# The New Jersey Voting-machine Lawsuit and the AVC Advantage DRE Voting Machine

Andrew W. Appel* Princeton University
Maia Ginsburg Princeton University
Harri Hursti
Brian W. Kernighan Princeton University
Christina D. Richards Princeton University
Gang Tan Lehigh University
Penny Venetis Rutgers School of Law – Newark

**Abstract**

As a result of a public-interest lawsuit, by Court order we were able to study, for one month, the hardware and source code of the Sequoia AVC Advantage direct-recording electronic voting machine, which is used throughout New Jersey (and Louisiana), and the Court has permitted us to publicly describe almost everything that we were able to learn. In short, these machines are vulnerable to a wide variety of attacks on the voting process. It would not be in the slightest difficult for a moderately determined group or individual to mount a vote-stealing attack that would be successful and undetectable.

## 1 Litigation and legislation in New Jersey

In October 2004 a group of public-interest plaintiffs, represented by Professor Penny Venetis of the Rutgers Law School, sued the State of New Jersey (in NJ Superior Court) over the State's use of direct-recording electronic (DRE) voting machines in New Jersey. By 2004, most of New Jersey's counties had adopted the Sequoia AVC Advantage full-face DRE. Currently 18 out of New Jersey's 21 counties use this DRE.

The plaintiffs argued that the use of DRE voting machines is illegal and unconstitutional: illegal, because they violate New Jersey election laws requiring that all votes be counted accurately and that voting machines be thoroughly tested, accurate, and reliable; and unconstitutional, because they violate the New Jersey constitution's requirement that all votes count.[1] The plaintiffs argued that one cannot trust a paperless DRE machine to count the vote. The defendant, the State of New Jersey, has taken the position that enhanced physical security measures will prevent access to AVC Advantage ROM chips, and thus prevent rigging of the voting machines.

From 2005 to 2007, the trial focused on issues related to the adoption and implementation of voter-verified paper ballots. When voter-verified paper ballots not in place by January 2008, Judge Linda Feinberg ordered a trial to determine whether it is constitutional to use paperless DREs. The case is Gusciora *et al. v.* Corzine *et al.*, Docket No. MER-L-2691-04, Superior Court of New Jersey.

In the "Super Tuesday" Presidential Primary of February 5, 2008, at least 37 voting machines in at least 8 different counties exhibited an anomaly in their results reports: the number of Republican primary votes was larger than the number of Republican primary voters (or on some machines, Democratic/Democratic), as reported on the results-report printouts by the AVC Advantage at the close of the polls. This could only be explained by a software bug.

Until this point the State had maintained that these voting machines are 100% accurate. Based on the inaccuracies demonstrated on Super Tuesday, Plaintiffs were finally able to gain access to the source code by a court order. In March 2008 the plaintiffs issued a subpoena, which was then enforced by the Court, ordering that the State provide to plaintiffs' expert witnesses for examination: AVC Advantage voting machines complete with their source code, build tools, operator manuals, maintenance manuals, and other documents. The Court initially proposed that the expert, Andrew Appel of Princeton University, should make a brief visit to the warehouse to inspect the machines. Plaintiffs explained that the examination would require a team of computer scientists, in a laboratory with equipment and

*This research was supported in part by National Science Foundation award CNS-0627650. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

[1] Article II, Section 1, paragraph 3 of the New Jersey Constitution. New Jersey Statutes Annotated 19:48-1, 19:53A-3, 19:61-9.

computers, for a period of months. At this point Sequoia Voting Systems vigorously protested against any examination of their source code. Sequoia also made a motion to be admitted as a party, not as a defendant but for the limited purpose of defending its intellectual property through the scientists' examination phase. The Court admitted Sequoia as a party for this limited purpose. It took months of litigation, until June 20, 2008, to negotiate a Protective Order (a court-ordered nondisclosure agreement) that equally dissatisfied all the parties.

The Protective Order permitted the examination by a team of up to 9 computer scientists, for a 30-day period, at a room in the State Police Headquarters. In the end, the team comprised 6: Andrew Appel, Maia Ginsburg, Harri Hursti, Brian Kernighan, Chris Richards, and Gang Tan, all working *pro bono.* The team was permitted to install a local network of computers, disconnected from the Internet. To permit the installation of software tools on the examination computers, a one-way transfer of information to, not from, these computers was permitted via USB thumb drives.

We examined voting machines and source code during July and August 2008, and delivered our report with video to the Court on September 2. The Protective Order permitted us to publish our report in October, which we did [3] (with some redactions pending a hearing by the Court on whether certain sections do or do not reveal trade secrets). The trial ran between January 27, 2009 and May 11, 2009. The Court is expected to issue a decision in late 2009.

The plaintiffs' key witness was Professor Andrew Appel, who testified extensively about the ways in which the Sequoia Advantage 9.00H DRE is vulnerable. Those insecurities are discussed in this paper. Our study of the AVC Advantage is legally significant because it is the first court-ordered study of voting-machine hardware and source code by plaintiffs' experts. It established a legal precedent for other similar cases ongoing in other states (e.g., Pennsylvania).

We will summarize our findings and describe the architecture of the system, its vulnerabilities, the failures of authorities, and our conclusions. Our full report [3] covers these in more detail and covers additional issues; accompanying it is a video demonstration [2] of some of the inaccuracies and vulnerabilities that we observed. After our original report the State introduced new supposedly tamper-evident seals. In Section 12 we present our security analysis of these seals.

# 2 A summary of our findings

Basic classes of insecurities and inaccuracies in voting machines are well established in the scientific literature, and we were guided by these in our study, as this table shows. For each general class of inaccuracy/insecurity that we found in the AVC Advantage, we present its consequences, related prior studies on other voting machines, and the section of this paper that describes detailed findings.

| FLAW OR VULNERABILITY | CONSEQUENCES | PRIOR STUDIES | § |
|---|---|---|---|
| User interface flaws | Lost votes; Duplicate votes | Herrnson [12] | 4 |
| Firmware replacement, viral propagation, and WinEDS | Vote stealing; election manipulation | Hursti [13]; Feldman [9]; Blaze [6]; McDaniel [18]; Balzarotti [5] | 6 |
| Tampering with cartridges | Vote stealing; 2 votes for 1 button | Blaze [6][18] | 7 |
| Naive crypto. authentication | cartridge tampering | Kohno [17] | 8 |
| Program bugs | Wrong primary ballot<br>Buffer overrun DOS | various | 5<br>6 |
| Hardware faults | Lost votes; exposure of trust placed in cartridges vis-a-vis paper | | 10 |

- A string of prior studies (e.g., [17, 13, 9, 6, 5, 18]) showed that voting machines are insecure. These studies were informative to bootstrap our process and also gave us a menu of patterns to look for when we examined the AVC Advantage. Although the AVC Advantage has not been examined by prior studies and its architecture is quite different from other machines, we have confirmed through both experiments and source code review that, like all other voting machines studied, it is vulnerable to firmware replacement and tampering with storage media that hold ballot definitions or voting results.
- We found *user interface design flaws* of the AVC Advantage, different from those on touch-screen DREs, which have the potential to cause inaccuracy in recording votes.
- In 2008, an AVC Advantage experienced a hardware fault that caused its results cartridge to disagree with its close-of-polls paper printout. Even though (as we determined) the paper printout is more accurate in such a

case, county election officials used the electronic totals in the cartridge for this machine, and ignored the paper printout.

- We also carefully studied the source code, and the AVC Advantage's Independent Test Authority (ITA) report. We found that the source code does not follow best software engineering practices, and the ITA report does not accurately and sufficiently assess the security of the AVC Advantage. We found at least two program bugs that had slipped through the ITA review.

To summarize our conclusions, the AVC Advantage is vulnerable to election fraud via firmware replacement and other means. Even in the absence of fraud, the AVC Advantage has user interface flaws that could cause votes not to be counted.

# 3 Architecture of the AVC Advantage

The Sequoia AVC Advantage is a "direct-recording electronic" (DRE) voting computer. That is, the voter indicates a selection of candidates via a user-interface to a computer; the program in the computer stores data in its memory that (are supposed to) correspond to the indicated votes; and at the close of the polls, the computer outputs (what are supposed to be) the number of votes for each candidate.

Ballots are prepared and results are tallied with a Windows application called "WinEDS" that runs on computers at election headquarters in each county. Ballot definitions (contests, candidate names, party affiliations, etc.) are transmitted to the Advantage via a "results cartridge," which is inserted at the election warehouse before the machines are transported (by private trucking contractors) to polling places a few days before the election. The votes cast on an individual machine are recorded in the same cartridge, which pollworkers bring to election headquarters after polls close. The voting machines are left at the polling places for a few days until the trucking company picks them up.

We were given access to a Windows computer running WinEDS that was capable of reading and writing cartridges, but we did not have the source code of the WinEDS application, which appears to have been written by another company and sold or licensed to Sequoia.

Appel had previously purchased five surplus AVC Advantage 5.00E machines from a county in North Carolina. Halderman and Feldman reverse-engineered the hardware and parts of the software of these machines in 2007 [11].

*Four unattended AVC Advantage voting machines in a polling place accessible to the public, the weekend before an election [10].*

*Unfolded for an election*

**Hardware.** Physically, the AVC Advantage is a big 200-pound purple box on wheels. The computer and associated electronics are mostly on a single motherboard inside a metal box inside a locked enclosure. The technology largely dates from the early 1980's. The motherboard has a Z80 processor, with a 64 KB address space. There is no "automatic" virtual memory but 16 KB segments can be mapped from 128 KB of RAM and three 128 KB ROM chips. The ROMs can be removed from their sockets, and read and written by a standard PROM burner. The Advantage was introduced circa 1987, and there have been several firmware upgrades since then (e.g., version 5 circa 1997, version 9 circa 2003).

A voter panel (38x28 inches) has 42 rows and 12 columns of half-inch square buttons. To the left of each button is a green LED light in the shape of an X (1/4 inch square). The entire panel is covered by a large sheet of paper on which the names of contests and candidates are preprinted, one for each button/light that will be in use. This paper is covered by a transparent mylar sheet. On the paper sheet, next to each candidate name, is printed a box about half-inch square, directly over a button. When a voter presses this place on the mylar sheet, the button underneath the paper is pressed. When the Advantage illuminates a green X, it shines through the paper.

*Segment of voter panel (this one has arrows instead of Xs)*

The Z80 can at any time read buttons and illuminate lights but the firmware does not actually interpret these buttons to indicate votes unless the machine has been "activated" by the operator; that is, a pollworker presses a button on the "operator panel" at the side of the machine to indicate that a voter may cast a ballot.

On the side of the machine (when unfolded), an operator panel has an LCD display with two rows of 25 characters, and has 14 buttons used by pollworkers to enable voting, set party affiliation during primaries, and other operations. There is a printer inside the cabinet that prints on standard 4.25 inch rolls of thermal paper; this is used to print diagnostics, status, and results at the close of the polls, and is normally inaccessible while voters are voting.

The "results cartridges" are about the size and shape of a VCR cartridge. They contain (typically) 128 KB static RAM maintained by AA batteries (as the technology predates flash memory). They plug into the AVC Advantage motherboard or into a WinEDS computer with an IEEE 488 connector, though they don't necessarily communicate using the IEEE 488 protocol.

**Audio Kit.** The Advantage 9.00 has an "audio kit" that provides an audio description of the ballot and a minimal four-button interface for any voter who wishes to vote by audio—because of vision impairment, mobility impairments, inability to read, or any other reason—instead of on the regular voter panel.

Because the Z80 is slow and has little memory, the audio-kit computer resides on a "daughterboard," inside the cabinet but separate from the main circuit board of the AVC Advantage. The daughterboard contains an entirely separate and much more powerful 486-compatible processor, 8 MB of DRAM mapped into the 486 address space, and 2 MB of flash memory formatted as a standard Microsoft FAT file system. This flash memory is not directly executable, but the daughterboard operating system has a bootstrap loader that automatically copies from the onboard flash memory and/or the Audio Ballot Cartridge to the DRAM on start-up.

An audio ballot cartridge is a PCMCIA cartridge, typically 64 MB, that plugs into a PCMCIA slot on the top of the audio kit daughterboard. It too is formatted with a FAT file system and is accessible to the 486 processor as a virtual disk drive. On the Audio Voting Assembly (the handheld unit with the four-button interface, connected by a cable to the audio-kit daughterboard) there is another processor, very possibly containing flash memory containing executable code as well as data.

**Software.** By Court Order we had two AVC Advantage 9.00H voting machines belonging to Union County, New Jersey, and their source code provided to us by Sequoia via Wyle Laboratories. We also had a copy of the very similar 9.00G source code. The software consists of almost 130,000 lines of source code (including comments and empty lines, including both motherboard and some daughterboard code) in over 700 source files. Somewhat over 25,000 lines are in Z80 assembly language and the rest are in C. Excluding comments and blank lines, there are 38,000 lines of source, of which 12,000 are in assembly language.

The Z80 runs a special purpose operating system written by Sequoia or one of its predecessors. Since memory is limited, an overlay mechanism swaps code segments in from ROM. The operating system implements a special purpose in-memory file system with "files" for system parameters, ballot definitions, votes cast so far and the like. The results cartridge is also mounted as a file system.

Source code comments describe myriad changes from 1987 through October 2005, by at least a dozen different people. The changes include bug fixes, rearrangements to cope with resource constraints, and revisions to meet programming guidelines and requirements from the Federal Election Commission.

The daughterboard runs a version of MS-DOS. We examined source code for the audio-voting application and execution-environment components such as AUTOEXEC.BAT. In spite of Court orders, we never did obtain the full

source code and development tools for other daughterboard components, such as the operating system, though we were able to examine all components in executable form by extracting them from the flash memory.

On power-up, the daughterboard's AUTOEXEC.BAT executes. It does something related to the installation of new firmware from the audio-ballot cartridge into the daughterboard flash memory, and starts up the audio-voting application.[2]

**AVC Advantage Failures and Vulnerabilities.** The Advantage has design flaws, software bugs, failures, and vulnerabilities; our full report [3] lists several dozen in the broad categories of fraudulent firmware, daughterboard and WinEDS viruses, user interface problems, and errors in design and code. In this paper, we describe some of the most significant.

# 4 User interface flaws

We found two design flaws of the AVC Advantage which may cause inaccuracy in counting votes: (1) *the AVC Advantage sometimes appears to record a vote when in fact it does not, and* (2) *vice versa.* Thus, a voter may mistakenly think she has voted, when she has not; or a voter may vote, and then be invited to vote again by a pollworker who mistakenly thinks her vote was not recorded.

We were unable to measure this quantitatively, because we examined only the voting machine and not its interaction with real voters in real elections. However, these design features are consistent with reports that voters and pollworkers were not sure whether votes were recorded, and pollworkers asked voters to reenter the voting machine and try again.[3] They are also consistent with a 1% undervote observed in the one precinct in which we subpoenaed "voting authority" stubs.[4] In precinct 6 in Pennsauken, NJ on February 5, 2009, there were 283 Democratic voting-authority stubs but the public counters of the 3 AVC Advantage machines added up to only 280, with 280 votes recorded. There was only one race on the ballot, and the AVC Advantage is not supposed to permit casting of an entirely blank ballot *once the machine is activated for the voter.* Therefore it is possible that the design features we describe in this section may cause significant inaccuracy. This warrants further research, in the form of user studies and/or by auditing the pollbooks (voter sign-in books) of actual elections versus precinct-by-precinct vote totals in those elections.

**Normal behavior.** To enable a voter to vote, the pollworker presses the green "Activate" button on the operator panel to make the Advantage ready to accept votes. The Advantage indicates readiness by emitting a chirping sound for 1/4 second, turning on the fluorescent light on the inside of the top panel of the machine to illuminate the inside of the booth, and (optionally) lighting a green X next to the name of each contest to be voted.[5]

After the operator has activated the machine, the voter selects candidates by pressing on the buttons (through the paper, at spots indicated by printed squares). A green X appears by each candidate that the voter selects. If the voter presses the wrong button, she can deselect the candidate by pressing the button again, and the X disappears, so that another candidate may be selected.

Also when a button is pressed to select a candidate, an LCD display at the bottom of the voter panel (about 30 inches from the floor) displays the name of the contest and the name of the candidate. This panel is about 3.75 inches wide and slightly over half an inch high; it displays two rows of 24 gray letters on a yellow-green background.

After at least one vote is selected for at least one contest, the machine illuminates the Cast Vote button in bright red. This button, about 7/8 inch by 1/2 inch, is below the voter panel at the right-hand side.

When a voter is satisfied with her choices, she presses the Cast Vote button. This causes the votes to be recorded, the overhead light to extinguish, the Cast Vote button to darken, and all the Xs to disappear from the voter panel. The machine chirps, and the LCD display under the voter panel changes to read "VOTE RECORDED THANK YOU".

[2] In October 2008 Sequoia asked the Court to redact many paragraphs of our report, claiming that they revealed trade secrets. We disputed this claim, since we do not believe the report contained trade secrets, in the legal sense. Pending a full hearing on these disputed claims, the Court redacted just four paragraphs (19.8,19.9, 21.3, 21.5) and certain appendices. From paragraphs 19.7, 19.10–19.14, 21.4, and 21.6, of our redacted report [3] the reader can get a sense of the firmware-upgrade mechanism and its security vulnerabilities.

[3] These reports come in the form of anecdotal evidence by some voters; in the form of sworn testimony from one voter in the NJ trial; and in a personal communication by the Union County Clerk, Joanne Rajoppi, to Penny Venetis in February 2009.

[4] "Voting authorities" are serial-numbered slips of paper, which the voter receives upon signing the pollbook register, and which the voter hands to the pollworker who stands at the operator panel of the voting machine before entering the booth.

[5] This last option is enabled in Mercer County and disabled in Union County, at least in the February 5, 2008 presidential primary.

At a time when the machine is activated but no candidates are selected (either because the voter has not selected any, or has selected and then deselected some), the Cast Vote button is unlit, inactive, and will not have any effect when pressed.

**Voting when the machine is not activated.** The Advantage gives the false impression that it is recording votes, even when it is not doing so. If a voter tries to vote when the Advantage is not activated, then it will give three different kinds of visual indications that the vote is recorded, even though it did not actually record the vote at all. Even though no vote is recorded, the Advantage lights the X by each selected candidate button (for one full second), it illuminates the Cast Vote button when pressed (for one second), and it continues to display "VOTE RECORDED THANK YOU" on the LCD panel visible to the voter (this message remains from the previous voter, even after candidate buttons are pressed in inactive mode). With this feedback, many voters would assume that their vote had been recorded.


Sequoia's apparent purpose in programming the AVC Advantage this way is to permit pollworkers to test buttons and lights between voters. However, it is a dangerous design. The pollworker who must press Activate for each voter is responsible for up to 6 voting machines in the same precinct. It is all too easy for the voter to enter the booth without the pollworker noticing, or for the pollworker to fail to press the activate button.[6]

**Inadequate feedback when a vote is recorded.** The Advantage makes a chirping sound when the machine is activated for a voter to vote. It makes the same sound when the voter presses the Cast Vote button (and a vote is recorded). The sound comes from a small speaker in the operator panel. We believe that, depending on the ambient noise level in the polling place and the hearing acuity of the pollworkers, the sound may be too quiet for its intended purposes: to alert all relevant witnesses that a vote is being cast (to prevent unauthorized votes), and to signal to the voter and the pollworker that the vote is recorded (to reduce uncertainty).

In addition to the audible feedback, the LCD display on the voter panel switches from voter-active mode back to voter-inactive mode, and the public counter (which counts the number of voters in this election) increases by one. But a pollworker observing an AVC Advantage in voter-inactive mode may not remember what the value of the public counter was before this voter entered, and may not remember whether he had activated the machine—in either case, the LCD display will be in voter-inactive mode.

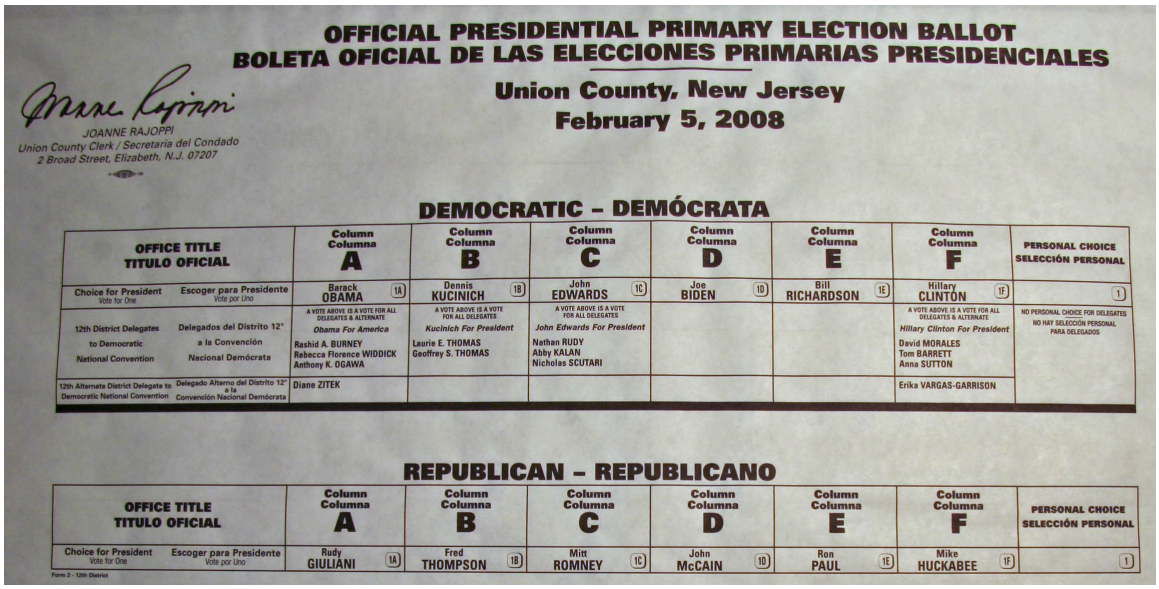
We believe that these design features have the potential to cause substantial inaccuracy in tallying votes in real polling-place conditions with real voters. It would be useful to study this issue quantitatively. Pollworkers in New Jersey issue consecutively numbered voting authority tickets in each precinct. In principle the number of voting authorities should match the public counters of the voting machines. A mismatch could be a measure of the user-interface problems we have described, or of other problems. However, County Clerks in New Jersey do not generally report the number of voting-authority tickets issued in each precinct, so it is difficult to audit this measure.

# 5 Software bug that disenfranchised some New Jersey primary voters

In any election, the Advantage counts the number of voters in this election (the "public counter") and the number of voters since the machine went into service (the "protective counter," which can be reset on command)[7], and the number of votes each candidate received ("candidate totals").

[6] A corrupt pollworker could even exploit this behavior to deliberately disenfranchise some voters, by failing to press the Activate button.

[7] When mechanical voting machines came into use in the early 20th century, they were equipped with a "protective counter," an odometer-like mechanical counter that increments each time a ballot is cast and can never be reset. That is, it counts the number of voters who have ever used the machine. In addition, they have a "public counter" which increments each time a ballot is cast, but is reset to zero before each election. Both these counters are visible to pollworkers (and in principle to the public) throughout the election. The purpose of the protective counter is to detect certain kinds of manipulation and/or unauthorized casting of ballots. New Jersey statute (Title 19) requires that voting machines be equipped with a protective counter. On the AVC Advantage, the protective counter and public counter are implemented as locations in the battery-backed internal RAM. They are displayed on the LCD of the operator panel; in our photograph on the next page labeled "Operator Panel", the protective counter is 4363 and the public counter is 0. On the AVC Advantage, the protective counter can be reset to zero via a menu command on the operator panel; this command is not available in election mode but is available between elections. We believe the AVC Advantage's "protective counter" does not serve the role commonly understood by that name, since it is easily manipulated.



**OFFICIAL PRESIDENTIAL PRIMARY ELECTION BALLOT**
**BOLETA OFICIAL DE LAS ELECCIONES PRIMARIAS PRESIDENCIALES**

**Union County, New Jersey**
**February 5, 2008**

JOANNE RAJOPPI
Union County Clerk / Secretaria del Condado
2 Broad Street, Elizabeth, N.J. 07207

**DEMOCRATIC – DEMÓCRATA**

| OFFICE TITLE / TITULO OFICIAL | Column A | Column B | Column C | Column D | Column E | Column F | PERSONAL CHOICE / SELECCIÓN PERSONAL |
|---|---|---|---|---|---|---|---|
| Choice for President / Escoger para Presidente (Vote for One / Vote por Uno) | Barack OBAMA (1A) | Dennis KUCINICH (1B) | John EDWARDS (1C) | Joe BIDEN (1D) | Bill RICHARDSON (1E) | Hillary CLINTON (1F) | (1) |
| 12th District Delegates to Democratic National Convention / Delegados del Distrito 12° a la Convención Nacional Demócrata | A VOTE ABOVE IS A VOTE FOR ALL DELEGATES & ALTERNATE *Obama For America* Rashid A. BURNEY, Rebecca Florence WIDDICK, Anthony K. OGAWA | A VOTE ABOVE IS A VOTE FOR ALL DELEGATES *Kucinich For President* Laurie E. THOMAS, Geoffrey S. THOMAS | A VOTE ABOVE IS A VOTE FOR ALL DELEGATES *John Edwards For President* Nathan RUDY, Abby KALAN, Nicholas SCUTARI | | | A VOTE ABOVE IS A VOTE FOR ALL DELEGATES & ALTERNATE *Hillary Clinton For President* David MORALES, Tom BARRETT, Anna SUTTON | NO PERSONAL CHOICE FOR DELEGATES / NO HAY SELECCIÓN PERSONAL PARA DELEGADOS |
| 12th Alternate District Delegate to Democratic National Convention / Delegado Alterno del Distrito 12° a la Convención Nacional Demócrata | Diane ZITEK | | | | | Erika VARGAS-GARRISON | |

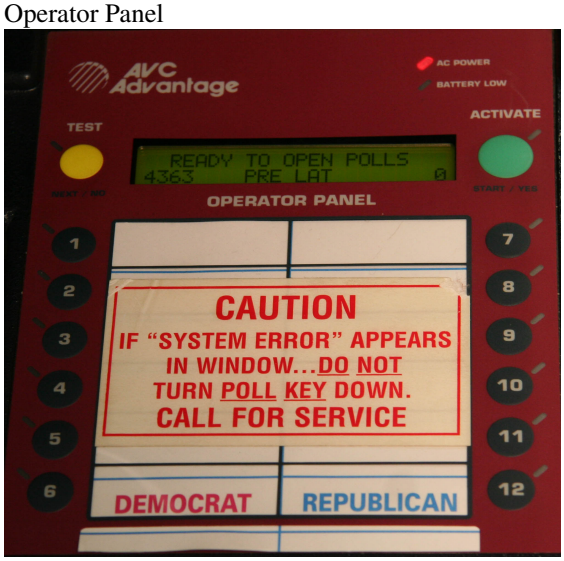
**REPUBLICAN – REPUBLICANO**

| OFFICE TITLE / TITULO OFICIAL | Column A | Column B | Column C | Column D | Column E | Column F | PERSONAL CHOICE / SELECCIÓN PERSONAL |
|---|---|---|---|---|---|---|---|
| Choice for President / Escoger para Presidente (Vote for One / Vote por Uno) | Rudy GIULIANI (1A) | Fred THOMPSON (1B) | Mitt ROMNEY (1C) | John McCAIN (1D) | Ron PAUL (1E) | Mike HUCKABEE (1F) | (1) |

Form 2 - 12th District

In a primary election, a voter may vote either in the Democratic primary or the Republican, but not both. The Advantage does not have the capability to show only the candidates for a single party, because the "display" is just a large paper sheet preprinted with candidate names and positioned over the appropriate buttons under the paper. Instead, only one party's ballot is enabled for a voter. Upon registering at the polling place, the voter is given a voting authority (a piece of paper) for his or her chosen party, which is handed to the pollworker. The pollworker tells the machine which party's ballot to activate, by pressing an extra button (an "option switch") before pressing the Activate button on the operator panel. The operator is supposed to press either "6" or "12", depending on the configuration set up on the ballot cartridge, then press Activate to permit the voter to cast his or her vote. Depending on which option switch is chosen, either the Democratic or the Republican candidate buttons on the voter panel will be active. "Active" simply means that the firmware will respond to it; the firmware ignores inactive buttons.

Operator Panel




At the close of the polls, the Advantage prints "option switch totals," the number of voters enabled to vote in each party's primary. In the New Jersey Presidential Primary of February 5, 2008, Union County Clerk Joanne Rajoppi noticed a discrepancy between candidate totals and option-switch totals printed out by some AVC Advantage voting machines. She alerted the county clerks of other counties, and they found dozens more similar discrepancies.

In all, anomalies were found on at least 38 voting machines in 8 counties. On several machines the number of votes for Democratic candidates *exceeded* the number of Democratic voters who had voted, according to the results report printed by the machine just after the close of the polls. Each of these voting machines *disagreed with itself* about how many Democratic primary voters there were. On other machines, the number of votes for Republican candidates exceeded the number of Republican voters.

A subsequent press release by Sequoia explained that this was caused by a software bug in the software's user interface module. The election worker, on being handed a voting authority labeled DEMOCRAT, was expected to press 6 (labeled DEMOCRAT) then the Activate button (both on the operator panel). If instead he pressed 6, then pressed an unlabeled button (1–5 or 7–11), then Activate, a bug caused the machine to behave incorrectly: the red light next to operator-panel button 6 would stay illuminated; the option-switch total would count as 6 (thus adding 1 to the total number of votes cast for Democrats); but the *Republican* ballot would be enabled on the voter panel, and the machine would accept votes only for Republican candidates. Thus the bug caused the wrong values to be recorded

in the option-switch totals, and causes candidate totals to be inconsistent with option-switch totals (which is what Ms. Rajoppi noticed).

It is easy and natural for a pollworker to make this mistake. Button 7 is directly under the Activate button. Pressing 6-then-7 instead of 6-then-Activate would be natural; attempting to correct the problem by pressing Activate leads to the sequence 6-7-Activate. The consequence (unmentioned in Sequoia's press release) is that the voter is precluded from voting in his or her selected primary (thus being disenfranchised) and at best is able to vote in the other primary (thus voting in a primary that she is not legally entitled to vote in). This is because, under New Jersey law, a voter who is registered in a party is entitled to vote in that party's primary and is *not* entitled to vote in the other party's primary.[8]

Our detailed examination of the source code, and experiments on the actual voting machine, confirmed Sequoia's explanation that a programming error (a bug in the code that handles input from the operator panel) caused the option-switch anomalies.

# 6 Firmware Replacement

The most dangerous insecurities in DRE voting machines, and in the Advantage in particular, permit an attacker to install a fraudulent vote-counting program to control the computer in the voting machine. We created such a fraudulent vote-counting program, installed it into the Advantage, and demonstrated that it was easy to change the votes that were cast.

The techniques that we used to create this program required only straightforward programming and standard software tools. It is easy to gain physical access to Advantage machines throughout New Jersey before and after elections. The locks and seals on the Advantage do not prevent this tampering. We had access to source code, which made our task easier, but it would be straightforward to reverse-engineer compiled code to achieve the same effect.

Our vote-stealing firmware is a small addition (122 lines of source code, $\sim$ 600 bytes of machine code) to the Z80 program resident in the motherboard ROMs. Installation of the firmware requires replacing just one ROM chip, installed in a socket on the motherboard. Design of the fraud requires either access to the source code, or reverse-engineering the firmware present in every AVC Advantage voting machine. Based on an experiment by Halderman and Feldman in reverse-engineering the AVC Advantage 5.00E firmware [11], we estimate that reverse-engineering the 9.00H firmware would take at most a few person-months; see our full report for details.

**Access to ROMs containing firmware.** The physical part of the attack requires access to the Advantage for a few minutes. Since machines are typically left unguarded at polling places for days before and after elections,[9] this is easy. The cabinet of the Advantage has a door at the rear, which must be opened to access the cartridge ports, the printer, and the circuit boards (which are additionally covered by a sheet-metal circuit-board cover). The door is equipped with a cheap wafer-tumbler key-lock. We found that the keys can be duplicated at our local hardware store. Even without a key, the door is easily opened by picking the lock. Appel had never before attempted to pick a lock before beginning this study, but with a day or two of practice, could reliably pick the lock in less than 15 seconds.

The motherboard is in a metal box with a circuit-board cover held in place by ten screws. Once the cover is off, it is easy to pry out one or more of the ROMs and replace them with new ones that steal votes or otherwise compromise the election process.

With a modicum of practice, Appel could consistently and repeatably pick the lock, remove the screws, replace the ROM, replace the screws, and lock the door, all in less than 7 minutes.

**Hacking many voting machines.** This attack requires physical access to a large number of voting machines for 10 minutes each. Such access can be obtained either at the factory where firmware-upgrade ROMs are prepared, at the election warehouse, or in polling places where voting machines are left unattended before and after elections. A typical county election warehouse holds 500 or more machines; for hacks of unattended machines at polling places, a

[8] Party registration is established the first time a voter votes in any party's primary; a voter not registered in either party becomes registered by voting in a primary. However, by the time a voter approaches the voting machine, she has already been handed a Voting Authority ticket for one party or the other. That is, party registration has already been established (or confirmed) at the sign-in desk. It is then inconsistent with State election law for the voting machine to present the wrong primary ballot, enabling the voter to vote in the wrong primary.

[9] Testimony of Edward W. Felten on his observations and photographs of unattended voting machines in the days before elections in Princeton; see also [10]. Also, depositions and trial testimony of three NJ county election officials confirmed that they deliver voting machines up to a week before the election, and collect them up to a week after; that the locations where they deliver the voting machines are often unattended (to the point where sometimes there is no person there even to accept delivery) and accessible to the public.

typical polling place has up to 4 machines (typically 2 machines per precinct; precincts are often colocated at polling places).

New Jersey uses about 11,000 voting machines for statewide elections; hacking 550 machines to each shift 20% of the vote would shift a statewide election by 1%; hacking 1,100 machines would shift a statewide election by 2%. A congressional district has about 850 machines, a legislative district has about 275 machines; a big-city municipal election has about 350. To cheat in these elections a much smaller number of machines would need to be hacked.

Once an attacker has installed fraudulent firmware in an AVC Advantage ROM, it can remain in place for election after election, stealing votes in favor of the same political party.

**Vote-stealing programs can avoid detection.** A nefarious program can deliberately misinterpret the voter's button-press by lighting the button for the voter's candidate while quietly recording a vote for an opponent; it can modify the record of votes cast in the machine's memories at any time before the polls close; or it can violate the privacy of the ballot by storing a record of how each voter actually voted, in sequential order. In our video demo [2] we illustrate modifying the votes cast to change the outcome of an election.

Our vote-stealing program moves votes from one candidate's total to another, while taking care not to change the total number of votes cast.

The Advantage has a "pre-election logic-and-accuracy testing" (Pre-LAT) mode, in which election officials can check the ballot definition to make sure the candidates' names are printed over the right buttons. But the control program for the AVC Advantage "knows" whether it is in Pre-LAT mode or Official Election mode; our fraudulent firmware takes care to change votes only in Official Election mode and does nothing untoward in Pre-LAT or Post-LAT mode.

Therefore pre-LAT testing is useless to detect fraudulent firmware. Many other forms of black-box testing will also fail to detect the fraud, since a real vote-stealing program would carefully examine its environment to ensure that it is in a real election—not in a test—by checking dates, date change history, voting patterns, how many hours the polls have been open, etc. Our demonstration fraud takes only two such measures: it cheats only in official election mode, and it waits until the 20th voter casts a vote. Then it walks through the saved ballot images in memory. On half the ballots it changes a vote from one candidate to another and adjusts the candidate totals accordingly. It writes its fraudulent ballot images and candidate totals both to the internal memory and to the Results Cartridge.

When the polls are eventually closed, the results-report printout is generated from the machine's internal memory. Therefore, all the so-called "audit trails" and results data agree with each other and with the printout.

To demonstrate a vote-stealing program on Union County's machines as they were set up for this election, we ran a fake election [2] in which 16 votes were cast for Mr. Richardson and 4 votes for Mr. Kucinich, both Democrats. When this sequence of votes is cast during the pre-LAT phase, the results are exactly as expected: Richardson 16, Kucinich 4. The identical sequence of votes was then cast in official election mode. This time Mr. Richardson only received 8 votes, while Mr. Kucinich received 12.

The AVC Advantage records votes in four different ways: candidate totals stored in internal (motherboard) memory, candidate totals stored in results-cartridge memory, ballot-image list (so-called "audit trail") stored in internal memory, and ballot-image list stored in cartridge memory. Our vote-stealing program alters all four of these memories, and therefore both the close-of-polls results-reports printouts and the cartridge tabulations will show this fraudulent result: Richardson 8, Kucinich 12.

Sequoia's *AVC Advantage Security Overview* [19] claims that cryptographic techniques are used that prevent such firmware replacement; this claim is false. A checksum of the contents is part of each ROM and also (conveniently) appears on a paper sticker on the chip. This checksum is merely the mod $2^{16}$ sum of the bytes in the ROM. To install our own firmware, we only had to insert our code in some unused part of the ROM, then add filler bytes so that the checksum was unchanged. Of course, even if Sequoia had used a more-secure cryptographic hash to validate ROM contents, this validation firmware would be in the ROM itself, and could be replaced by a fraudulent validation computation when the ROM is replaced by an attacker.

**Physical seals.** Until we had delivered our report on September 2, 2008, New Jersey's AVC Advantage voting machines had no tamper-evident seals to protect access to the motherboard. We believe that this is because there are 4 AA batteries on the circuit board that maintain the state of the RAM and those must be replaced often enough that replacing seals would be a nuisance.

A plastic strap seal is installed before each election, through the cartridge and through a slot in the Advantage sheet metal. Each seal is stamped with a serial number. This seal does not provide security against ROM-replacement

attacks because (1) It is possible to remove the circuit-board cover without affecting the seal. (2) Even if that were not possible, the strap seals are removed at the close of polls, leaving unattended voting machines in elementary schools and church basements for several days after the election with no seal in place. (3) Even if that were not possible, one can remove and replace such seals using very simple tools and techniques, such as "poke with a jeweler's screwdriver." (4) Even if that were not possible, the serial numbers appear to start over from zero whenever a new batch is obtained, so they provide no protection—if a seal were broken, a new one with the same number could be installed. (5) Even if that were not possible, numbered seals are useless if nobody checks the numbers. The seal numbers are supposed by recorded by pollworkers on the close-of-polls results-report printouts that they sign, but an examination of 50 such reports finds half of them with no seal numbers written down.

**Daughterboard Vulnerabilities.** The daughterboard on the AVC Advantage 9.00 does not count votes; for blind voters (or other audio voters) it plays the audio files, receives the vote from the audio-kit input device, and transmits that vote to the motherboard. On the AVC Advantage model 10, the daughterboard runs the election and counts the votes. Fraudulent firmware in the daughterboard has different consequences in the two models.

The daughterboard firmware resides in flash memory, which contains the election control program, as well as ballot definitions and other files. Unlike ROM, which cannot be modified without removing and replacing physical computer chips, flash memory can be written and rewritten by the software (or firmware) inside the computer.

Therefore, firmware in flash memory is inherently more vulnerable to fraudulent replacement than firmware in ROM. The fact that the election program can write to the very memory that stores the election program is potentially quite dangerous. The AVC Advantage is certified only to the 1990 standards; we believe this firmware design would not meet the 2002 or 2005 FEC/EAC voting systems standards.[10]

We installed new firmware into the daughterboard by exploiting Sequoia's firmware-upgrade mechanism: that is, simply by inserting an ordinary audio-ballot cartridge, without changing any ROMs at all. A virus carried this way into the daughterboard can steal votes, cause machines to fail in targeted ways, and propagate itself both to other AVC Advantage voting machines and to WinEDS computers where votes are tabulated.

Because an audio-ballot cartridge can simultaneously hold firmware replacements and audio ballots, installation of fraudulent firmware can be done inadvertently by a perfectly honest pollworker in the ordinary course of inserting an audio-ballot cartridge to prepare an AVC Advantage for an election.

In addition, because this fraudulent firmware can then copy itself onto any new audio-ballot cartridge later inserted into the Advantage, the fraud can become a virus that propagates itself from one Advantage to another. Such cartridge-borne voting-machine viruses are now well-understood [9].

Such a virus can also jump to WinEDS computers [8, §4.7], that is, computers used in the election warehouse to prepare new ballot cartridges and to tabulate election results. Such a virus could change vote data in the election database, and modify the tabulated results. From WinEDS computers, the virus can jump back to other Advantage machines.

**Stealing from the blind.** On the version-9 AVC Advantage that we examined, the daughterboard interprets the votes of only those voters who vote by audio. Fraudulent daughterboard firmware can change those votes. Daughterboard firmware cannot change votes cast through the main voter panel, or stored in motherboard memory or results cartridges.

**Denial of service.** The daughterboard computer is connected to the motherboard by a three-wire RS-232 connection. Upon startup, the motherboard computer sends a message to the daughterboard, and expects acknowledgment. If the daughterboard does not reply, or replies with an ill-formatted message, the motherboard reports an error on the operator panel. Because the daughterboard has information about the precinct-number of the voting machine, an attacker can program a daughterboard virus to perform targeted election-day denial of service. That is, voting machines in a certain set of precincts (chosen by the attacker) will fail to start up properly on the morning of election day, because the daughterboard virus disables the daughterboards of just those machines. Voters waiting in line may then leave the polls without voting, especially if pollworkers do not promptly deploy emergency paper ballots, or if the 30 emergency paper ballots (provided in each voting machine) run out.

[10] "The election-specific programming may be installed and resident as firmware, provided that such firmware is installed on a component (such as computer chip) other than the component on which the operating system resides." (FEC 2002 Voting Systems Standards, Sec. 6.4.1; EAC 2005 Voluntary Voting Systems Guidelines, Sec. 7.4.1.) But in fact, we found that the same flash memory chip on the daughterboard holds both the operating system and election-specific programming.

This denial-of-service attack is effective even if audio voting is disabled. If the ballot definition (installed in the motherboard results cartridge) does not enable audio voting, then the AVC Advantage is supposed to go ahead with an election even if the daughterboard does not respond. One might think that this would provide a defense against daughterboard denial-of-service attacks: just disable audio voting in the ballot definition. (Of course, this renders the election HAVA-noncompliant.)

However, in the motherboard program that receives messages from the daughterboard through the RS-232 cable, we found a buffer-overrun bug. This bug can be exploited by a daughterboard virus to crash the motherboard program, even if audio voting is disabled in the ballot definition. (We did not find a way to exploit this buffer-overrun to perform code-injection attacks or even return-to-libc attacks; we were able to return to address 0, which reboots.)

**WinEDS.** The WinEDS software, sold by Sequoia, is used by county election workers to prepare ballot definitions and to tabulate votes. WinEDS runs on ordinary personal computers running Microsoft Windows. By Court Order, New Jersey provided to us for examination one election-warehouse computer belonging to Union County: a Dell Latitude 110L laptop computer running Microsoft Windows XP SP3 and with WinEDS 3.1 installed.

The WinEDS computer is equipped with a reader for large-format Results Cartridges connected by a USB port. Audio-ballot cartridges connect into the standard PCMCIA port of the laptop computer, using a standard PCMCIA extender card.

Election workers use WinEDS to write ballot definitions into Results Cartridges and audio ballot cartridges before an election. These cartridges are then inserted into voting machines before the machines are transported to polling places. After the election, the cartridges are removed from the machines and transported back to county election workers, who use WinEDS to extract the election results and cumulate the results from all precincts.

**Virus propagation via cartridges.** Computer viruses carrying fraudulent vote-counting or vote-tabulation firmware can propagate through audio ballot cartridges.

When a PCMCIA flash memory card (such as an audio-ballot cartridge) is plugged into the PCMCIA port of a computer running Microsoft Windows, the operating system views the data on the card as a "removable disk." This is the case on the Union County computer we examined, and we presume that other computers are configured similarly.

The Sequoia audio-ballot cartridges, which are standard PCMCIA cartridges in a nonstandard plastic case, operate exactly in the standard way when plugged into a Windows computer. On Windows, when one inserts a CD-ROM disk, the folders in that disk become visible just like folders on the internal hard drive. Similarly, when one inserts the audio-ballot cartridge into a Windows computer that runs WinEDS, the cartridge is auto-mounted as a folder that is visible to Windows applications and to Windows Explorer.

In Microsoft Windows, when removable media such as PCMCIA or CD-ROM are inserted and automounted, Windows normally searches for files such as AUTORUN.INF that cause a program from the removable media to be executed as a Windows application. The California Top-to-Bottom study [8, §4.7] found that Sequoia configured WinEDS machines to leave Autorun enabled, and we found that the Union County computer was also configured this way. This means that merely inserting a virus-carrying cartridge causes infection; no user action is required and most users will never notice anything happening.

Thus, an "infected" audio-ballot cartridge can propagate the virus to a WinEDS computer by exploiting the Autorun vulnerability; and can propagate to an AVC Advantage by exploiting the firmware-upgrade mechanism. If an uninfected cartridge is later installed into an infected WinEDS computer or AVC Advantage voting machine, the virus can copy itself onto that cartridge. Also, while the virus resides on the WinEDS computer, it can copy itself onto other WinEDS computers on the same network.

**Virus propagation via networks.** Viruses can also infect the WinEDS computers when they are connected to the Internet and used for web browsing. We found that the Union County WinEDS computer had been used for a substantial amount of casual (personal) Internet surfing, contrary to guidelines and common sense. The security configuration of this computer was wide open, leaving many unnecessary services and ports active. Thus, the computers that run WinEDS in Union County are severely vulnerable to attacks from the Internet. There is no reason believe that the Union County computers are in any way different from WinEDS computers used in other counties in New Jersey.

Viruses that arrive from the Internet can propagate via cartridges into AVC Advantage voting machines, without the attacker ever coming near a voting machine.

**Version 10.** In the version 9 AVC Advantage, the consequences of a virus attack are limited "only" to stealing the votes of disabled voters (at the polling place), selective denial-of-service attacks (at the polling place), and wholesale fraud in vote tabulation (on WinEDS computers).

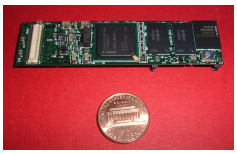
In contrast, the problem is potentially much worse on the version-10 AVC Advantage. The version 10 has the same hardware but much different firmware: the daughterboard computer runs the election and records the votes in the PCMCIA cartridge [21]. The motherboard serves only as an I/O processor for the voter panel. In the version 10, therefore, the consequences of fraudulent firmware installation in the daughterboard flash memory are *much more severe*. If fraudulent firmware were to propagate from a county's corrupted WinEDS computers via cartridges onto version 10 AVC Advantages, such firmware could steal votes in every precinct in that county. [11]

# 7 Tampering with Results Cartridges

Results Cartridges are used for transmitting the ballot definition to the Advantage, and transmitting the election results from the Advantage to a WinEDS computer. It is easy to physically and electronically manipulate Results Cartridges, either to change the votes in them or turn them into other types of cartridges (e.g., consolidation cartridges, early voting cartridges). Results cartridges are very insecure against tampering with the votes stored inside: there is no protection (either via hardware or via cryptography) against reading and writing the data in the cartridge.

We wrote a simple program that runs on an ordinary personal computer, to change votes inside the candidate-total files and ballot-image files stored in a Results Cartridge. When the altered Results Cartridge is inserted into WinEDS for tabulation, WinEDS notices nothing amiss about the fraudulent data.





*Top left: Cartridge reader/writer prototyped by Hovav Shacham's research group [7]. Bottom left: Our nonfunctional mockup of installation in cigarette pack. Right: "Gumstix" computer that could be programmed to alter votes in cartridge.*

It is possible to make a simple device that changes the votes in a Results Cartridge. The photo above shows a reader/writer prototyped at the University of California, San Diego; it connects a computer to a cartridge. One could add to it a tiny computer (shown at bottom right in the figure) to make a self-contained intelligent cartridge-data manipulation device. We made a nonfunctional mockup of such a device in a cigarette pack. One would plug this device into the Results Cartridge, and remove it after 2 or 3 seconds. The whole process could be done unobtrusively in 5 seconds. In that time the device could read the votes (candidate totals and audit trail) from the cartridge, and write fraudulent data (candidate totals and audit trail) to the cartridge. This could be done by the pollworker who removes the cartridge from the machine before bringing it to the table where the other pollworkers witness putting it into the bag, by a pollworker at the table while the other workers are busy with other tasks, by a person who transports the cartridge to county election officials for tabulation, or by a person who removes the cartridge from the bag before tabulating in WinEDS.

As we will explain in Section 8, no digital signatures protect the vote data in a Results Cartridge. Thus, once a Results Cartridge leaves the voting machine, it is *immediately* susceptible to modification of vote data. And as we show in Section 10, election officials rely on the cartridge data for election tabulation and certification, and there is no State requirement that they examine the paper printouts.

[11] We did not examine a version-10 AVC Advantage or its firmware; we rely on the architectural description of this machine given in the cited Wyle report to see that the hardware architecture is the the same as that of the 9.00H.

# 8 No effective digital authentication

No digital signature or cryptographic authentication protects the vote data in the Results Cartridge from modification. Sequoia claims, in its AVC Advantage Security Overview, [19, page 9]

> "After polls are closed, the Advantage immediately calculates and stores cryptographic signatures of each of the totals data files (ballot images, write in names, candidate summary totals, and selection code summary totals). The cryptographic signature values are stored in both the Audit Trail and Results Cartridge memories."

This is not true. Some hash functions and checksums are used, which are insecure; and apparently WinEDS does not even check for them in results cartridges.

"Cryptographic signature" is an informal term for the standard term *digital signature*. Digital signatures are used to protect computer data so that accidental or deliberate modification can be detected. A digital signature algorithm authenticates a data file by applying the signer's secret key to produce a signature. The important property of a cryptographic signature is that one can check the authenticity of a signature without knowing the secret necessary to sign a document. Only someone in possession of the *signing* key, someone who intends to authenticate this data, can produce this signature string. Therefore the signature string *proves* the authentication of this data.

In our examination of Sequoia's source code, we found no use of digital signatures (or "cryptographic signatures") at all.[12] Not a single piece of data or firmware is protected by the use of digital signatures against deliberate fraud.

The Advantage uses many different kinds of hash functions, CRCs, and checksums to protect different kinds of data. It calculates an 8-bit (CRC-8) checksum for the ballot definition, for vote totals, for each ballot image in the "audit*trail" and for the ballot-image file overall. If an attacker were to write new ballot images and candidate totals into a Results Cartridge, he could easily generate new CRC-8 checksums. This is because hash function and checksums are weaker than digital signatures—they are meant to detect accidental data changes but not intended to detect deliberate falsification.

But some of the checksum algorithms used in the AVC Advantage are even too weak to protect reliably against inadvertent data modification. For example, the contents of program ROMs are protected by a naive "checksum" computed by simply adding up the bytes, a method that has been obsolete for many years.[13]

# 9 Fraudulent ballot definitions

Given the ease with which viruses can propagate through the WinEDS computers that prepare ballot definitions, the possibility of election fraud by means of deliberately corrupt ballot definitions is of particular significance. The Advantage does some checking for ill-formed ballot definitions, but the ballot definition format is a complex linked data structure and the checking is not perfectly thorough. We found some potential vulnerabilities there, but did not have time in our limited access to the machines to develop these vulnerabilities into fully demonstrated attacks.

One can confuse the Advantage with a fraudulent ballot definition that yields two votes for one button, using the "endorsement" feature. "Endorsement" is not practiced in New Jersey, but even so an attacker could take advantage of its existence. In the ballot definition in the Results Cartridge, there is a data structure with links from each candidate to the place on the ballot where he appears. The same candidate can occur in several places. In principle, any *one* of these buttons will yield *one* vote for the candidate, but we found a way to construct the links to yield two votes for one button. This attack might be caught if pre-election logic-and-accuracy testing is sufficiently thorough.

A variation of this attack would be to use "endorsement" to link an unmarked button to a candidate. Recall that buttons are marked only by ink printed on the poster-size full-face paper covering all the buttons. The unmarked button could cast several votes for the candidate, whereas the marked button would cast only one. This variation would likely not by caught by Pre-LAT.

[12] Only with respect to handling "Technician Cartridges" (TCs) is there any use at all of cryptographic signatures. Depending on a parameter in the configuration ROM of the AVC Advantage, the voting machine may require a TC to be inserted before allowing certain commands on the Operator Panel. In some settings of this parameter, after insertion of the TC the technican may have to enter a password. Password checking is done using cryptographic signatures, but using an unsound and defeatable cryptographic protocol. In any case, the configuration ROM in New Jersey's AVC Advantage 9.00 machines is set to never require TCs to be used at all. There is no other use of cryptographic signatures in the source code of the AVC Advantage.

[13] Not to mention that this checksum is computed by the program in the ROM, so that replacing the ROM can install a fraudulent ROM-checking program.

# 10 No required canvass of paper printouts

At the close of the polls, the AVC Advantage communicates election results in two ways: via the Results Cartridge that pollworkers remove from the machine, and by printing a paper printout of vote totals from its internal memory. In New Jersey, pollworkers sign this paper before leaving the polling place. Then the paper printouts and the Results Cartridges are brought to a central place for tabulation. The Results Cartridges are plugged into a WinEDS computer for election-night tabulation. Are the paper printouts ever examined?

At trial, the only two county clerks who testified made it clear that they certify election results based on the cartridge data. In these two counties, they do later compare the cartridge data with the paper printouts, but it is not clear that this audit is performed in all counties. Indeed, the Director of the New Jersey Division of Elections testified that he has not instituted a requirement that county clerks compare the results cartridge with paper results-report printouts.[14] In light of the vulnerability of the cartridge to electronic tampering after the close of the polls, it is unwise to trust the cartridge to the exclusion of the paper.

An incident in Camden County provides further evidence that even when the cartridge disagrees with the paper, the cartridge data is used.

On February 5, 2008, one AVC Advantage in Camden County produced a results report with a vote total exceeding the public counter! We examined results-report printouts, precinct-by-precinct election data, Camden's election-day trouble-report logs, a review of the AVC Advantage source code, and performed experiments. We conclude that, as a vote was being recorded, the motherboard lost communication with the results cartridge. The machine detected a fault, indicated a 2-digit error code, and was taken out of service.

Normally the AVC Advantage firmware executes these steps (among others) to record a ballot: (1) add to candidate totals in internal memory; (2) add to candidate totals in cartridge memory; (3) add to public counter in internal memory; (4) add to public counter in cartridge memory. The loss of communication (through a bad electrical connection in the cartridge socket) happened some time in the last several seconds or minutes (after the previous voter's ballot was recorded), but was first detected at the beginning of step 2. Thus, the candidate totals in the internal memory disagreed with the cartridge; and the candidate totals in internal memory disagreed with the public counter in internal memory. As a result, the machine produced a results report of 30 total votes (paper close-of-polls results reports are printed from the internal memory), but the results cartridge (and the public counter on the paper printout) showed only 29 votes.

This failure mode—a cartridge not well seated in its socket—appears not to be unusual in the AVC Advantage. The handwritten Camden County technician logs from the February 2008 Presidential Primary show several references to ill-seated Results Cartridges.

In principle there may be enough information in the 2-digit error code to deduce that the paper results-report (printed at close of polls from the internal memory) will be more accurate than the contents of the Results Cartridge. But this subtlety appears to be lost in practice. In tabulating election results the Camden County Clerk appears to have relied on the cartridge data, not the paper Results Report, even when

- both were available and they disagreed with each other;
- the voting machine in question was known to have exhibited abnormal behavior;
- the cartridge could not be read by the normal WinEDS tabulation software, only by the WinEDS "cartridge utility," and the votes had to be re-entered by hand into the tabulation database after using the utility to read them from the cartridge.[15]

Thus, election officials used only the cartridge even though that actually required more effort than using the paper printouts.

# 11 Programming Issues

The Advantage code is commented and each major routine includes a pseudo-code description of what it does. At the same time, the code is complicated and difficult to follow, and there are sometimes questionable software practices. This is not surprising for a program that has undergone continuous modifications for two decades, and must operate on a tiny and long-obsolete machine.

[14] Robert Giles Testimony, 161:6-9, March 3, 2009.

[15] Letter from Deputy Attorney General Jason Postelnik (July 30, 2008) states that this is what they actually did.

The code suffers from the usual infelicities of software, such as: multiple versions of computations; inconsistent naming conventions; frequent use of literal numeric values ("magic numbers"); subtle linkages among status values; numerous global variables; generic and undescriptive names; names that differ in only a single character; inconsistent declarations for external data objects; and subtle dependencies on datatypes and other properties.

Comments in the code hint that the standards have sometimes cost precious memory space, which can lead to an uncomfortable tradeoff: ignore the rules or adopt other potentially risky techniques to recoup. The use of an older, obsolete version of the C programming language (i.e., function prototypes are written in 1970s style) makes it harder for compilers and other automatic tools to help catch programming errors. Standard library routines for tasks like memory allocation, copying and comparison are written from scratch, presumably for efficiency, but this can lead to confusion and potentially to errors. For example, the order of arguments differs between the standard function `memset` and the Sequoia equivalent `memfill`.

The use of a home-grown operating system and file system, required because the Z80 is so restricted, increases the size of the code base, often leads to complicated programming, and may limit the use of standard tools for analysis of code and data. The amount of assembly language is problematic as well, since it is much harder to work with than is a higher-level language.

The combination of all these problems can lead to complex and fragile code, in which it is hard to find errors by inspection or with mechanical aids, and in which it has been difficult to make changes to adapt to new requirements.

**ITA reports.** Sequoia contracts with an Independent Test Authority ("ITA") to certify that its voting machines meet certain standards. Sequoia then provides the ITA reports to New Jersey, which may or may not read them and rely upon them. Our analysis of the ITA reports, in conjunction with the actual Sequoia Advantage source code, shows that the *source code review* portions of these reports do not ensure the reliability or security of the voting machines.

The AVC Advantage was certified for use in NJ in 1987, before the ITA system existed. The first time the Advantage went through the ITA process was in 1994, when Wyle Laboratories of Huntsville, AL examined it pursuant to FEC 1990 standards.[16]

Wyle performed and reported on hardware functional testing and "shake and bake" testing of robustness; we will not comment on this section of Wyle's report. In addition, Wyle performed what they called "in-depth source code review" of the Advantage firmware: "The source code was reviewed to ensure it followed the recommended programming guidelines as contained in the FEC standards." [20, p. 5 & p. 18]

Wyle's ITA report is inadequate in two ways. First, Sequoia did not provide to Wyle, and therefore Wyle did not examine, several firmware components installed in the Advantage. One of the components that Wyle did not examine was extremely significant, because it was the pathway for the voting-machine virus: the AUTOEXEC.BAT that loads new software into the daughterboard operating system. Wyle did not report on this problem.

Second, the 1990 standards, as they relate to software, are fairly cursory. The State's own expert has concluded that a voting machine certified to the 1990 standards would "not pass the 2002 guidelines."[17] The standards require, and Wyle performed, only a superficial examination of the source code. For a few of the source files in a few of the versions of the software, the Wyle report lists a handful of failures to meet FEC standards. Most of these "Source File Specific Notes" are perfunctory, for instance, citing a function that does not have all the required sections in its header comments, a variable declaration that does not have a comment, or an occasional single-character variable name. Only a handful of comments deal with substantive issues.

In conclusion, the ITA software examination performed on the AVC Advantage was inadequate to prevent errors and security vulnerabilities from slipping through the certification process.

# 12 Seals, seals, and more seals

The defense witnesses presented by the State of New Jersey did not challenge the findings discussed in this paper (and testified to by Appel at trial), that the Sequoia Advantage DREs are susceptible to fraud by ROM replacement. It was clear at the trial that the State seems to have accepted this premise. As the trial approached, starting in September 2008 the State of New Jersey shifted its attention to protecting the physical security of the New Jersey DREs.

In our report delivered to the Court and to the State on September 2, 2008, we cited the scientific literature to explain that physical seals in general are easily defeated [16], and therefore are not the solution. Nonetheless, after

[16] Terwilliger Testimony 21:8-17, March 30, 2009.

[17] Shamos Testimony 178:13-18, March 23, 2009.

Appel demonstrated the replacement of the legitimate ROM chip with a fraudulent ROM chip that stole votes, the State represented to the Court that it would begin using "tamper evident and tamper proof security seals" on the DREs to ensure that hackers did not gain entry to the State's DREs' legitimate ROM chips. The State did not consult any independent security experts before deciding which seals to use, but rather relied solely on representations of vendors that their seals were "tamper proof and tamper evident."

After the delivery of our report, the State installed on the circuit-board cover of its AVC Advantages: an adhesive-tape seal, a "cup seal" (a.k.a. "security screw cap"), and a wire cable seal. We observed these seals in use in the November election; the plaintiffs requested and obtained samples of these seals from the State; and in a report to the Court on December 1, Appel demonstrated how to defeat all three seals—that is, to remove and replace the seal without evidence of tampering [1]. The defeat did not require much sophistication: it used simple tools and techniques.

In December 2008 the State decided to abandon those three defeated seals, and to adopt three new ones: a different cup seal, a plastic and steel padlock seal, and a different adhesive tape seal.[18] During cross-examination at trial in February 2009, Appel demonstrated for the Court, on an AVC Advantage voting machine in the courtroom, how to defeat all three of those seals (and replace a ROM). He used low-cost devices that he made in his basement workshop.

The State's response was to propose to apply superglue (cyanoacrylate) to some of the seals, and to replace some of the defeated seals with other ones represented by the vendors as being foolproof. Plaintiffs then engaged Dr. Roger Johnston of Argonne National Laboratories, one of the world's leading experts in physical security, to evaluate New Jersey's security seals. Johnston examined the State's proposed seals as applied to an AVC Advantage.[19]

Johnston has found that supposedly tamper-evident seals and tape can be defeated [16]. It is easy to manufacture counterfeit seals from components of legitimate seals, because these seals are readily available for sale or as free samples.[20] Johnston demonstrated in the courtroom how to defeat each of the seals that the State had proposed for use.

It does no good to have seals without a rigorous protocol for inspecting them [14]. Testimony by NJ election officials made it clear that New Jersey does not have any such protocol.[21] Such protocol (and the training it requires) is expensive to implement and execute, in proportion to the number of different kinds of seals being inspected. New Jersey's proposed solution uses six different seals. A comprehensive program of training and seal inspection would cost hundreds of thousands of dollars per year for these seals.

The proposed seals are also impractical because they require the use of highly toxic solvents. The seals must be removed to inspect them [15] (a thorough examination of a tamper-evident seal includes the observation of its behavior when removed, e.g. is the adhesive as sticky as it should be?). The seals also need to be removed for routine maintenance of the DRE, such as changing batteries on the motherboard. However, one of the tape seals proposed by the state has an adhesive that leaves a sticky residue behind; this residue must be cleaned off before new seals can be applied. When Johnston was demonstrating this clean-up in the courtroom, using acetone-based solvents, the court reporter had to leave the room because she could not bear the solvents' fumes.

Finally, Johnston found an attack that bypassed all the seals altogether. [4] He removes a segment of the voter panel (with buttons and lights) and replaces it with one that is rigged with a radio remote-control device that causes it to begin swapping one button signal for another (and to swap the corresponding green-X feedback indicators). Thus the signals fed to the Z80 are fraudulent; even though the legitimate ROMs are in place, votes are miscounted. Another radio signal near the close of the polls will switch the voter-panel back to legitimate mode, so that testing of the machine will not catch the fraud.

# 13 Conclusions

The AVC Advantage 9.00 is easily hacked, by the installation of fraudulent firmware. This is done by prying just one ROM chip from its socket and pushing a new one in, or by replacement of the Z80 processor chip. We have demonstrated that replacing a ROM chip takes just 7 minutes, including lock picking, removing the cover, and restoring everything. This vulnerability *cannot be remediated* by means of firmware improvements. Installing physical seals is not a practical way of eliminating this vulnerability.

The fraudulent firmware can steal votes during an election, and the fraud cannot practically be detected. There is no paper audit trail on this machine; all electronic records of the votes are under control of the firmware, which can

[18] Certain aspects of this tape seal are covered by a protective order and we cannot discuss it in detail.

[19] His expert report in this case is filed under seal, and parts of his testimony as well.

[20] For example, www.brookseals.com/images/product/pdfs/Tapes and Labels Brochure.pdf, www.brookseals.com/images/product/pdfs/Plastic Strap Seal Brochure 04202007.pdf, www.americancasting.com/info-cup-seals-01-TOC.asp

[21] Robert Giles Deposition, January 6, 2009; Robert Giles Testimony, March 3, 2009.

manipulate them all simultaneously. Any fraudulent program will always report that it is behaving correctly.

Without even touching a single AVC Advantage, an attacker can install fraudulent firmware into many Advantage machines by viral propagation through audio-ballot cartridges. The virus can steal the votes of blind voters, cause AVC Advantages in targeted precincts to fail to operate; and cause WinEDS software to tally votes inaccurately.

Design flaws in the user interface of the AVC Advantage have the potential to disenfranchise voters by causing votes not to be counted; we were not able the quantify the rate at which this occurs in the field, but we believe this is worthy of future study.

AVC Advantage Results Cartridges can be easily manipulated to change votes, after the polls are closed but before results from different precincts are cumulated together.

The source code examination conducted by the ITA (Wyle Labs) was not rigorous, and was inadequate to detect security vulnerabilities. Programming errors that slip through these processes can miscount votes and permit fraud.

Most of the anomalies noticed by County Clerks in the New Jersey 2008 Presidential Primary were caused by a programming error on the part of Sequoia, and had the effect of disenfranchising voters; one anomaly was caused by a hardware failure during the election.

The AVC Advantage has been produced in many versions. The fact that one version may have been examined for certification does not give grounds for confidence in the security and accuracy of a different version.

The AVC Advantage is vulnerable to fraud through firmware replacement or cartridge manipulation. These vulnerabilities, combined with the lack of an auditable paper trail, make it too insecure for the voters of New Jersey to rely upon. Other means of counting votes exist that have an auditable, voter-verified paper ballot—*precinct-count optical scan* and *DRE with paper-ballot printer*. In our opinion, precinct-count optical scan is more robust, more trusted by technologists, and has the benefit of wide experience in many states.

# References


[1] A. W. Appel. Certification of December 1, 2008; Superior Court of New Jersey, Law Division – Mercer County, Docket No. MER-L-2691-04. http://citp.princeton.edu/voting/advantage/seals/, Dec. 2008.

[2] A. W. Appel. Video demonstration of AVC Advantage vulnerabilities and inaccuracies. http://citp.princeton.edu/advantage, Oct. 2008.

[3] A. W. Appel, M. Ginsburg, H. Hursti, B. W. Kernighan, C. D. Richards, and G. Tan. Insecurities and inaccuracies of the Sequoia AVC Advantage 9.00H DRE voting machine. http://citp.princeton.edu/voting/advantage/, Oct. 2008.

[4] Argonne Vulnerability Assessment Team. Electronic vote tampering. Argonne National Laboratory Video Report APT #64451, May 2009.

[5] D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, R. Kemmerer, W. Robertson, F. Valeur, and G. Vigna. Are your votes really counted? Testing the security of real-world electronic voting systems. In *Proceedings of the ACM/SIGSOFT Int'l Symposium on Software Testing and Analysis (ISSTA'08)*, pages 237–248, July 2008.

[6] M. Blaze, A. Cordero, S. Engle, C. Karlof, N. Sastry, M. Sherr, T. Stegers, and K.-P. Yee. Source code review of the Sequoia voting system. http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf, July 2007.

[7] S. Checkoway, A. J. Feldman, B. Kantor, H. Shacham, J. A. Halderman, and E. W. Felten. Can DREs provide everlasting security? The case of return-oriented programming and the AVC Advantage. In *EVT/WOTE'09: 2009 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections*, Aug. 2009.

[8] Computer Security Group, UC Santa Barbara. Security evaluation of the Sequoia voting system: Public report, July 2007.

[9] A. J. Feldman, J. A. Halderman, and E. W. Felten. Security analysis of the Diebold AccuVote-TS voting machine. In *Proceedings 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*, Aug. 2007.

[10] E. Felten. NJ election day voting machine status. Freedom-to-Tinker blog, http://freedom-to-tinker.com/blog/felten/nj-election-day-voting-machine-status, June 2008.

[11] J. A. Halderman and A. J. Feldman. AVC Advantage: hardware functional specifications. Technical Report TR-816-08, Department of Computer Science, Princeton University, Mar. 2008.

[12] P. S. Herrnson, R. G. Niemi, M. J. Hanmer, B. B. Bederson, F. C. Conrad, and M. W. Traugott. *Voting Technology: The Not-So-Simple Act of Casting a Ballot*. Brookings Institution Press, Washington, DC, 2008.

[13] H. Hursti. Critical security issues with Diebold TSx. http://www.blackboxvoting.org/BBVreportIIunredacted.pdf, May 2006.

[14] R. G. Johnston. The real deal on seals. *Security Management*, 41(93), 1997.

[15] R. G. Johnston. Some comments on choosing seals and on psa label seals. In *7th Security Seals Symposium*, Santa Barbera, Feb. 2006.

[16] R. G. Johnston and A. R. E. Garcia. Vulnerability assessment of security seals. Technical Report LA-UR-96-3672, Los Alamos National Laboratory, 1996.

[17] T. Kohno, A. Stubblefield, A. D. Rubin, and D. S. Wallach. Analysis of an electronic voting system. In *IEEE Symposium on Security and Privacy*, pages 27–42, 2004.

[18] P. McDaniel, K. Butler, W. Enck, H. Hursti, S. McLaughlin, P. Traynor, M. Blaze, A. Aviv, P. Cerny, S. Clark, E. Cronin, G. Shah, M. Sherr, G. Vigna, R. Kemmerer, D. Balzarotti, G. Banks, M. Cova, V. Felmetsger, W. Robertson, F. Valeur, J. L. Hall, and L. Quilter. Everest: Evaluation and validation of election-related equipment, standards and testing. http://www.sos.state.oh.us/sos/upload/everest/00-SecretarysEVERESTExecutiveReport.pdf, 2008.

[19] Sequoia Voting Systems, Inc. AVC Advantage security overview, 2004.

[20] Wyle Laboratories. Test report 48761-03: Change release report of the AVC Advantage DRE voting machine (firmware version 9.00G), Apr. 2004.

[21] Wyle Laboratories. Test report 51884-08: Hardware qualification testing of the Sequoia AVC Advantage DRE voting machine (firmware version 10.1.5), Apr. 2006.