards with valid election data, and we observed the state of these cards over time. For those

Audit	Election	% Cards with Data Loss
Post-election	November 2009 election	12%
Pre-election	November 2009 election	9%
Post-election	November 2008 election	8.9%
Pre-election	November 2008 election	8.9%
Post-election	August 2008 primary	15.4%
Pre-election	August 2008 primary	5.4%
Post-election	February 2008 primary	4.8%
Post-election	November 2007 election	8%
Pre-election	November 2007 election	3.4%

Table 1: Historical occurrence of cards with data loss

cards that failed to retain data, we replaced their batteries and we repeated the timed test. We contrasted the results for these cards with the results obtained from a test on a control set of 50 cards from the same election.

We designed the timed memory card tests to perform the following.

1. For the cards that were found to have lost their data, test the possibility of the cards to lose data again after proper initialization (reprogramming).

2. For the cards that do lose their data again in (1), establish a time frame within which such behavior is observed.

3. Perform statistical analysis on data retention after reprogramming the card with a valid election data.

4. Examine the behavior of the cards that lost their data after the batteries are replaced with new batteries.

5. Contrast the behavior of the test group of card with the cards that have not been previously identified as the cards that lost their data.

We present the results of the series of of three dependent tests, and contrast them with the results of a test on a control set of cards. In these tests each card is going through the following three stages: (*i*) programming, (*ii*) content extraction, and (*iii*) content validation. Content extraction and content validation stages were performed periodically after each card was programmed. This process continued for a predefined time period (at least 4 weeks). The *performance* of each card was measured in terms of how many days the card retained its data during the interval. In addition to the three stages, each test included recording of the appearance of the low-battery indication on the AV-OS display. This information on low-battery indication for each card was obtained immediately prior to extracting the card data.

Our three tests, plus the control test, are summarized as follows:

- **Test 1** includes all cards that previously lost their data. The main goal of this test is to measure the performance of these cards after reprogramming by repeatedly validating the content of the cards. This test is designed to assess the longevity and the likelihood of these cards to lose their data again after reinitialization.

- **Test 2** is performed on the cards that had the worst performance during Test 1. Specifically, it is performed on the cards that lost their data within the first two days of Test 1. We repeat the steps of Test 1 with these cards to assess whether these cards tend to lose their data in a short period of time. We compare the performance of the cards in Test 2 with the performance of the same cards in Test 1.

- **Test 3** is performed on the cards that performed poorly during Test 2. We aimed to test the hypothesis that depleted batteries caused properly programmed cards to lose their data. To test this we replaced the batteries for all of these cards with new batteries and we measured the performance of these cards. In particular, we aimed to contrast the behavior of the cards that previously lost their data with the behavior of the same cards, but with new batteries. For each such card, we recorded the battery voltage reading of the original battery.

- **Control Test** includes 50 cards that were randomly selected from the available cards from the same election that satisfied the following two conditions during the post-election audit: (1) the cards contained valid data, and (2) the cards did not contain duplication events in their logs, as card duplication has been used in some cases to restore the data on the cards that lost it. In this timed control test we reprogrammed and repeatedly validated the contents of these cards.

We now describe our testbed. We first describe the steps that comprise the initialization (programming) and the initial testing performed prior to each test.

According to the election procedures in the State of Connecticut the programmed cards are to be sealed in their target AV-OS machine at least two weeks prior to the election day. Allowing for the typical two weeks for the cards to be programmed and delivered to each voting district, this means that most of the cards are programmed approximately four weeks before the election day. Therefore, we chose four weeks (approximately) as the minimum time frame for each test.

In the tests we are concerned with card performance. We pay special attention to "worst performers", that is, cards that lose their data in a short period of time. Throughout this experiment we use a two day time period as the threshold. A card *fails* a test if it loses its data by the end of the timed test. A card *passes* a test if by the end of the timed test it still holds its data.

We used the election data from the election management system (GEMS) database files for November 2008 elections to program the cards. After programming the cards, we ran a series of "cold" (cards are installed in the tabulator that is turned off) and "hot" tests (cards are installed in the tabulator that is turned on) to check whether a card is capable of holding the data immediately after programming.

To program (initialize) a memory card we perform the following steps: (1) power-off the tabulator, (2) insert the memory card, (3) power-on the tabulator, (4) program the card, and (5) power-off the tabulator.

Immediately after programming we perform a *cold test* by *powering-on* the tabulator without removing the newly programmed card. A *hot test* follows by *removing* and *reinserting* the card in the tabulator for three times with the tabulator *powered-on*. Finally we *restart* and then *power-off* the tabulator and remove the memory card. This completes the initial testing procedure for a card.

3.2 Test Results

The high level summary of the test results is presented in Table 2. We now discuss the results of each test.

Test 1. In this test we used all 55 cards previously identified to have lost their data. Cards were initialized on 3/24/2009 (14 cards), and the rest on 3/25/2009 (41 cards). The duration of the test was 38 days. 34 cards (62% of 55) lost their data one month after programming. This means that cards that lost their data previously have a high chance of losing their data again after reprogramming. It is also worth noting that 28 cards (51% of 55) lost their data within the first week after the initialization.

Test 2. This test is designed to test the conjecture that a high percentage of cards that fail relatively quickly will fail again in a short period of time. In this test we used the worst performing 20 cards from Test 1. The duration of the test was 31 days. Our results show that 17 out of 20 cards (85%) lost their data within the first 2 days, and 18 out of 20 cards (90%) lost their data within 10 days.

Test 3. This test is conducted with the 17 cards that had the worst performance in Test 2. The duration of the test was 29 days. We took the batteries out of the cards and recorded the voltage reading of each battery.

We then installed new batteries in each card and repeated the timed test. Here we discovered that 4 out of 17 cards lost their data even after the installation of the new batteries.

The four cards (12% of the total) that failed appeared to have hardware problems or showed signs of physical damage. Two of the cards showed abnormal behavior, in particular, one card appeared to have an internal short circuit as it was draining the battery to 0V within a very short time after installation. Two other cards were in a physically damaged condition. Out of the four cards, three were physically damaged (e.g., as in Figure 1).

Recall that for physical security, identification and sealing purposes, the memory cards have tamper-evident, self-adhesive label that also covers the battery compartment. The card is built in layers, with the card circuit positioned within a frame that is in turn sandwiched between two covers. We noticed that if the paper label is damaged, absent or does not wrap around the card, then such cards may start coming apart, in particular exposing the battery compartment (one can see the battery in the lower right corner of the card, see Figure 1). Poll workers may not necessarily be aware of this damage. Cards in this condition can lose their data in the event of the battery disconnection during normal handling. It is likely that such cards may lose their data during normal handling and shipping.

Control Test. In this test we used 50 randomly selected cards satisfying the following conditions as determined in the post-election audit: (a) they contained valid data, and (b) their logs did not contain duplication events.

	Total Cards		Failed		Passed		Start	End	Duration (days)
Test 1:	55	(100%)	34	(62%)	21	(38%)	03/24/2009	05/01/2009	38
Test 2:	20	(100%)	18	(90%)	2	(10%)	04/07/2009	05/08/2009	31
Test 3:	17	(100%)	4	(24%)	13	(76%)	04/09/2009	05/08/2009	29
Control:	50	(100%)	0	(0%)	50	(100%)	05/12/2009	06/12/2009	31

Table 2: Results of the timed memory card test

Figure 1: Memory Card – enclosure is apart from frame

Cards were initialized on 5/12/2009 (20 cards), and the rest on 5/13/2009 (30 cards). As expected, not a single card lost its data in this test.

However we note that 8 cards (16% of 50) had shown a low battery indicator symbol at least once during the test. This is another cause for concern having to do with establishing the expected longevity of batteries.

3.3 Summary of the Experimental Observations

Although the tested sample of 55 cards is modest in size, the timed tests provide very strong evidence that the main factors that cause data loss in memory cards are: (a) depleted or improperly seated batteries, and (b) physical damage and wear of the cards, that might permit loss of electrical contact with the batteries.

The results of Test 1 establish that the majority of cards that experience this data loss do so within the first week after initialization (programming). The results of Test 3 suggest that changing the battery will make the card more reliable with a success rate of over 75%.

These results are contrasted with a timed test of the control group of 50 memory cards from the November 2008 elections that were properly programmed and that did not experience any problems. There were not instances of data loss in such cards.

Additionally, there is good evidence that the AV-OS function designed to warn of a low voltage battery is not a reliable predictor of the card data longevity. In the absence of warning the cards may still lose data in a short period of time. We have observed in Tests 1 and 2 that the low battery indicator symbol, in the majority of cases, was displayed only intermittently.

It remains to be determined why renewing the battery in the undamaged cards in Test 3 did not prevent loss of data. Given that we identified one card as having a hardware problem (internal short circuit), it is plausible that some other cards may also have internal damage or are in the process of degrading (e.g., as the result of electrical overstress from electrostatic discharge). While we cannot rule out secondary failure factors based on the experimental data, we do observe strong evidence that depleted batteries account for a large majority of failures. Our analysis of the memory card design (presented in the next section) provides further evidence.

4 The Causes

Section 3 presented experimental evidence that a depleted battery prevents a card from holding its programmed data. It might be helpful at this point to draw a distinction between battery service lifetime and end-of-service warning time, and also a distinction between average value, and a value that corresponds to an acceptably low failure rate.

One could easily imagine that a battery's service lifetime could be weeks or months, but its suddenness of failure being quite swift. One could easily imagine, by contrast, that a battery enters a slow decline from the onset of its use, and that slow decline remains slow, yielding a long end-of-service warning interval.

Both the service lifetime and the end-of-service warning interval are quantities characterized by probability distributions; often the average and the standard deviation are a sufficient characterization of such a quantity. An average over many samples (typical, or expected) service lifetime can be estimated using extensive sampling. A histogram of these samples can be used to estimate the probability density function. To keep a failure rate below an acceptably small amount (presumed to be significantly less than 50expected value is needed.</new>

Consistent with the presence of the battery warning subsystem, one of the vendor's manuals [31] says to replace or recharge the battery when the warning system indicates that voltage is low. While the datasheet for a similar memory card [28] states that 5.7 years is the expected (typical) lifetime for Seiko batteries when used in this card, our analysis, making use of appropriate design values, indicates it is prudent to plan for a much shorter lifetime.

From the perspective of the battery designer, it is desirable to minimize the waste of energy stored in the battery: the voltage should remain in the adequately high region until as much as possible of the energy stored is delivered. The design goal to avoid waste of energy, and therefore maintain an adequate voltage when there is energy still in the battery, results in a battery end-of-life behavior that has a "sudden" loss of voltage, in turn implying a short warning interval. Some of this voltage change behavior is represented in what is called the *depletion curve*. This curve shows how the voltage provided by the battery behaves, as the stored energy within the battery is being consumed. The battery depletion curve is provided on the battery specification sheet, for some brands of batteries. Laboratory measurements confirm the data supplied on the manufacturers' datasheets; manufacturers' data are used explain the loss of data in memory cards. The battery depletion curve can be combined with the battery monitoring technique, to calculate the warning time provided by the battery warning indicator.

Certainly it is the case that batteries run out in many kinds of devices; it is also the case that the AV-OS tabulator includes a function for providing a warning. What is significant for reducing the occurrence of data loss is the recognition that there is limited information available to provide a warning, and what information there is does not give enough advance warning for the current combination of electoral process and battery replacement policy. This section explains how much advance warning can be achieved, given the nature of the battery, by describing certain technical details of battery behavior that pertain to detection of end-of-service-life of a battery. Then we show, with a case study of one of the cards used in the AV-OS, the amount of warning time to be expected.

We define "warning time" to mean the amount of time, starting when a warning is issued and ending with the loss of card memory contents. The warning time depends upon battery design features and the *load* on the battery, which is characterized, by the manufacturers (as well as herein) by the current drawn from the battery, and also by the impedance inducing that current. Experiments can establish this current load by attaching a resistor. Informed by the battery datasheets that the battery voltage falls off quite steeply when it declines, we began by investigating the battery depletion curve (Section 4.1). We describe how we then examined the end-of-service-life detection strategy employed in the design of the particular memory card in the case study and also in the AV-OS machine software (Section 4.2). We combine the battery depletion behavior and the detection strategy, to develop our estimate of warning time. We compare the warning time with the time interval for a typical electoral process, contrasting the warning time with an election time frame.

4.1 Battery Depletion

We consider the battery voltage, as it can be expected to behave over time. As current is drawn from the battery by any circuit, the energy stored within the battery is *depleted*. The behavior of the voltage supplied by the battery, as current is drawn, is expressed in a *depletion curve*. The significance of depletion curves had long been recognized [4, 6]. Datasheets (e.g., Energizer [9] and Maxell [21]) document the specifications according to which the products can be predicted to perform, and publish the dependence of voltage output upon stored energy remaining for their batteries. We used manufacturer specified data for our calculations of warning times. We measured several batteries from each of several manufacturers, to observe how our measurements corresponded to manufacturers' data when that was available, and to assess with what confidence we might regard our measurements when manufacturer's data was not available. Maxell is one manufacturer specifying temperature dependence [21] for this battery. It reports that a reduction of battery service lifetime of about 20% can be obtained by operating the battery at $-20°$C. This is significant for shipment by air, or transportation in winter weather in some regions of the United States.

We conducted laboratory measurements and obtained the depletion curves on several batteries that were both electrically and mechanically compatible with the memory card. Our laboratory measurements on batteries from three different manufacturers are shown in Figure 2. Each depletion curve is expressed as voltage vs. time; while measurements were collected at several values of load between 6.71 kOhms and 33 kOhms, on the plots the loads have been normalized to allow comparison among Manufacturers A, B, and C. In particular, the load was normalized to 10 μA, and 25 weeks was chosen for the time (horizontal) axis. Explanation of why this value of the load, and this value of the time were chosen are found in Sections 4.2 and 4.3 respectively. Table 3 presents the comparison between the depletion time of the batteries, normalizing the load to 300 kOhms.

The measurements range from 0.6 to 1.5 of the predicted lifetime of this type battery given by one battery manufacturer [21]. (Also, the predicted lifetime differs by about a week from the shelf life of a line of memory cards manufactured by the same memory card manufacturer, Smart Modular Technologies.) We are also pursuing the measurements of the battery depletion curve using memory cards, to be reported in the future.

As seen in the plots of Figure 2 the watch battery depletion curve has a flat region followed by a *steeply dropping region*. As the reserve of stored energy in the battery is reduced, the voltage also tends to decline. We reiterate that there are good reasons (e.g., avoiding waste of energy) for designing batteries to maintain output voltage within a narrow region while the energy is being depleted. In particular, batteries have a design feature that holds the remaining voltage above a designed level until most of the stored energy has been used. This design feature has the purpose of delivering the energy stored in the battery in a manner efficient for its intended application. In other words, electronic circuits waste less energy if no excess voltage is delivered, and they can be expected to fail to function if insufficient voltage is applied. Thus, the minimum waste of energy is obtained when batteries deliver a constant voltage over their service life.

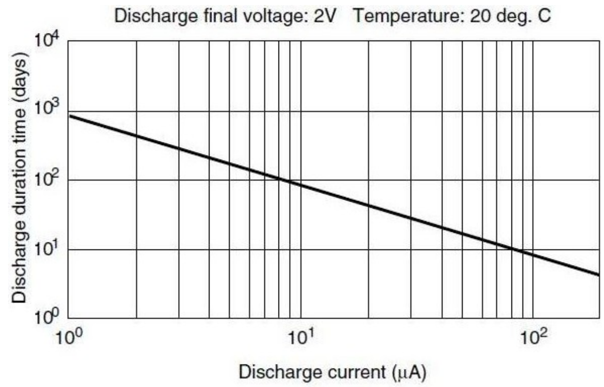


Figure 3: Significance of load upon battery for service lifetime

Using the Maxell datasheet [21] that provides information (shown in Figure 3) about depletion time as a function of load to support our extrapolation, we compute the anticipated depletion curve for the battery when the memory card is the electrical load. It can be seen on this plot that a current demand of 10 μA, obtained from a memory chip datasheet, corresponds to a service lifetime of approximately 90 days (12.9 weeks).

4.2 Detecting End-of-Service Life of the Battery

To warn of depletion of the battery and subsequent loss of data, the AV-OS provides a functionality that notifies the terminal operator that the voltage of the battery has dropped to a "low" value. On the memory card type we examined, a hardware chip, the Dallas Semiconductor DS1312, is used to compare the battery voltage under load with a voltage level set at the factory when the chip was manufactured. This chip produces a signal, based upon its examination of the battery voltage, and that signal, nominally at 5V for no battery warning, and below 2V when a battery warning is being issued, is routed from the memory card to the AV-OS processor. The software in the AV-OS compares this battery warning signal with 5V. The software uses the result of this comparison to inform the operator.

Figure 4 illustrates the finite state machine (FSM) of the operation of the DS1312 chip, using information obtained from the DS1312 datasheet [5]. It also presents a legend of the possible values, as a result of the variability in the manufacturing process, that the various thresholds may take. The chip has three responsibilities of which we describe two (the third function is write protection of the memory). The two relevant responsibilities are (as

Manufacturer A Manufacturer B Manufacturer C

Figure 2: Depletion curve measurements upon batteries from three different manufacturers (scaled to 10 μA).

Battery	Load	Time Interval above 2V
Manufacturer A	adjusted to 300 kOhms	8.6 weeks
Manufacturer B	adjusted to 300 kOhms	7.8 weeks
Manufacturer C	300 kOhms	18.9 weeks

Table 3: Comparison of the depletion interval with the load adjusted to 300 kOhms.

used by the memory card): (*i*) keep continuous power supply to the memory chip, and (*ii*) send a signal when low-voltage is detected in the battery. The chip has two voltage inputs: an input connected to the main power of the AV-OS (VCCI), and an input connected to the battery of the memory card (VBAT).

The FSM starts from the "No Power" state. Once we add a new battery in the card we move to a freshness seal mode where it does not supply the memory with power until the VCCI exceeds the predefined threshold (VCCTP). This threshold is the least amount of voltage that the chip expects from the main power input. When the AV-OS is turned on this threshold is reached and we move to the "Operating on Main Power" state. Here, the chip supplies the RAM chip with the power received from VCCI. Also, as soon as we get to this state we test the battery voltage ("Test VBAT" state). A second threshold is used here (denoted by VBTP), which defines the acceptable voltage we should receive from the battery. If VBAT is less than VBTP, the battery warning (BW-) signal changes from nominally 5V (floated) to 0V (pulled low). If VBAT is greater than VBTP then the BW- signal remains high. In this case the chip resets an internal clock and rechecks the battery voltage every 24 hours. The FSM moves to the "Operating in Battery" state if the VCCI drops below the supply switch threshold (VSW) and VBAT (and thus AV-OS is turned off). In this state the DS1312 supplies the RAM chip using the VBAT voltage. If the VCCI becomes greater than VSW, then from this state we move back to the "Operating the Main Power" state. Notice that the battery voltage is checked in this case as well.

We can conclude that the battery is checked in two cases: (*i*) startup (when the machine is turned on with the memory card already in it, or when the memory card is inserted while the machine is already on), or (*ii*) periodically while the machine is left on and 24 hours have passed from the last check. The threshold VBTP cannot be set higher than the voltage of a new battery, otherwise new batteries will immediately be declared to be at end of life. Therefore, the highest meaningful value of VBTP is the nominal voltage of the fresh battery, 3 volts. The lowest possible value of that threshold is the value needed by the memory circuits to retain data. Between these maximum (fresh battery voltage) and minimum (smallest according to RAM specification) voltages is the region within which a voltage threshold has a chance of being useful. In this region, higher values of threshold correspond to earlier warnings.

We traced the BW- signal on the memory card by examining the printed circuit board. We found that on this circuit card, the battery warning output signal from the DS1312 is routed to pin 2 on the card. This pin's signal is then provided to the comparator input port of the processor. The software of the AV-OS in turn, monitors the signal on the port. Because this signal is nominally a digital signal raised to approximately 5V when the DS1312

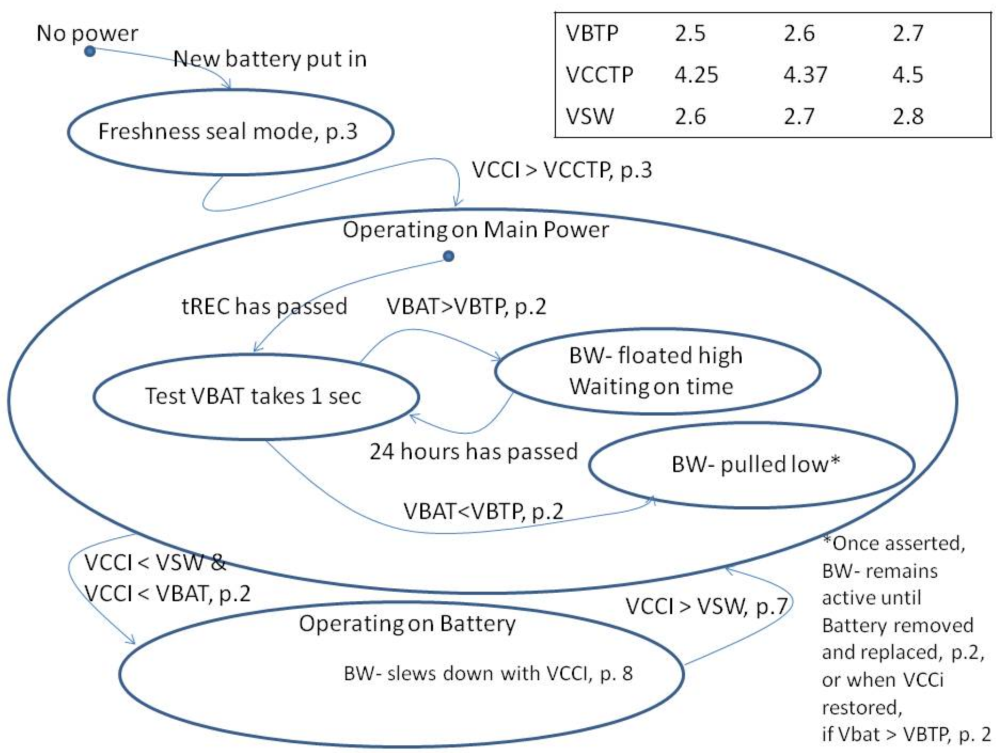


Figure 4: Operation of DS1312.

has not detected a battery warning condition, the processor software uses a threshold to evaluate the BW- signal. This threshold is set at 5V which is consistent with the desire to provide a warning as soon as possible after the DS1312 has detected a warning condition.

Thus, we conjecture that the detection strategy, when this version of memory card is used, is a combination of a hardware detection by the DS1312 circuit followed by a software detection of the "BatteryWarning" active low signal output from the DS1312 on the comparator input port. Though we have an idea of the method used in AV-OS, it is perhaps more useful to consider the limits for any implementation, rather than specifically addressing one instance of implementation. For example, were a gate array to be used for the battery warning function, as mentioned in [27], the limitations on detection approaches are still completely relevant.

Choice for Load Current. To estimate the service lifetime of the battery of the memory card, we need an estimate of the load that the card places upon the battery.

By examination of the memory card, we identified that the card is equipped with a Hynix HY628100B RAM chip. From the RAM's datasheet [15], we obtained the standby current level at which the RAM is guaranteed to retain data. According to the datasheet the particular RAM chip requires no more than 10 μA of standby current load. This is the value of current we use as the load upon the battery.

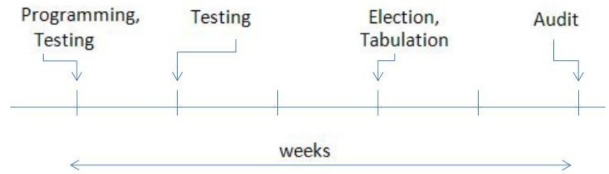
Battery Lifetime. The voltage of the battery is used to detect the beginning of its end-of-life. The voltage threshold (VBTP) should be lower than the nominal operating voltage, or the false alarm rate (the frequency with which good batteries are declared to be at end-of-life) will be unreasonably high. Let us postulate then, that the threshold level is 2.8V. We know from above that the the HY628100B series RAM requires no more than 10 μA of standby current load. Given this information we observe from the Energizer datasheet [9] that for a threshold voltage of 2.8V and a minimum acceptable voltage of 2.0V, we expect to obtain 2000 hours of warning (12 weeks). If the threshold voltage were 2.5V, and the minimum acceptable voltage were 2.0V, we expect to obtain a warning time of 800 hours (4.8 weeks). From the Maxell datasheet, we find that for a threshold of 2.8V, and a minimum acceptable voltage of 2.0V, we expect to obtain a warning time of 2,600 hours (15.5 weeks), and for a threshold voltage of 2.5V with a minimum acceptable voltage of 2.0V, we expect to obtain a warning time of 800 hours (4.8 weeks).

In the case of the Dallas Semiconductor DS1312 [5] the VBTP threshold was 2.5V (the minimum possible threshold). In this case the warning time would be, considering the above batteries, less than *five weeks*. If the battery voltage were supplied to the RAM through the DS1312 battery monitor circuit, it would experience a voltage drop between its measurement point and its point of application to the RAM. This drop is specified to be no worse than 0.2V. In this case, 2.2V is the least voltage necessary for the DS1312 to deliver 2V to the RAM. Hence, in this case the warning time equals to the amount of time to move from 2.5V to 2.2V and that is 900 and 600 hours, respectively, or less than *5.3 or 3.6 weeks*. Other battery brands may differ.

The steepness of the battery depletion curve, which is an intended design feature of the battery (see Section 4.1), causes the strong influence of these factors (current drawn, voltage threshold) upon the warning time. Figure 5 depicts the depletion curve of the battery and shows the warning time in weeks from 2.5V (point A) and 2.4V (point B) to 2.2V (point C) and 2V. The plot is scaled to correspond to 10 μA of load. The shape of the curve differs between manufacturers, so the warning time depends upon the brand of the battery; nevertheless, the warning time is too short for all of the batteries we have investigated.

4.3 Battery Lifecycle in an Election

So as to suggest the least possible criticism of the design, while addressing the cause of the memory card data loss, we chose to assume the following: (a) No current is drawn from the battery during the presence of a voltage supply from the AV-OS. (b) No transient spike of drawn current occurs at any point in the lifecycle. (c) The memory is in a standby, lower current consumption mode of operation, when the *battery backup* is being used. (c) Because battery lifetime is specified at room temperature, the effect of cooling, as would expected if air shipment were used, has not been taken into account. In effect, we have assumed that the battery is maintained within the range for which it is specified to operate, even though that is unlikely to be the case, because the internal temperature inside the equipment while operating is very likely to be higher than room temperature and the temperatures experienced during shipping during winter



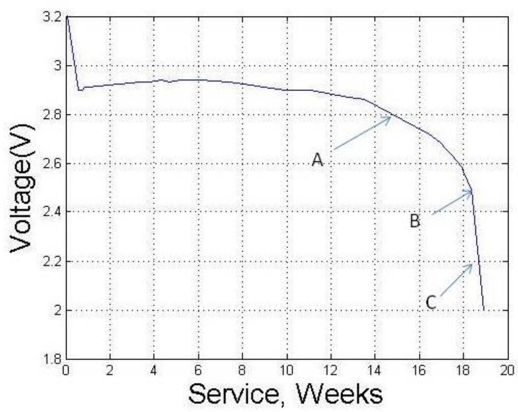
The lifecycle of a memory card used in an election includes preparation, delivery, use in the tabulation of cast ballots, use in aggregation. Eventually the interest in the data as represented in the card memory is over. If the lifecycle lasts six weeks, the warning time ought to be at least six weeks.

Figure 6: The lifecycle of a memory card in an election

might be colder than room temperature.

The recommended lifecycle begins with a fresh battery being installed in the memory card. As shown in Figure 6, the battery experiences a sequence of events related to an election. After a fresh battery is installed in a memory card using the DS1312 (Figure 4), the battery is protected from its load until after the first time the main power from the tabulator is applied. Whenever the memory card is inserted into the tabulator, there are two possibilities, either the tabulator is already on, or the tabulator is turned on. We start our estimate of lifetime with the later of these two events, because that is the event when the electrical power of the tabulator is applied to the memory card.

Adequate Warning Estimation. Now let us consider whether an adequate amount of warning can be obtained. As described earlier, the battery voltage is used to indicate the remaining service life of the battery. Using the battery voltage as the signal of remaining service life suggests measuring the prevailing battery voltage, and also establishing a voltage level against which the prevailing battery voltage is compared. When the result of this comparison is that the prevailing voltage has declined below the threshold voltage, then an action, such as the issuance of a message to an operator, can be initiated. Higher threshold values have the potential to warn earlier, possibly wasting more stored energy. Lower threshold values have the potential that the battery energy runs out before the battery is replaced. Thus the threshold value is set in an attempt to give adequate warning. It is worth considering whether it is possible to obtain adequate warning. One part of this consideration is, how much warning is adequate.



(A) Depending upon the brand of the battery, the output voltage of the battery can cross below 2.8V almost immediately in the life of the battery [21] or not until 12 days prior to end of life [9].
(B) With a threshold setting of 2.5V, a warning time of 7 week with one brand of battery is obtained, and with another brand, 5 weeks.
(C) 2V is the voltage specification for a possible SRAM chip, 2.2V specified so that a DS1312 chip would (by specification sheet) deliver 2V to the RAM. Using 2.2V shortens the warning time for a threshold of 2.5V from 7 weeks to 5 weeks, and from 5 weeks to less than 4 weeks.

Figure 5: Estimating warning time

The lifecycle of an election is part of the consideration of what an adequate warning time would be. A typical electoral process follows the stages presented in [2]. In brief, the electoral process consists of five main stages: programming, testing, election, tabulation and auditing. Shipment occurs several times; this should not be neglected because it offers opportunities for weather and adversaries to interfere with the mission of the memory card.

A memory card is first prepared to support the election. Once the card is programmed it remains idle until it is tested in the precincts. The programming of the card is expected to be performed at least three weeks before the election. Subsequently, testing and election stages are assumed to be performed at almost the same time. After the election is completed the card remains idle until the central tabulation of the results is completed (where this is the norm—central tabulation is not performed in Connecticut); tabulation is usually completed the same day as the election (but in Connecticut the cards reside at the precincts for at least two weeks after that). Then the card is used for auditing and the data should be retained for at least one more week; see Figure 6. This stage completes the cycle of the election process and determines the expected time—six weeks—during which the card is going to be idle and the battery energy is subject to depletion as illustrated in Figure 5.

Let us now assume that when the card is programmed for election, the status of battery warning is checked and is seen to pass inspection. Recall that the battery voltage declines at end-of-service life, but the decline is quite steep. As shown in Figure 5, at 2 weeks prior to the end-of-service life, the estimate of the measured voltage is 2.6V. Thus a warning threshold would have to be higher than 2.6V. Examining the graph, the warning voltage threshold of 2.8V or higher appears, for this brand of battery, to provide as much as four weeks of warning. This threshold level is close to the normal voltage range of the battery, suggesting that the rate of false alarms, i.e., warnings issued when not warranted, might be high.

Let us call detection of end-of-service life "detection". Let us call declaration of end of service life, when that declaration is premature, "false alarm". By setting the voltage threshold higher, we increase both the probability of detection and the probability of false alarm. If we set the threshold value to reduce false alarms, we also reduce the probability of detection. This sort of system behavior is often shown in receiver operating characteristic (ROC) curves. Some choice, informed by the relative values of a missed detection and a false alarm, is made about what point on the ROC will be chosen. We ascribe a significant value to a missed detection, especially for a DRE, but we need to avoid constant false alarms. Using the threshold implemented in the memory card we analyzed, and good quality batteries, we determined that that threshold provides twelve days of warning.

Estimating service life. We close this section with a brief description of how to estimate the service life of a battery that could be used to guide the decision of when batteries need to be replaced. A procedure for estimating the service life of a battery is as follows.

1. Estimate how much current load one should plan on being presented to the battery. For example, if the battery supplies a single RAM, and that RAM in standby mode is specified to require no more than 10 μA, then one would use 10 μA.

2. Choose a battery whose datasheet supplies a depletion curve.

3. Estimate the values of some relevant parameters, e.g., if the datasheet gives various depletion curves depending upon operating temperature, and the temperature makes a significant difference to the depletion curve, then it is advisable to estimate the operating temperature, and select the depletion curve for that temperature, or perhaps interpolate between curves for higher and lower temperatures to estimate the corresponding depletion curve.

4. Obtain the value of voltage needed from the battery, so that the circuit supplied by the battery can function. For example, if the RAM requires at least 2.0V, and an intervening circuit produces, worst case, a voltage drop of 0.2V, add these to obtain the 2.2V required of the battery.

5. Using the current load from item 1 and the curve obtained in item 3, read the amount of time it takes for the battery's output voltage to decline to the voltage value obtained in item 4.

5 Recommendations

Our main conclusion for the AV-OS system is that it is not advisable to rely on the (absence of) low-voltage warning as an indication that the memory card will retain its data for the entire duration of the electoral process. If the state of the battery is unknown, the absence of low-voltage warning at best means that the battery will last for for at least two weeks, which may be sufficient.

In general, *when using battery-backed RAM, ensuring fresh batteries in the process of preparing for the election is recommended.* The batteries can be purchased in quantity for about $0.50, so the cost of replacement can be expected to be dominated by labor costs; those are unknown to us. If labor costs were low enough, and memory cards and batteries uniquely identified, batteries could be removed in between elections. Records could be kept of time-in-use of individual batteries. In the more likely event that labor costs dominate and without a means to assign a cost to environmental impact, for the case where battery-backed RAM cards continue to be used, the recommendation is to provide fresh batteries. Given the technology used to implement the cards and the characteristics of the batteries, setting the warning threshold at a higher voltage (even if this were practically implementable) would result in frequent premature warnings of battery depletion, necessitating battery replacements even if the batteries have adequate energy left. This will not avoid replacing most (or all) batteries at the point where the preparation for election is started.

The memory card can be expected to draw battery current from the first time the card is powered by other than the battery, i.e., by the tabulator. Subsequently the card is going to draw current for any interval when the card is not supplied power from another source. Therefore it is important to choose batteries whose depletion curve remains above 2.5V for the required interval of time. For example, if a card is to retain its data for up to 1/2 year, then a battery needs to be chosen so that it maintains 2.5V or more for at least 26 weeks, when a load of 10 μA (corresponding to the datasheet specification of current load for a low power CMOS RAM) is applied.

If we assume standby mode for the memory, and use memory that requires no more than 10 μA of standby current load (with no other components drawing current), and use the Energizer CR2016 battery (a better battery), we estimate that the life of the battery should be approximately one year. This number is obtained as follows. The battery voltage is nominally 3V, and we assume the Hynix RAM whose datasheet [15] specifies 10 μA current drawn in standby mode. The lifetime of the Energizer battery, when its voltage remains above the 2V needed for data retention in standby mode, at that current load, according to its datasheet [9] is 9,000 hours or approximately one year.

Given that it is possible that a memory card is used for elections once a year, it leads us to the same conclusion: For each election, a decision would be made, whether or not to replace the batteries for this election. The decision would be based on the amount of time since the batteries were last replaced and on the estimate of the service life of the battery (e.g., using the procedure at the end of the previous section).

6 Conclusions

This paper presents experimental and analytical evidence that the primary cause of the loss of data frequently observed with the AccuVote Optical Scan (AV-OS) memory cards is due to battery depletion. Memory cards are prone to losing their data even if the AccuVote low-battery warning is absent at the time the cards are programmed.

Supplementing the experimental data, our analysis explains why memory cards lose data, and why they do so unexpectedly. In our assessment, a memory card can be relied upon to hold its data for no more than 2 weeks after programming when the AV-OS does not issue a low-battery warning.

Because the warning time is short, we suggest that election officials and memory card programmers do not rely on these warnings. Instead, they should take mitigating measures, for example, consider replacing batteries before cards are prepared for elections. Concurrently, the feasibility of using non-volatile removable media ought to be explored.

The factors contributing to the short warning time are the steepness of the battery depletion curve (a function of how fast energy is drawn from the battery), and the particular rate with which energy is drawn from the battery. Because these two factors can be expected to be similar in other electronic voting systems using battery backed RAMs, it appears likely that other such electronic voting would experience failures of the kind seen in the AV-OS. It appears likely that, in all such battery-backed RAM systems, it is not practical to provide earlier warnings because there are bound to be many false warnings with perfectly healthy batteries.

It would be extremely important to obtain experimental support for our conjecture by analyzing other electronic voting systems that use battery backed RAMs, however this would require the level of access to such systems that, as of this writing and upon our belief, is only available in Connecticut (where only AV-OS is used). Our study should motivate further research for other election systems that rely on battery powered cards for data retention, e.g., OS ES&S Model 100 and DRE AVC Advantage.

We also recommend that audit procedures—hand-counted audits in randomly selected precincts, and pre- and post-election audits of memory cards—be put in place in any jurisdictions that encounter memory card failures. If a memory card fails prior to a technical audit, it is also recommended that the precinct where the card was used is automatically selected for hand-counted ballot audit (for systems that have voter-verified ballots).

In addition to renewing batteries, based on our observations election officials should inspect the cards for physical wear and damage. The visual inspection needs to focus on loose or damaged enclosures, and such cards must be replaced or repaired.

Lastly, while recommending proactive battery replacement programs, additional work is necessary to develop feasible logistics and estimate the costs of such programs.

Because the warning time is short, we suggest that election officials and memory card programmers do not rely on these warnings. Instead, they should take mitigating measures, for example, consider replacing batteries before cards are prepared for elections. Concurrently, the feasibility of using non-volatile removable media ought to be explored.

Addressing the broader landscape, it is extremely important to assess both the security and reliability aspects of electronic voting systems. Beyond the obvious need for these systems to be reliable and dependable, defects and benign failures in such systems and their components could be used by nefarious actors to mask tampering. For example, attackers can hope to cover their tracks by using the knowledge that volatile memory cards with weak batteries are likely to lose their data within days, thus potentially thwarting subsequent forensic investigation. Understanding the reliability limitations of existing voting systems further motivates the development of better new systems and helps improve safe use procedures for existing systems.

Acknowledgment

We thank the anonymous reviewers for their insightful and detailed comments that helped us to significantly improve the presentation.

References

[1] Antonyan, T., Davtyan, S., Kentros, S., Kiayias, A., Michel, L., Nicolaou, N., Russell, A., and Shvartsman, A. Automating voting terminal event log analysis. In *Electronic Voting Technology Workshop/ Workshop on Trustworthy Elections (EVT/WOTE09)* (2009).

[2] Antonyan, T., Davtyan, S., Kentros, S., Kiayias, A., Michel, L., Nicolaou, N., Russell, A., and Shvartsman, A. A. State-wide elections, optical scan voting systems, and the pursuit of integrity. *Trans. Info. For. Sec. 4*, 4 (2009), 597–610.

[3] Bannet, J., Price, D. W., Rudys, A., Singer, J., and Wallach, D. S. Hack-a-vote: Security issues with electronic voting systems. *IEEE Security & Privacy 2*, 1 (2004), 32–37.

[4] Chardack, W. M., Gage, A. A., Federico, A. J., Schimert, G., and Greatbatch, W. Clinical experience with an implantable pacemaker. *Ann N Y Acad Sci. 111* (Jun 1964), 1075–1092.

[5] DallasSemiconductor. Ds1312 nonvolatile controller with lithium battery monitor.

[6] Davies, G., and Siddons, H. Prediction of battery depletion in implanted pacemakers. *Thorax 28*, 2 (March 1973).

[7] Davtyan, S., Kentros, S., Kiayias, A., Michel, L., Nicolaou, N. C., Russell, A., See, A., Shashidhar, N., and Shvartsman, A. A. Pre-election testing and post-election audit of optical scan voting terminal memory cards. In *Proceedings of the 2008 USENIX/ACCURATE Electronic Voting Workshop (EVT 08), July 28-29, 2008, San Jose, CA, USA* (2008).

[8] Davtyan, S., Kentros, S., Kiayias, A., Michel, L., Nicolaou, N. C., Russell, A., See, A., Shashidhar, N., and Shvartsman, A. A. Taking total control of voting systems: Firmware manipulations on an optical scan voting terminal. In *Proceedings of the 24th Annual ACM Symposium on Applied Computing (SAC 09)* (2009).

[9] ENERGIZER HOLDINGS, I. Energizer cr2016 lithium coin.

[10] FELDMAN, A. J., HALDERMAN, J. A., AND FELTEN, E. W. Security analysis of the Diebold AccuVote-TS voting machine. http://www.usenix.org/event/evt07/tech/full_papers/feldman/feldman.pdf, 13 September 2006.

[11] HAUSER, R. G., WIMER, E. A., TIMMIS, G. C., GORDON, S., ET AL. Twelve years of clinical experience with lithium pulse generators. *PACE. 9* (1986).

[12] HAYES, D. L., AND VLIETSTRA, R. E. Pacemaker malfunction. *Ann Intern Med. 119* (1993).

[13] HURSTI, H. Critical security issues with Diebold optical scan design. http://www.blackboxvoting.org/BBVreport.pdf, 4 July 2005.

[14] HURSTI, H. Diebold TSx evaluation. Black Box Voting Project, http://www.blackboxvoting.org/BBVtsxstudy.pdf, 11 May 2006.

[15] HYNIX. Hy628100b series, 4 2001.

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

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

[18] KLOEPPEL, T. Automated Election Services - Optech III Information. http://www.boisforte.com/documents/AESINFO.doc, 3 2010.

[19] KOHNO, T., STUBBLEFIELD, A., RUBIN, A. D., AND WALLACH, D. S. Analysis of an electronic voting system. In *Proceedings of the IEEE Symposium on Security and Privacy* (2004), pp. 27–42.

[20] LEE, Y. S. Battery depletion monitor, 2009. United States Patent 4313079, http://www.freepatentsonline.com/4313079.html, viewed 1 July 2009.

[21] MAXELL/HITACHI. Lithium manganese dioxide rechargeable batteries ml2016, June 2003.

[22] MEDTRONIC. At500 pacing system follow-up protocol, 2009. http://www.medtronic.com/crm/performance/articles/at500_battery.html, viewed 1 July 2009.

[23] MORGAN, M. Election night in washtenaw county, November 2009. The Ann Arbor Chronicle.

[24] NORDEN, L. The machinery of democracy: Protecting elections in an electronic world, 2005. Brennan Center Task Force on Voting System Security, http://www.brennancenter.org/page/-/d/download_file_36343.pdf.

[25] ROOS, M., KOBZA, R., AND ERNE, P. Early pacemaker battery depletion caused by a current leak in the output circuitry: Rectification not exchange. *Pacing and Clinical Electrophysiology 30*, 5 (2007). ON: 1540-8159 PN: 0147-8389 AD: Division of Cardiology, Kantonsspital Luzern, Luzern, Switzerland.

[26] SBE. M100 Battery Primer. Document Control #: VS-02-14, Copyright 2006 by Election Systems & Software, 11208 John Galt Blvd., Omaha, NE 68137-2364, all rights reserved. Printed in the USA, 2 2010. North Carolina State Board of Elections.

[27] SEIKOEPSON. SRAM IE Series.

[28] SHVARTSMAN, A., KIAYIAS, A., MICHEL, L., RUSSELL, A., ANTONYAN, T., DAVTYAN, S., KENTROS, S., AND NICOLAOU, N. Post-election audit of memory cards for the november 2008 elections, version 1.0. *UConn VoTeR Center* (May 2009).

[29] SHVARTSMAN, A., KIAYIAS, A., MICHEL, L., RUSSELL, A., ANTONYAN, T., DAVTYAN, S., KENTROS, S., AND NICOLAOU, N. Statistical analysis of the post election audit data 2008 november elections. *VoTeR* (May 2009).

[30] Verified Voting. http:/www.verifiedvoting.org.

[31] VERIFIEDVOTING. Electronic Voting Machine Information Sheet - Sequoia Voting Systems - AVC Advantage. http://www.verifiedvoting.org/downloads/2008SequoiaAVCAdvantage-full.pdf, 2008.

[32] VORA, P. L., ADIDA, B., BUCHOLZ, R., CHAUM, D., DILL, D. L., JEFFERSON, D., JONES, D. W., LATTIN, W., RUBIN, A. D., SHAMOS, M. I., AND YUNG, M. Evaluation of voting systems. *Commun. ACM 47*, 11 (2004), 144.

[33] WAGNER, D., JEFFERSON, D., AND BISHOP, M. Security analysis of the Diebold AccuBasic interpreter. Voting Systems Technology Assessment Advisory Board, University of California, Berkeley, 14 February 2006.

[34] WERTHEIMER, M. A. Trusted agent report Diebold AccuVote-TS voting system. RABA Innovative Solution Cell, http://people.csail.mit.edu/rivest/voting/reports/2004-01-20%20RABA%20evaluation%20of%20Diebold%20AccuVote.pdf, January 2004.