

Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine

Andrew W. Appel*
Princeton University

Maia Ginsburg
Princeton University

Harri Hursti

Brian W. Kernighan
Princeton University

Christopher D. Richards
Princeton University

Gang Tan
Lehigh University

October 17, 2008



Executive Summary. The Sequoia AVC Advantage is a direct-recording electronic (DRE) voting machine used in New Jersey, Pennsylvania, and other states.

I. 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 this “hack” takes just 7 minutes to perform.

The fraudulent firmware can steal votes during an election, just as its criminal designer programs it to do. The fraud cannot practically be detected. There is

*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.

no paper audit trail on this machine; all electronic records of the votes are under control of the firmware, which can manipulate them all simultaneously.

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

III. Design flaws in the user interface of the AVC Advantage disenfranchise voters, or violate voter privacy, by causing votes not to be counted, and by allowing pollworkers to commit fraud.

IV. 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.

V. Sequoia's sloppy software practices can lead to error and insecurity. Wyle's ITA reports are not rigorous, and are inadequate to detect security vulnerabilities. Programming errors that slip through these processes can miscount votes and permit fraud.

VI. Anomalies noticed by County Clerks in the New Jersey 2008 Presidential Primary were caused by two different programming errors on the part of Sequoia, and had the effect of disenfranchising voters.

VII. 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. New Jersey should not use any version of the AVC Advantage that it has not actually examined with the assistance of skilled computer-security experts.

VIII. The AVC Advantage is too insecure to use in New Jersey. New Jersey should immediately implement the 2005 law passed by the Legislature, requiring an individual voter-verified record of each vote cast, by adopting precinct-count optical-scan voting equipment.

NOTE REGARDING REDACTIONS. As paragraph 1.1 and Appendix L explain, this research was conducted pursuant to a Court Order by the Hon. Linda Feinberg of the New Jersey Superior Court. Sequoia Voting Systems filed a motion alleging that certain parts of this report contain protected trade secrets. Plaintiffs dispute Sequoia's contentions. Judge Feinberg has expressed her intention to preserve Plaintiffs' objections until the time of the hearing when she will rule on the merits of Sequoia's claims of trade secret. We are confident that the Court will then permit release of the full, unredacted report. In the interim, the Court encouraged us to release the report with redactions. Paragraphs 19.8, 19.9, 21.3, and 21.5, as well as Appendices B-G, are redacted in this release.

Contents

1	Introduction	8
2	Description of the AVC Advantage	10
I	Fraudulent firmware can steal votes	15
3	Vote-stealing firmware can be installed in the AVC Advantage	16
4	We demonstrate vote-stealing firmware in an AVC Advantage	17
5	Installing fraudulent software into Z80 Program ROM	22
6	Vote-stealing firmware can avoid detection	24
7	The technical knowledge to write vote-stealing programs is basic computer science, widespread in our society	27
8	It is easy in New Jersey to gain unsupervised access to an AVC Advantage, in order to replace ROM chips	28
9	Picking the lock on the AVC Advantage cabinet takes only seconds	30
10	The seals in the AVC Advantage do not provide tamper-evidence	33
11	Reverse engineering allows construction of fraudulent firmware even without access to trade-secret source code	40
12	Fraudulent firmware can be installed inside the Z80 processor chip	46
13	Would anyone go to these lengths?	49
14	There is no means to reliably detect fraudulent firmware in AVC Advantages	50
15	Many insiders have access sufficient to tamper with AVC Advantage voting machines	51
16	The danger of fraudulent firmware is widely recognized by experts	52
17	Conclusion of Part I	55
II	Daughterboard and WinEDS viruses can disenfranchise voters	56
18	The audio-kit daughterboard is a second computer in the AVC Advantage	57
19	One can install fraudulent daughterboard firmware by inserting a cartridge—even unwittingly	58
20	Vote-stealing computer viruses can infect AVC Advantage and WinEDS	61
21	Viruses can propagate through the AVC Advantage	63
22	Viruses can propagate through WinEDS computers	64
23	WinEDS computers have severe security vulnerabilities and are routinely connected to the Internet	67
24	The daughterboard can steal votes or selectively disable voting machines	71
25	No genius required for daughterboard attacks	72

26	The motherboard is vulnerable to malicious daughterboard firmware	73
27	Security vulnerabilities in WinEDS 3.1	74
28	Conclusion of Part II	75

III User-interface inaccuracies and insecurities can disenfranchise voters 77

29	How we vote in New Jersey	77
30	AVC Advantage falsely indicates votes are recorded, when they are not	80
31	Pressing an option switch deactivates the Advantage so that no votes are recorded	82
32	Sound on activation is not an effective signal for voter, pollworkers, or witnesses to determine when votes are cast	83
33	The AVC Advantage’s lack of feedback leads voters to undervote	85
34	Voter can’t tell which primary is activated	86
35	Pollworker can see who the voter votes for	86
36	Can’t undo write-in vote, in violation of FEC guidelines	88
37	Procedures for fleeing voter leave opportunities for violating the privacy or integrity of the ballot	88
38	Conclusion of Part III	89

IV Design errors and programming bugs make the AVC Advantage insecure 90

39	Vote data is not electronically authenticated, making it vulnerable to tampering	90
40	Manipulating Results Cartridges	92
41	Some NJ County Clerks use the less trustworthy source of data in tabulating official election results	94
42	The Advantage can print a paper report from a fraudulent Results Cartridge	95
43	One can confuse the AVC Advantage with a fraudulent ballot definition that yields two votes for one button	96
44	Results Cartridges can be easily converted into other kinds of cartridges and used for fraud	98
45	Early Voting Cartridges permit fraud in States that use them	99
46	Manipulating Consolidation Cartridges	99
47	Wireless access to Results Cartridges opens avenues to manipulation	101
48	Fraudulent intelligent Results Cartridges could steal votes	103
49	Electronically stored “ballot images” compromise privacy of the ballot	104
50	Conclusion of Part IV	106

V	Insufficiently rigorous design and certification processes leave the firmware vulnerable	108
51	Sequoia’s sloppy software practices can lead to error and insecurity	108
52	Wyle Laboratories examines firmware only superficially	110
53	New Jersey officials neglected to read the ITA reports, and thus had no opportunity to notice how their inadequacies	112
54	Sequoia does not keep track of what firmware is installed in its DREs	113
55	Conclusion of Part V	116
VI	Computer-programming errors have actually disenfranchised NJ voters	117
56	Primary election party-affiliation bug disenfranchised voters	117
57	Hardware malfunctions can disenfranchise voters	123
58	Conclusion of Part VI	130
VII	Different versions of the AVC Advantage have different vulnerabilities	131
59	Advantage versions 9.00G and 9.00H have identical vulnerabilities	131
60	The AVC Advantage has changed a great deal in successive versions	132
61	Version 10 AVC Advantage is extremely vulnerable to fraud	134
62	Version 8 AVC Advantage is vulnerable to fraud in some ways that version 9 is not	137
63	Conclusion of Part VII	139
VIII	Conclusions and recommendations	140
64	New Jersey should not continue to use the AVC Advantage 9.00, because it is insecure	140
65	New Jersey should immediately remove the Audio Kits	140
66	There is a way to safely use computers to count votes	141
67	Forms of voter-verified paper ballots	142
68	SUMMARY OF CONCLUSIONS REACHED IN THIS REPORT	145
IX	Appendices	147
A	Memory Devices	147
B	Buffer overrun reading messages from daughterboard	148

C	Technical details of the option-switch bug that disenfranchised some primary voters	149
D	How the ballot images can be unshuffled, thereby violating voter privacy	149
E	The Source Code violates the FEC's software-engineering guidelines for voting-machine firmware	149
F	Installing fraudulent software into Z80 Program RAM	149
G	The security measures in Technician Cartridges are easily defeated	149
H	Printer inaccuracy can change vote totals in results report	150
I	Inadequate indications of undervotes	151
J	Cumbersome procedure for dealing with fleeing voters	153
K	Bug in WinEDS causes ballot programming to be extremely slow	156
L	The Court Order	157

List of Figures

1	The AVC Advantage, from the front.	9
2	AVC Advantage voter panel covered by a printed paper ballot . . .	11
3	Excerpt from Results Report	13
4	Results Cartridge	13
5	Inside the AVC Advantage cabinet, from the rear.	20
6	The motherboard of the AVC Advantage	21
7	Z80 and ROM chips on the motherboard	21
8	ROM reader/programmer	23
9	Unattended voting machines in public places	29
10	Keys for an AVC Advantage	31
11	Picking the lock of an AVC Advantage	32
12	Plastic strap seal	34
13	Plastic-strap seal as installed by Union County	34
14	DO NOT REMOVE sticker	36
15	Results report tape with seal number not filled in	38
16	List of AVC Advantage voting machines sold by Govdeals.com . .	42
17	Description of the AVC Advantage machines sold by Govdeals.com	43
18	Desoldering tool	48
19	Audio ballot cartridge, front and back	58
20	WinEDS computer	65
21	Close-up of voter panel with paper-ballot overlay	78
22	Green X appears by selected candidate	79
23	Cast Vote button	79
24	VOTE RECORDED THANK YOU	80

25	Operator Panel	82
26	Peeking through the slot	87
27	Tiny computer for hacking results cartridges	92
28	Cigarette-pack hacking device	93
29	Hacking a Results Cartridge	93
30	Buttons behind paper ballot on voter panel	97
31	Eye-fi card for wireless access to cartridge	101
32	Digital voice recorder	105
33	Operator Panel	119
34	Results report tape demonstrating option-switch bug	121
35	Three results-report printouts demonstrating inconsistencies	126
36	Inconsistent data from Pennsauken 6, in Camden County.	129
37	Version 10 Results Cartridge	136

1 Introduction

1.1 In 2004 a group of public-interest plaintiffs, represented by Professor Penny Venetis of the Rutgers Law School, sued the State of New Jersey over the State's use of direct-recording electronic (DRE) voting machines. Most of New Jersey's counties had adopted the Sequoia AVC Advantage full-face DRE.

The plaintiffs argued that the use of DRE voting machines is illegal and unconstitutional. Illegal, because they violate New Jersey election laws requiring all votes be counted accurately and that voting machines be thoroughly tested accurate, and reliable. Unconstitutional, because they violate the New Jersey constitution's requirement that all votes count. The plaintiffs argued that one cannot trust a paperless DRE machine to count the vote.

The case was dismissed by the trial court in January 2005. The dismissal was appealed. While the appeal was pending, in the summer of 2005 the New Jersey legislature passed (and the governor signed) a bill requiring that, no later than January 1, 2008, any voting system in New Jersey must produce a voter-verified paper ballot.

In 2006 the Appellate Court reinstated the lawsuit, and instructed the trial judge to monitor the progress of State election officials in meeting the legislature's deadline. In 2008, when the executive branch twice requested that the deadline be extended, the legislature obliged, each time with a six-month extension. Based on an Appellate Division's decision of June 2006, expressing concern that the State would not meet the legislature's January 2008 deadline, the trial judge, the Hon. Linda Feinberg, ordered a trial to proceed on the constitutional issue. The case is *Gusciora et al. v. Corzine et al.*, Docket No. MER-L-2691-04, Superior Court of New Jersey.

Judge Feinberg ordered that the State provide to Plaintiffs' expert witness, for examination, AVC Advantage voting machines complete with their source code. Appendix L shows the terms of the Court Order. The authors of this report examined voting machines and source code during July and August 2008, and delivered our report to the Court on September 2. The Court Order permits us to make our findings available to the public 30 days later.

1.2 Based on our examination of the AVC Advantage voting machine, it is our opinion that:

1. The AVC Advantage can be "hacked" to steal votes by replacing its firmware;
2. The "hack" can be perpetrated by a person with only ordinary training in computer science;



Figure 1: *The AVC Advantage, from the front.*

The large full-face voter panel (white) is visible. In normal use it would be covered by a printed ballot sheet, which is not present in this photo. An array of buttons, 12 across by 42 down, is visible; when in use, these are hidden behind the printed sheet. Below the voter panel is the write-in keyboard. To the left of the write-in keyboard is an LCD display, and to the right (not quite visible) is the Cast Vote button.

This machine is owned by Andrew Appel; the photograph was taken in 2007 at Princeton University.

3. A person can easily gain enough access to voting machines to install this hack;
4. Once installed, the fraudulent firmware is practically impossible to detect;
5. Once installed on a voting machine, the fraudulent firmware can steal votes in election after election without any additional effort;
6. The AVC Advantage is vulnerable to hacks (fraudulent manipulations) in several different ways;
7. Some of these hacks take the form of viruses that can automatically propagate themselves from one voting machine to another;
8. Even when not “hacked,” the AVC Advantage (in its normal state) has design flaws that can cause votes to be lost, or cause voters to be given the wrong primary ballot to vote;
9. Even when not “hacked,” the AVC Advantage in its normal state has design flaws that encourage voter error and pollworker error, and permit fraud.

1.3 **As part of this report, we have prepared a video demonstrating several of these vulnerabilities and inaccuracies. This video will be available at**
<http://citp.princeton.edu/advantage>

2 Description of the AVC Advantage

2.1 The 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.

2.2 In the case of the AVC Advantage, the primary input device used by the voter is a large panel, containing a two-dimensional array of buttons and lights (see Figure 1). This panel is covered by a sheet of paper on which contests and candidate names are printed (see Figure 2). Markings on the paper are placed over the buttons that are to be pressed for the corresponding candidates; the lights on the panel, when lit, are visible shining through the paper. On the side of the machine, an “operator panel” contains additional buttons and an LCD alphanumeric display with two rows of 24 characters each. During an election, before each voter can vote, a

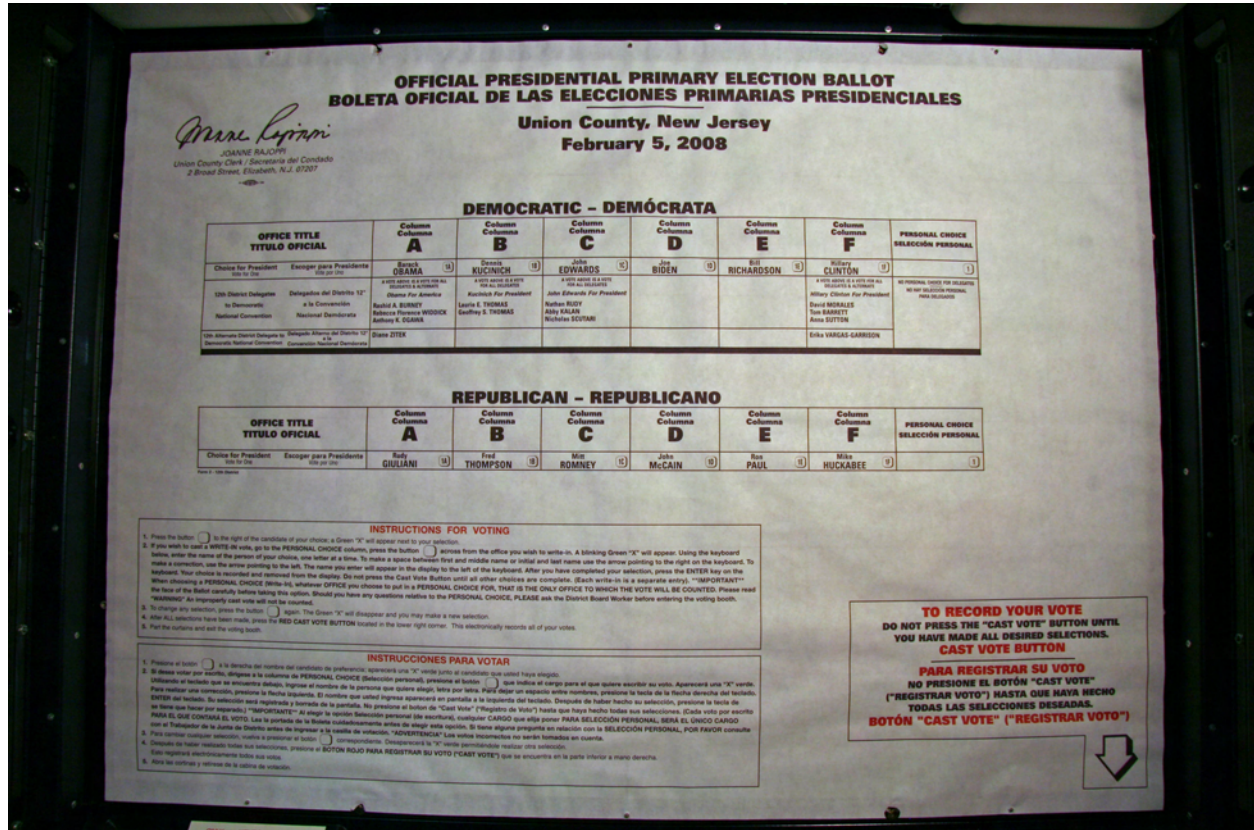


Figure 2: The AVC Advantage voter panel covered by a printed paper listing contests and candidates. This is the 2008 New Jersey Presidential Primary Election, as printed for Union County. The printed paper covers the hundreds of buttons shown in Figure 1.

pollworker must press a button on the operator panel to “activate” the machine to accept votes. As elections are conducted in New Jersey, the pollworker is supposed to do this upon being handed a paper ticket (a “Voting Authority”) by the voter.¹

2.3 The DRE ballot is laid out so that, to the layman, there is an intuitive connection between the candidate’s name (shown on a printed ballot sheet) and the input device (a button behind a sheet of plastic). In the hardware of the voting machine, however, there is no direct connection between the button and the vote counter. Observing the click of a button and accumulating a corresponding candidate total is totally under software control. Since there is no inherent internal connection between the buttons and the totals kept in memory and reported at the end of the election, erroneous or malfeasant software can readily add to the wrong total or make some other error at any time during an election, thereby misrecording votes. **Even though the software produces a so-called “audit trail” of the results, it can always display an “audit trial” consistent with its fraudulent results, and report that it has performed correctly.**

2.4 The AVC Advantage is a paperless DRE voting computer. That is, during the election, while the votes are being cast, there is no paper trail of each vote. While the polls are open, no paper is printed at all by the AVC Advantage. This means that the only record of the votes is in the computer’s memory. Every so-called “audit trail” in the AVC Advantage, including all records of votes, can be modified at the discretion of the firmware. (“Firmware” is software that has been installed semipermanently in a computer.) As we will discuss throughout this report, the firmware can be replaced by fraudulent firmware that abuses this discretion, to steal votes.

2.5 At the close of the polls, the AVC Advantage communicates vote totals to election officials and to the public:

- First, it prints a paper printout of candidate totals.
- Second, it writes these totals (along with a record of the votes cast in each ballot, the “ballot image”) to a Results Cartridge, about the size of a VCR tape, that is then removed from the voting machine.
- Third, it keeps these totals (with the ballot images) in its internal memory. Election workers can extract this information from the AVC Advantage by

¹ The AVC Advantage is available with an option, not used in New Jersey, by which the voter can activate the machine with a smart card obtained when she signs the pollbook.

Candidate	Candidate Totals	Total
***	1-DEM	***
*	US President C7	(1)
D7	Hillary Clinton	86
E7	Barack Obama	45
F7	Bill Richardson	1
G7	John Edwards	1
H7	Dennis Kucinich	0
I7	Joe Biden	0

Figure 3: excerpt of a paper Results Report printout from an AVC Advantage in the 2008 NJ Presidential Primary election



Figure 4: Results Cartridge

using the menu buttons on the Operator Panel: the machine can be instructed to print the internally stored data onto its printer, or copy it to a fresh cartridge.

2.6 If there is fraudulent firmware in the voting machine, the fraud will have already taken place by the time the polls close. The paper printout, the Results Cartridge, and the ballot images, will agree with each other, but they will not be a true record of the actual votes cast. Instead, they will show whatever numbers the designer of the fraudulent computer program chooses. No amount of “auditing” these records will detect any discrepancy.²

2.7 Therefore it is absolutely crucial that the firmware should be correct in all circumstances, and the voting-machine firmware should be immune to tampering. But

² Thus, a DRE cannot be effectively audited. In contrast, an optical-scan voting machine *can* be audited in a way that is truly independent of any computer program that might be suspected of cheating. An optical-scan voting machine works as follows: the voter fills in a paper ballot by using a pencil to fill in circles or ovals next to the name of the candidates she wishes to vote for. Then, (in “precinct-count optical-scan”) she takes the ballot to the optical-scan machine, and feeds the ballot through. The machine counts her votes, then drops her ballot into a ballot box. To audit an optical-scan voting machine, it suffices to recount the paper ballots by hand. This method does not work with DREs that have no paper ballot.

this is not the case.

2.8 **We have found that the Advantage AVC firmware has errors. We have also found that it is easy to replace firmware in the AVC Advantage with fraudulent firmware that can undetectably steal votes and thus change the outcomes of elections. Furthermore, some kinds of fraudulent firmware can automatically virally propagate themselves from one AVC Advantage voting machine to another, without the attacker being physically present. Once fraudulent firmware is installed in the AVC Advantage, it can steal votes in election after election without any additional effort by the attacker.**

2.9 We examined the firmware and hardware of the AVC Advantage models 9.00G and 9.00H, which are used by most counties in New Jersey. The conclusions in this report apply to those “version 9” models. However, based on the evidence available to us, we can also draw certain conclusions about the version 8 AVC Advantage (a few of which are still owned by Mercer County) and the version 10 (which has been proposed, but not yet certified, for use in New Jersey). See Sections 62 and 61 for details.

PART I

FRAUDULENT FIRMWARE CAN STEAL VOTES

- 2.10 The most dangerous insecurities in DRE voting machines, and in the AVC Advantage in particular, permit an attacker to install a fraudulent vote-counting program to control the computer in the voting machine. In this part of the report We describe how we created a fraudulent vote-counting program and installed it into the AVC Advantage. Such programs can be made practically undetectable; we deliberately made our program detectable just to demonstrate it.
- 2.11 We will also explain in detail that,
- The skills and methods we used to create this program are those available to many thousands of computer programmers with a bachelors-degree-equivalent education in computer science.
 - It is easy to gain access to AVC Advantage machines owned by New Jersey counties, in order to tamper with them.
 - The locks and seals on the AVC Advantage do not prevent this tampering.
 - Keeping the “source code” secret cannot prevent this tampering. “Source code” is the human-readable form of a computer program. If it is kept secret, then the attacker just has to take the extra step of “reverse-engineering” the firmware back into source code, as we will explain.
- 2.12 **Definitions.** A computer takes its instructions in the form of “machine language,” which is inconvenient for humans to read and write. Computer programmers write programs in a human-readable formal language called “source code,” which is then translated by “build tools” such as a “compiler” into machine language. A computer program, once it is installed in read-only memory (ROM) inside a device such as a microwave oven or a voting machine, is often called “firmware.” Henceforth we shall refer to “source code” and its corresponding “firmware.”

3 Vote-stealing firmware can be installed in the AVC Advantage

3.1 **Summary: It is not difficult to replace the firmware of the AVC Advantage with fraudulent firmware that steals votes while leaving no detectable evidence.**

3.2 The computer program (firmware) in the AVC Advantage that translates the voters' button-pushes into votes, and counts those votes, can be replaced by fraudulent firmware.

3.3 We found that we could make fraudulent firmware that can cheat in any of the following ways:

1. The program can deliberately misinterpret the voter's button-press, recording a vote for Candidate B even when the voter pushed the button labeled for Candidate A. At the same time, it will light the indicator "X" by the candidate the voter selected, giving no hint that the program is cheating.
2. The program can count votes accurately until late in the election day, and then simply modify the record of votes cast (ballot images and candidate totals) in the voting machine's memories before the polls close.
3. The program can violate the privacy of the ballot by storing a record of how each voter actually voted, in sequential order.

In the video that accompanies this report, we demonstrate a program that uses method #2. But it is straightforward to use any combination of these methods.

3.4 In the next few sections of this report, we will explain

- How a criminal might design a fraudulent computer program to steal elections.
- How to physically replace the legitimate firmware in the AVC Advantage with fraudulent firmware.
- How it is impossible to detect the fraudulent firmware during or after the election. A simple, relatively low-tech fraud could not be detected by any means now in use in New Jersey; more sophisticated frauds, which are straightforwardly achievable today, could not be detected by any means that it is practical for New Jersey to employ in the foreseeable future.

4 We demonstrate vote-stealing firmware in an AVC Advantage

- 4.1 We built a vote-stealing program, and “burned” it into a ROM chip that we installed into an AVC Advantage. This program moves votes from one candidate’s total to another, while taking care not to change the total number of votes cast.
- 4.2 The AVC Advantage has a “pre-election logic-and-accuracy testing” (Pre-LAT) mode, in which election officials can “debug” 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. Our vote-stealing firmware does nothing untoward in Pre-LAT or Post-LAT mode.
- 4.3 An election official might think of testing the voting machine in Official Election mode to see if it will cheat. As we will explain later, a real vote-stealing program would have several means to avoid detection.³ Our demonstration fraud illustrates just one of these, which is to wait until a large number of votes have been cast. In official election mode, for every voter before or after the n th voter, the program does nothing. It waits until the 20th voter casts a vote (a real fraud would wait until the 150th voter, to better distinguish a real election from a test). At that time the fraudulent program walks through the list saved ballot images in the AVC Advantage’s memory. On half the ballots it changes a vote from one candidate to another, and it adjusts the candidate totals accordingly. It writes its fraudulent ballot images and candidate totals both to the internal memory and to the Results Cartridge.
- 4.4 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.
- 4.5 We could build a practically undetectable vote-stealing program—so undetectable that we could not demonstrate it, because it would steal votes only in real elections,

³ As we will explain in Section 6, a well-designed vote-stealing program carefully examines its environment to ensure that it is in a real election, not in a test. It must be a real election day (dates of which are known decades in advance); the time/date in the machine must not have been fiddled with recently; the polls must stay open for at least 12 hours; at least 150 votes must have been cast; and so on. If we built such a program and installed it in the AVC Advantage, it would not serve the purpose of showing how easy it is to steal votes, because observers would never catch it red-handed. Any demonstration we made for the Court, of such a program, would not show it stealing votes.

not in demonstrations. Therefore, for purposes of demonstration we purposely built a *less* sophisticated vote-stealing program. Our exploit is intentionally simple so it can be explained and intentionally unsubtle in its attack so the theft is visible. A real vote-stealing program would be more clever and would be practically undetectable.

4.6 A real vote-stealing program, which will stay installed in the machine for election after election, might steal votes only in general elections. It would not need to be programmed with knowledge of a particular ballot design, or the names of particular candidates. Instead, it would steal from generic Republican candidates for particular offices, or from Democratic candidates, depending on the goals of the attacker.

4.7 A real vote-stealing program might also steal votes in primary elections. If one party's political machine wished to make sure that primary challengers never win, in any election in the future, then it could install firmware that steals votes in favor of the candidate in the first column (where party-endorsed candidates are listed).

4.8 **The context of our demonstration.** We demonstrate a vote-stealing program on the AVC Advantage machines provided to us by Union County, NJ under the Court's order. We show that the voting machines are hackable in exactly the state in which Union County had configured them for an election. The voting machines are configured for the Presidential Primary of February 5, 2008. That is, the voter panel is covered by a poster-size printed ballot paper listing the candidates in that election, and the Results Cartridge is programmed with a ballot definition for listing candidates.

4.9 We designed our vote-stealing program to match this particular, artificial scenario. It does not steal from a generic Republican in favor of a generic Democrat (or vice versa) because that cannot happen in a primary election. It does not steal in favor of a generic party-endorsed candidate, because there were none in this presidential primary.

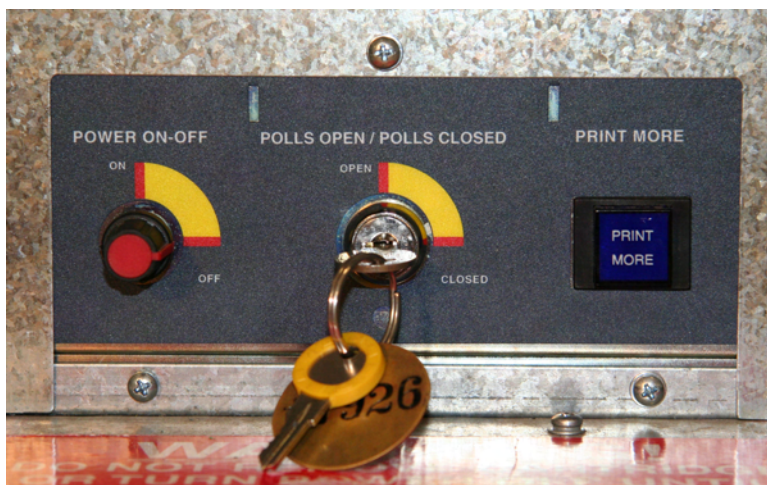
4.10 To demonstrate a real vote-stealing program in practice on Union County's machines as they were set up for this election, we decided to steal votes from Bill Richardson and gives them to Dennis Kucinich. We have the highest respect for the integrity of Mr. Kucinich, and we hope that he will not take offense, but we had to choose someone whose name was on the ballot. Our program waits until at least 20 votes are cast, then takes half of Mr. Richardson's votes and gives them to

Mr. Kucinich.

- 4.11 **We ran a fake election in which 16 votes were cast for Mr. Richardson and then 4 votes for Mr. Kucinich. 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 results tape and the audit trail tape both show this fraudulent result. There is no inconsistency in the results output from the machine; they all agree: Richardson 8, Kucinich 12.**
- 4.12 We made our program simple and specific, just to clearly and unambiguously demonstrate how the AVC Advantage is vulnerable to fraud. In section 6 we will explain how it is a matter of simple computer programming to make the fraudulent firmware do much more sophisticated thefts that are not specific to a single election.
- 4.13 The AVC Advantage program fits in three ROM (read-only memory) chips of 128 KB (kilobytes) each. Our vote-stealing program is a modification of just one of these ROMs, which makes the physical installation simpler for the attacker. we added our cheating code to the function that implements “add 1 to the public counter,” because this function was most convenient: it happens to reside on a ROM chip that has empty space, and the function executes once for each voter.
- 4.14 **Our vote-stealing program is 122 lines of source code. It translates into less than 600 bytes of firmware. It took two of us about two days to write.**



Figure 5: Inside the AVC Advantage cabinet, from the rear. Visible is the main circuit-board cover (sheet-metal, approximately 17x14 inches), through which protrude two ports, currently labeled “Results” and “Auxiliary.” In this picture, the Results port contains a Results Cartridge and the Auxiliary port is empty. To the right of these ports is a smaller metal box containing the audio-kit daughterboard, with a cable leading to a black nylon bag (at lower right) containing more audio-voting accessories. At center left are the power on-off knob, the polls open/closed keyswitch, and the “Print More” button. At upper right is a printer used for printing results reports. This machine is owned by Union County, NJ.



Close-up of the on/off knob, polls open/closed keyswitch, and Print More button.

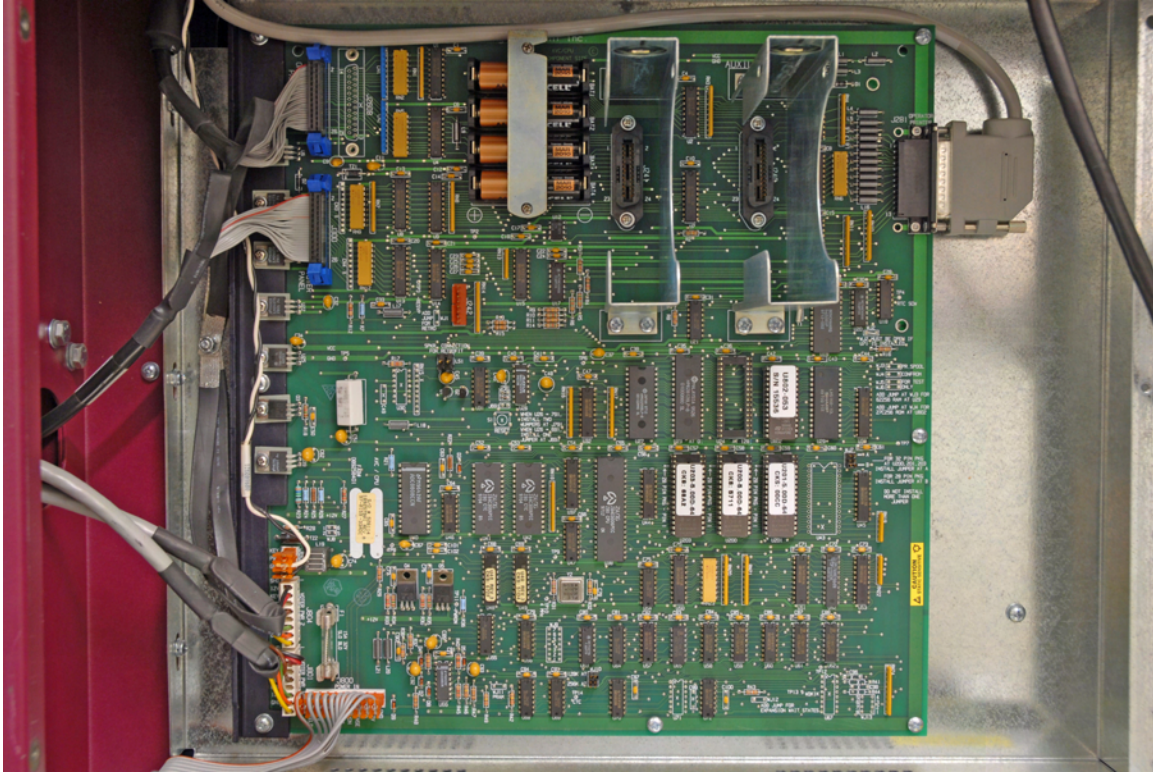


Figure 6: The motherboard of the AVC Advantage The Z80 is the largest chip, at center right. The ROMs have white labels. This machine is one that Appel purchased in 2007; the motherboards of the machines we examined from Union County, NJ are similar.

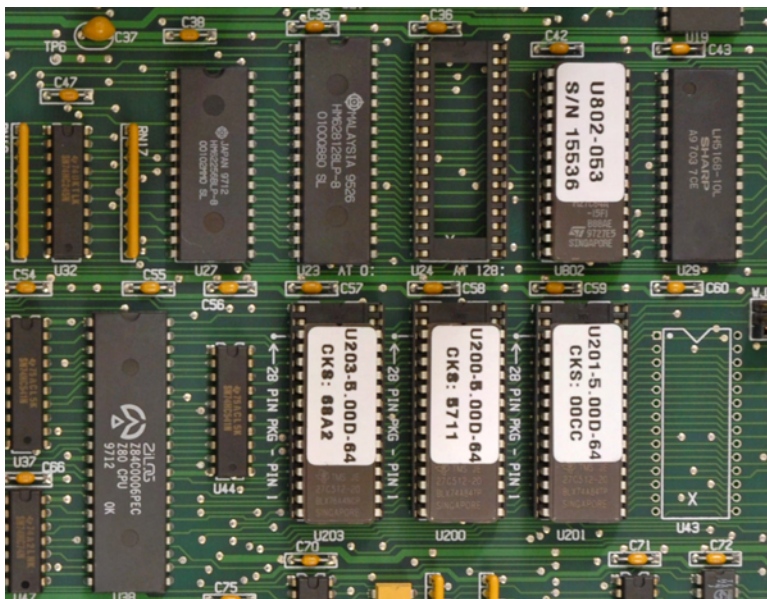
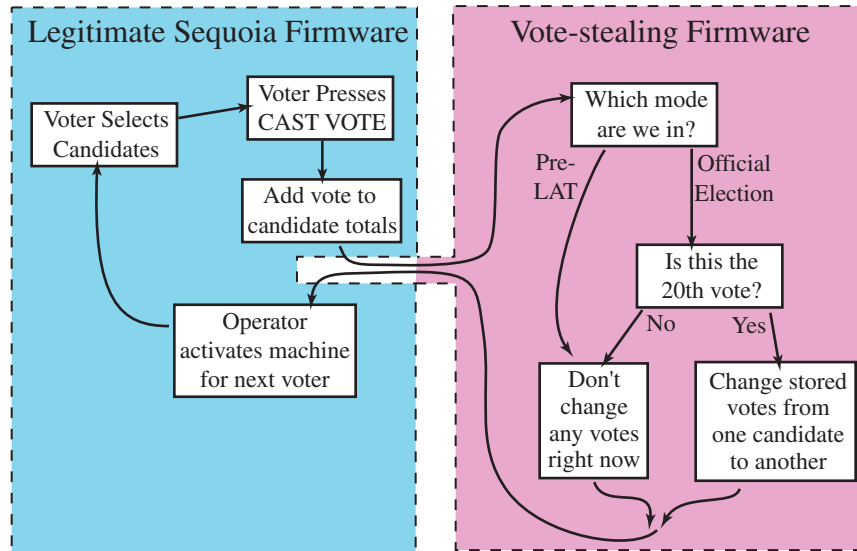


Figure 7: Z80 and ROM chips on the motherboard. The Z80 is the large chip at lower left. The ROMs have white labels.



4.15 This flowchart illustrates the logic of our vote-stealing firmware. The vote-stealing program is a small addition to Sequoia’s factory-installed firmware (of which we have illustrated only a tiny portion here).

5 Installing fraudulent software into Z80 Program ROM

5.1 **Summary:** With just a few minutes of unsupervised access to an AVC Advantage, one can easily replace the motherboard firmware to steal votes and change election results. We have demonstrated this replacement on video that accompanies this report.

5.2 The “motherboard” of the AVC Advantage is a large circuit board containing a Z80 computer and many other chips that serve as memory, input-output devices, and so on. The computer-program firmware that controls how votes are interpreted and added resides in ROM chips on the motherboard. We will refer to these as “Z80 Program ROM.”

5.3 To prepare a ROM chip containing our vote-stealing firmware, We bought some “erasable programmable ROM” (EPROM) chips⁴ for \$3.87 each.

⁴UV-erasable EPROM, 27C1001, from Allied Electronics, www.alliedelec.com

- 5.4 The device for writing firmware into the ROM chips costs \$150;⁵ We borrowed an old one. An attacker would use this device to prepare fraudulent ROM chips in advance of gaining access to the voting machine.



Figure 8: ROM reader/programmer;
cost \$150;
approx. 3 inches by 2 inches

- 5.5 To install fraudulent software into the Z80 Program ROM, one removes the ROM chips from the motherboard and inserts replacement ROM chips. Since our vote-stealing program is such a small modification to the firmware, we had to replace just one ROM chip on the AVC Advantage motherboard.

- 5.6 On the AVC Advantage motherboard, the ROMs are installed in sockets—not soldered directly to the circuit board. Although this is a standard industrial practice for computer equipment, it is not a wise practice for voting machines. Computer equipment has most chips soldered directly to the circuit board, but ROM chips are often placed in sockets so that they can be easily removed and replaced with new ROMs containing new (upgraded) firmware. However, for voting computers this poses a grave security risk. To access the ROM sockets in order to replace the ROM chips, we removed the main circuit-board cover. This is a rectangle of sheet metal, approximately 17x14 inches, held in place by 10 sheet-metal screws. Then we pried the ROM from its sockets using a screwdriver, and pressed the replacement ROM into place.

- 5.7 A flexible plastic-strap seal is sometimes installed, that is supposed to provide tamper-evidence if the circuit-board cover is removed. Section 10 describes how such seals are easily defeated, how we were able to defeat this seal, and how at

⁵Batronix USB EPROM Programmer, \$149.50, <http://www.progshop.com/shop/programmer/usb-chip-programmer/index.html>

many times the seals are not even installed at all.

5.8 The AVC Advantage firmware attempts to detect replacement of the Z80 Program ROM by computing a “checksum,” a kind of digital fingerprint of the contents of ROM. Then the firmware in ROM compares the checksum against what it should be. That is, it attempts to detect the replacement of itself! This is not an effective security measure, because once the firmware is replaced, obviously it is no longer there to perform this detection. Any new, fraudulent ROM can simply omit this check.⁶

5.9 In fact, we found that the design of the AVC Advantage’s ROM-checksum algorithm is so weak and insecure⁷ that we were easily able to construct a fraudulent firmware with a checksum that matched the legitimate one.

5.10 The AVC Advantage firmware attempts to log events such as “different Program ROM installed” in the its Maintenance Log. However,

1. This logging is done by firmware in the Program ROM itself, and a fraudulent ROM can avoid logging anything it doesn’t want to; and
2. A fraudulent program ROM can modify the Maintenance Log in any way it wants to, since the Maintenance Log is kept in writable memory.

6 Vote-stealing firmware can avoid detection

6.1 **Summary: It is well known how to design a vote-stealing program so that it can avoid detection: the program takes care not to cheat in any circumstance where someone can compare the actual votes cast with the program’s computed results.**

6.2 Fraudulent voting-machine firmware can be easily written to take all of the following steps to avoid detection.

6.3

- It would take care to maintain a correct Public Counter. This is a counter of how many voters cast votes on the machine. Election workers and pollwatchers representing the parties can see how many voters use the machine during

⁶ In addition, the firmware in the Z80 Program ROM computes a checksum of itself and writes this to the Maintenance Log, where it can be printed. This is not an effective security measure against fraudulent ROM replacement, because fraudulent firmware would simply write the known “good” checksum into the Maintenance Log.

⁷Function “checksum” in asm/checksum.asm is simply the sum of the 8-bit bytes, taken modulo 2^{16} ; even 50 years ago this algorithm was known to be insecure.

the day, and there are Voting Authority tickets that tabulate this number, so if the program gets this number wrong, it will be “caught.”

- 6.4 • It would take care that the candidate totals are consistent with the Public Counter, that is, equal to or slightly less. In real elections, voters sometimes do not vote every contest.
- 6.5 • The fraudulent firmware must take care not to steal too many votes. For example, if some machines in a heavily Republican district vote Democratic by a 90%–10% margin, suspicions will be raised. Experts in the field of election auditing usually assume that 20% of the votes can be stolen without raising suspicions.⁸
- 6.6 • The fraudulent firmware would take care not to cheat in “pre-election logic-and-accuracy testing” (Pre-LAT) mode. Pre-LAT is *not* an examination of the firmware itself—it is a “mock election” in which election workers cast a few votes on the voting machine, and make sure that the totals come out right. The voting machine’s computer program (firmware) knows exactly what mode it is in. On the AVC Advantage, it is a design feature that the program makes sure that election workers perform Pre-LAT testing before switching to “official election” mode. It is easy to make the fraudulent firmware take care not to cheat in Pre-LAT mode, where inaccuracy would be detected.
- 6.7 • The fraudulent firmware would defend itself against pre-election testing in “official election” mode. (We have seen no evidence at all that this kind of testing is done in New Jersey, but the criminal would be prudent nonetheless.) In this kind of testing, election workers set the date of the machine forward to election day, and test the machine as if it were a real election. However, changing the date of the machine is done under control of the firmware itself. Thus, it can examine the maintenance log for date-change commands entered through the Operator Panel, and try to estimate what the real date is. The fraudulent firmware might choose not to cheat if the date has recently been changed.
- 6.8 • The fraudulent firmware can to defend itself against “parallel testing.” This is a practice for attempting to detect fraudulent DREs. It is not used in New Jersey, as far as we know. In parallel testing, election officials wait until the morning of election day itself, and then randomly select some voting

⁸ “Random Auditing of E-Voting Systems: How Much is Enough,” by Howard Stanislevic, www.VoteTrustUSA.org, August 9, 2006.

machines. These machines are taken out of service, and are not used in the actual election. Instead, people cast votes on the machine as if it were a real election, trying to “fool” the election-stealing firmware, in case any were installed. Then the results are compared with the actual votes cast.

6.9 Cleverly designed fraudulent firmware can detect differences in the patterns of use between testers and real voters. The simplest way is to wait until at least 150 votes have been cast, spread over several hours, before altering any votes in memory; that way, parallel testing must be very thorough to succeed.⁹

6.10 • Some voting machines, including the AVC Advantage, have firmware that computes and reports a “digital fingerprint” of itself, a several-digit number that summarizes the contents of the firmware. The fraudulent firmware can simply lie about itself: the author of the fraudulent program knows what the right number is (because the legitimate voting machines print it out when asked), and the author writes the program to just print that number.

6.11 While this might seem a long list of criteria for an effective vote-stealing program, it is actually quite straightforward computer programming to implement a program that works this way. It would take a trained computer programmer a month to write this program.

6.12 **General-purpose vote-stealing firmware.** A fraudulent vote-stealing program, installed just once in a voting machine, can steal votes in election after election without the criminal ever needing to give it further instructions.

6.13 • **In general elections** the fraudulent program can easily tell which are the Republican candidates and which are the Democrats, since the ballot definition in the Results Cartridge contains this information. Therefore, once the fraudulent firmware is installed, it needs no further instructions: it will always cheat in favor of the attacker’s party.

6.14 • **In primary elections with organization-endorsed candidates**, like most primary elections in New Jersey, the ballot layout makes it clear who is the endorsed candidate. A fraudulent firmware can be installed to cheat in favor of endorsed candidates, for example.

⁹ In addition, the firmware has access to the timing of button-pushes down to a fraction of a second, and a tester who casts a hundred votes will settle into a very different pattern than 150 different real voters do. These patterns can probably be effectively distinguished by standard methods of Computer Science, such as the statistical techniques called “Machine Learning.”

- 6.15
 - **For other kinds of elections**, the attacker may not know *today* how he wants the machine to cheat in a future election. Consider, for example, the 2016 Presidential Primary or the 2016 Princeton Regional School Board election. It is difficult to imagine now what candidates will be on the ballot. An attacker with access to the voting machines now can install firmware that steals votes in many elections between now and 2016. But he can easily leave himself the flexibility to steal votes in those elections too. He can do so by any of the following means:
- 6.16
 - Design the vote-stealing program steal votes away from candidates with Hispanic-looking names, or whose first names look like women’s names.
- 6.17
 - Design the vote-stealing program so that one could communicate to it the name of the candidate to favor. For example, one could say, “steal in favor of the second candidate voted for in the Pre-LAT.” Then a corrupt election worker could arrange, in the Pre-LAT, to vote for that candidate on the second test ballot. The technical term for this kind of under-the-table communication is a “secret knock.”
- 6.18
 - One can make secret knocks that do not require a corrupt election worker. For example, a corrupt voter could signal to the corrupt firmware to cheat in favor of Candidate X as follows: first select and deselect each candidate in the race (by pushing the button twice for each candidate), then vote for Candidate X. It is easy to design a computer program that can recognize this sequence. The corrupt voter can vote at any time of day, since the firmware can do the actual transfer of votes just before the polls close.
- 6.19
 - Finally, of course, one can simply install (on many machines used in a particular election) fraudulent firmware that is specific to that election. Then the attacker does not get the benefit of “hack the machine once and for all,” but the single election is effectively stolen.

7 The technical knowledge to write vote-stealing programs is basic computer science, widespread in our society

- 7.1 Technical knowledge and skills are needed to design, create, and install fraudulent vote-stealing computer firmware into voting machines. However, this knowledge and these skills are widespread. The fundamental skill needed is a basic knowledge of computer programming, and a basic knowledge of computer organization, at the level taught in the core of the undergraduate curriculum of most

colleges and universities that offer a degree in Computer Science or in Computer Engineering. In *each year* from 1983 to 2004, at least 25,000 bachelor's degrees in Computer Science were awarded in the United States alone.¹⁰ Thus there is a pool of over half a million people who have the kind of technical skills needed to perform the hack that we performed.

- 7.2 The technical skills to create fraudulent voting-machine firmware are similar in many ways to the skills needed to create computer viruses. There are tens of thousands of known computer viruses.¹¹

8 It is easy in New Jersey to gain unsupervised access to an AVC Advantage, in order to replace ROM chips

- 8.1 **Summary: Voting machines are left unattended in public places for several days before and after each election. It's not difficult to gain ten minutes of unsupervised access to the voting machine.**

- 8.2 The Sequoia AVC Advantage weighs about 250 pounds. Therefore the machines are delivered several days before the election, and removed several days after the election.¹²

- 8.3 Polling places are sites to which the public generally has access: elementary schools, colleges, firehouses, churches, and so on. At these places in New Jersey, AVC Advantage voting machines are left unsupervised for days on end.

- 8.4 On Tuesday, June 3, 2008, the day of the New Jersey (nonpresidential) primary election, Professor Edward W. Felten wrote,

[V]oting machines were left unguarded all over Princeton, as usual. On Sunday and Monday evenings, I visited five polling places in Princeton and found unguarded voting machines in all of them—18 machines in all. The machines were sitting in school cafeteria/gyms, entry hallways, and even in a loading dock area. In no case were there any locks or barriers stopping people from entering and walking right

¹⁰Science and Engineering Degrees: 1966–2004. Maurya M. Green, project officer, Division of Science Resources Statistics, National Science Foundation, Arlington, VA, January 2007.

¹¹“A-Z Listing of Threats and Risks,” Symantec, Inc.

http://www.symantec.com/business/security_response/threatexplorer/azlisting.jsp

¹² See certifications of approximately 15 county officials filed with the court by Defendants in October 2004.

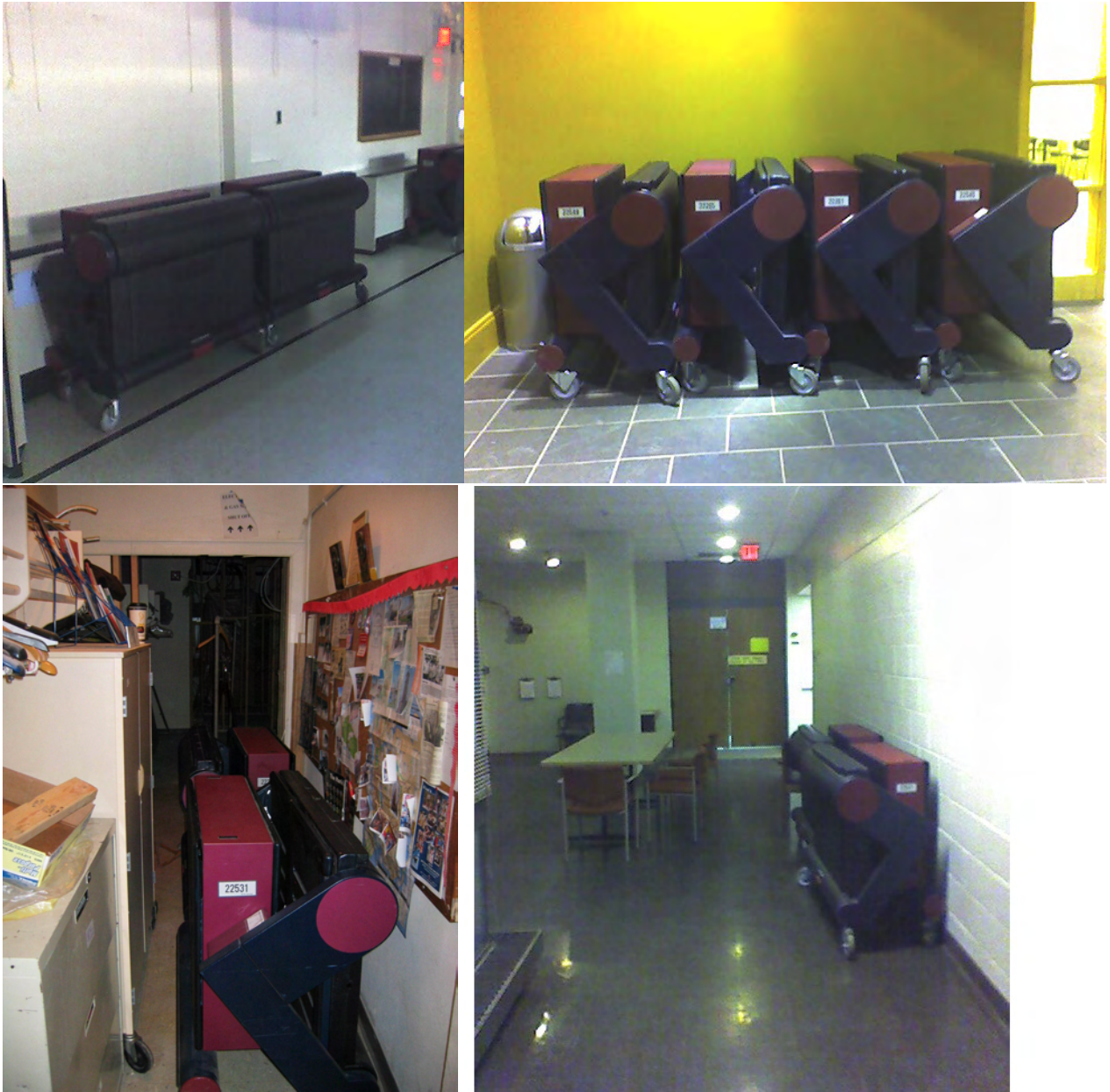


Figure 9: *Unattended voting machines at four different polling places in Princeton, NJ on June 1 and June 2, 2008, before the June 3 primary election. Photos by Edward Felten.*

up to the machines. In no case did I see any other people. (This was in the evening, roughly between 8:00 and 9:00 PM). There were even handy signs posted on the street pointing the way to the polling place, showing which door to enter, and so on.¹³

Figure 9 shows some photographs that Professor Felten took of these unattended AVC Advantage machines.

8.5 On Saturday, November 4, 2006, three days in advance of a Tuesday Federal election, Professor Felten reported seeing unattended voting machines at a polling place in Princeton, NJ, with no other people in sight.

8.6 When a voting machine is left unattended in a public place *before* an election, it's obvious that an attacker could tamper with the machine before an election. But even when the voting machine is left unattended *after* an election, this is an opportunity to install fraudulent firmware to cheat in the *next* election (and in every subsequent election).

8.7 Between elections the voting machines are kept in county warehouses, where any number of employees have access to them. Voting machines are delivered to the polling sites, and picked up from polling sites, typically by private trucking companies.¹⁴

9 Picking the lock on the AVC Advantage cabinet takes only seconds

9.1 **Summary: The lock on the cabinet of the AVC Advantage is simple, cheap, and easy to pick. This is significant, because many of the attacks we describe require access to the inside of the cabinet.**

9.2 The cabinet of the AVC Advantage has a door at the rear, equipped with a key-lock. The door must be opened to access any of the following devices inside the cabinet:

1. the ports for inserting Results Cartridges (and other types of cartridges);
2. the printer (that prints pre-election and post-election reports);

¹³ "NJ Election Day: Voting Machine Status," by Ed Felten, freedom-to-tinker.com, June 3, 2008.

¹⁴ See footnote 12 on page 28.

3. the hook where the Operator Panel is stored while not in use;
4. the nylon bag containing the Audio Voting equipment;
5. the Emergency Ballot Box;
6. the computer circuit boards (which are additionally covered by a sheet-metal circuit-board cover).

9.3 At the polling place, election-board workers unlock this door in the morning to remove the Operator Panel and print a zero tape, then (normally) lock the door before voters arrive. During the election, they may need to unlock the door to access audio-voting equipment, which can only be accessed with the door open. At the end of the election day, the board workers open the door again to close the polls, print a results report, and remove the Results Cartridge.

9.4 Inside this locked door, the switch labeled “Polls open/closed” is operated by a different key. That is, the election-board workers are given a keyring containing the door key, the polls-open/closed key, and a metal tag with the serial number of the machine.¹⁵

9.5 AVC Advantage voting machines are delivered to polling places several days before the election (see Section 8), without their keys, and removed from the polling places several days after the election.



Figure 10: *Door key (left) and polls open/closed key (right) for an AVC Advantage*

9.6 “By the day preceding the Election, upon notification of the Municipal Clerk, one election clerk [i.e., election-board worker] shall obtain from the Clerk’s office,

¹⁵“Official Instructions for Members of the District Boards of Elections, Presidential Primary Election – February 5, 2008.” Mercer County. Bates number MERCER 004642 in Gusciora et al. v. Corzine et al.

the registration binders and all the other election supplies to be delivered to the Polls for the Election.”¹⁶ These election supplies include the keys to the voting machines. Thus, the keys arrive with the election-board workers, on the morning of the election, and are removed after the polls close; they are sent back to the county election warehouse after the close of the polls.

9.7 The door lock is described by its manufacturer (Illinois Lock Co.) as “Economical die cast cam locks for high quantity applications;” it is a cheap 5-tumbler lock which does not provide very much security. We were easily able to get the key duplicated at the local hardware store, for \$1.69 plus tax.

9.8 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. In July 2008, he received a few minutes of advice about lock-pick tools and instruction on their use from a Princeton University graduate student. Lock-picking tools are easily available on the Internet. He bought a set of lock-picking tools for less than \$40, no questions asked (except credit-card number, of course).

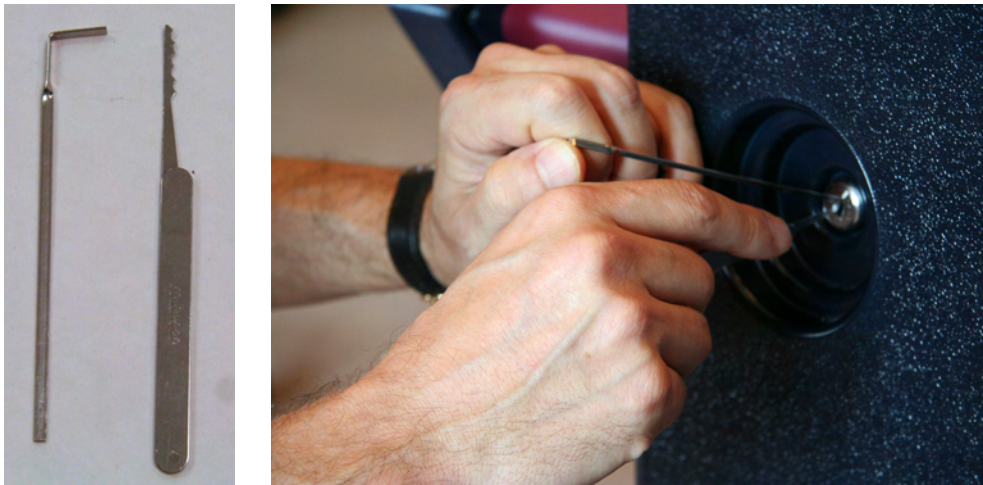


Figure 11: *Picking the lock of an AVC Advantage*

9.9 Two days later, Appel could pick the door lock of an AVC Advantage voting machine in an average of 13.2 seconds (measured over 10 trials on two different

¹⁶ “Official Instructions for the District Board of Elections,” Middlesex County Board of Elections, Revised Jan 2008. Bates Number *Middlesex 1048*, page 3.

voting machines).

9.10 The key switch for polls-open/closed is very similar, and also easy to pick. However, picking this lock is not necessary for any of the firmware-replacement attacks that we designed.

9.11 The AVC Advantage would not be made resistant to fraud simply by using better locks, for example, a “pin tumbler” lock instead of the cheap “wafer tumbler” lock that Sequoia uses. Professor Matt Blaze of the University of Pennsylvania is an expert in computer security (and one of the Plaintiffs’ experts in this case). Since computers are often embedded into physical devices (such as voting machines and ATMs) with physical locks, Professor Blaze has spent considerable time on the academic study of the security of locks. In 2004, he taught a class on security at the University of Pennsylvania; in one of the laboratory sessions for this course, he taught the students how to pick pin-tumbler locks (which are of substantially better quality than the locks used on the AVC Advantage). In the 3-hour laboratory session, every one of the half-dozen students in the class was successful in learning how to pick a pin-tumbler lock.

9.12 Aside from the fact that the locks can be picked, there is the fact that many people have access to the keys. Until a few days before the election, they are in the Municipal Clerk’s office; one or more days before the election, the keys are transferred to the custody of *one* election-board worker.¹⁷ Anywhere in this chain of custody, someone can make a copy of the key, or someone can use the key to tamper with the voting machine.

9.13 **Therefore the locks on the AVC Advantage do not prevent tampering with the internals of the machine.**

10 The seals in the AVC Advantage do not provide tamper-evidence

10.1 **Summary: The supposedly tamper-evident seals in the AVC Advantage provide no significant protection.**

10.2 In its promotional literature, Sequoia claims that the AVC Advantage design permits the installation of numbered security seals that are supposed to provide

¹⁷See footnote 16

tamper-evidence in case the ROMs are replaced.¹⁸ These flexible plastic-strap seals give no real protection, as we explain in this section.



Figure 12: *Plastic strap seal*

10.3 The AVC Advantage machines are prepared for each election by installing a Results Cartridge containing a ballot definition. This is done by employees of the Superintendent of Elections (or equivalent) before the machines are transported to the polling places. After the cartridges are inserted, a plastic strap seal is inserted, passing through the cartridge and through a slot in the AVC Advantage sheet metal. Each seal is stamped with a serial number.

10.4 Figure 13 shows an AVC Advantage with a green plastic seal, installed by Union County, in the Results port. Union County provided two AVC Advantage machines for examination; one of them had this plastic seal in place; the other had no seal.

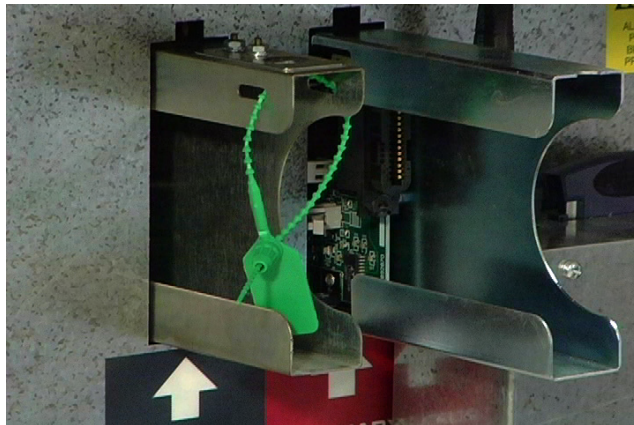


Figure 13: *A green plastic-strap seal in the Results Port of an AVC Advantage, exactly as installed there by Union County, New Jersey. This seal is supposed to prevent removing the circuit-board cover without breaking the seal, but in fact it is possible to remove the circuit-board cover without removing the seal.*

10.5 At the close of the election day, the election workers at the polling place remove the cartridge, which now contains records of the votes cast. To do this they cut the

¹⁸“AVC Advantage Security Overview,” Sequoia Voting Systems, Inc., 2004.

seal. They *are supposed to* record the serial number of the seal in a space provided on the “results report” printout that came from the voting machine, before they sign this document. Then they are supposed to place the cartridge, the results report, and the serial-numbered seal into a bag. They are supposed to seal this bag with yet another serial-numbered tamper-evident seal, and transport the bag immediately to county election officials typically several miles away. Then the bag is opened, the Results Cartridge is removed from the bag and inserted into a computer so that election results from that voting machine can be extracted and accumulated with other precincts.

10.6 For a system of tamper-evident seals to provide effective protection, the seals must be consistently installed, they must be truly tamper-evident, and they must be consistently inspected. With respect to the Sequoia AVC Advantage, this means that *all five* of the following would have to be true. But in fact, *not a single one* of these is true in practice, as we will explain.

1. The seals would have to be routinely in place at all times when an attacker might wish to access the Z80 Program ROM; but they are not.
2. The cartridge should not be removable without leaving evidence of tampering with the seal; but plastic seals can be quickly defeated, as we will explain.
3. The panel covering the main circuit board should not be removable without removing the seal; but in fact it is removable without disturbing the seal.
4. If a seal with a *different* serial number is substituted, written records would have to reliably catch this substitution; but we have found major gaps in these records in New Jersey.
5. Identical replacement seals (with duplicate serial numbers) should not exist; but the evidence shows that no serious attempt is made to avoid duplication.

10.7 Now we will explain in detail why not a single one of these necessary conditions (for tamper evidence) actually holds in practice, in New Jersey.

10.8 **Circuit-board cover seal does not exist.** In addition, Sequoia claims that a numbered seal can be installed on the circuit-board cover, but in practice no such seals are actually installed.¹⁹ This seal is supposed to be installed through the hole labeled “DO NOT REMOVE → ” in on the circuit-board cover.

¹⁹“AVC Advantage Security Overview,” Sequoia Voting Systems, Inc., 2004.



Figure 14: Close-up from Figure 5. The hole labeled *DO NOT REMOVE* contains no seal.

In actual practice, the circuit-board cover seal is not installed. On all five machines bought from Buncombe County (North Carolina), and on both of the machines we examined from Union County (New Jersey), the circuit-board cover seal is not in place, notwithstanding the sticker labeled “DO NOT REMOVE.” We believe this is because the four AA batteries on the main circuit board must be replaced periodically. To do this, a maintenance technician (typically, someone employed by the county Superintendent of Elections or equivalent) must remove the circuit-board cover. The instructions in the maintenance manual²⁰ for replacing the batteries *make no mention* of reinstalling a seal on the circuit-board cover.

10.9

Sloppy logging of seals. In New Jersey, the pollworkers who remove the seals from a voting machine at the end of the day are asked to sign a paper form (printed by the AVC Advantage at the end of the “results report” at the close of the polls). This form indicates the vote totals from that voting machine, and has a blank in which the pollworkers are supposed to write the number of the tamper-evident seal. In a sample of 51 such “result report” forms from the New Jersey primary election of February 5, 2008, just half (26) of these had a seal number filled in the blank (See Figure 15).²¹

²⁰Sequoia Voting Systems AVC Advantage Maintenance Manual, Release 9.00, Document Version 1.02, January 2005; page 4-1.

²¹I obtained these 51 results reports via an OPRA (Open Public Records Act) request made in March 2008 by Edward Felten. The following AVC Advantage voting machines were represented in our data: 9520 9521 6838 6837 6702 6703 19507 19475 19551 19533 19564 19592 19650 19624 19646 [s/n illegible, mansfield twp 4D] 19678 19677 19688 19696 19697 19744 19748 19749 19756 19757 19786 19787 19799 19496 19843 19842 19853 19872 19552 22791 22951 23133 23301 23146 23038 22980 22977 22970 22938 22902 22891 22867 22810 [2327x?, Bayonne W3] [23880?, Bayonne].

The others were either blank or (erroneously) contained the serial number of the voting machine. This lapse indicates either that there was no seal on the machine, or that the pollworkers neglected to note the number. Therefore, even if the plastic tamper-evident seal technology actually worked, the recordkeeping procedures used in connection with the seals are inadequate in practice.

10.10 **Seals routinely not in place.** The seal holding the Results Cartridge must be removed at the close of the polls, in order to send the Results Cartridge back to county election officials. No new seal is installed by pollworkers.²² Then the AVC Advantage voting machine remains at the polling site for several days before it is collected by a transportation contractor. During this time, no seal is in place protecting the circuit-board cover. Replacing the Z80 Program ROMs at this time will affect all future elections conducted with this machine.

10.11 **Audio-ballot cartridge has no seal.** As Part II of this study discusses, the audio-ballot cartridge is especially vulnerable to attack. It is completely unprotected by any seals, so once the main lock is picked, a trivial task, the audio cartridge can be replaced.

10.12 **Removing the cover without removing the seal.** Because the plastic strap seal that holds the Results Cartridge in place is so flexible, we were able to remove the circuit-board cover without removing this seal. To remove the circuit-board cover, after the screws are removed, one pulls the cover straight out; in Figure 5 this would be towards the viewer of the picture. This removal would be equally easy with or without the Results Cartridge in place.

10.13 **Duplicate seals reduce security.** In studies of computer security, we often consider protocols that have “sequence numbers” that have no duplicates, so that fraudulent messages cannot be inserted. The same issue arises with plastic security seals: they should have no duplicate numbers, otherwise the attacker can simply cut the seal and replace it with a duplicate.

10.14 Union County has been running elections for many decades, with several hundred voting machines. If the county were maintaining a consecutive sequence of seal numbers without duplicates, the serial number on one of today’s seals would be in the hundreds of thousands. But we found that the Union County voting ma-

²²Page 12, “Official Instructions for Members of the District Boards of Elections, Presidential Primary Election – February 5, 2008.” Mercer County. Bates number MERCER 004642 in Gusciora et al. v. Corzine et al.

XX
 OFFICIAL ELECTION RESULTS REPORT
 XX

Date 02/05/08, Time 8:03 PM
 Serial Number 6837
 Protective Counter 5583
 Public Counter 130
 Precinct/District Englewood Cliffs 4
 Polling Place ID ENGC-D4
 Ballot Version 1
 Report Source Internal Machine Memory
 February 5, 2008

Figure 15: Results report tape from the NJ Presidential Primary of February 5, 2008, as signed by witnesses at the close of the polls in Englewood Cliffs, NJ.

Candidate	Candidate Totals	Total
*** REPUBLICAN ***		***
* US President C11		(1)
D11 Rudy Giuliani		1
E11 Ron Paul		0
F11 Fred Thompson		0
G11 Mitt Romney		9
H11 Mike Huckabee		3
I11 John McCain		29
B11 Personal Choice		0
*** DEMOCRAT ***		***
* US President- 19th Dist C18		(1)
D18 Barack Obama		46
E18 Joe Biden		0
F18 John Edwards		2
G18 Hillary Clinton		39
H18 Dennis Kucinich		0
I18 Bill Richardson		0
J18 Uncommitted		0
B18 Personal Choice		1
Write In Votes		
* US President- 19th Dist C18		(1)
XNNRN MITT ROMNEY		
Option Switch Totals		
1 UNUSED		0
2 UNUSED		0
3 UNUSED		0
4 UNUSED		0
5 UNUSED		0
6 REPUBLICAN		42
7 UNUSED		0
8 UNUSED		0
9 UNUSED		0
10 UNUSED		0
11 UNUSED		0
12 DEMOCRAT		88
Total		130

The seal number is not filled in the blank just above the signature lines, as it should be. About half of the 51 results reports we examined had the seal number missing.

At right, a close-up of the same report.

Election Officers
 Please Complete After Closing The Polls
 We the undersigned Election Officers do hereby certify that on the 5th day of FEB 2008 this board under the scrutiny of each member, closed the polls from further voting, obtained this printed record of votes cast on this machine and that after the polls closed, the Protective Counter read 5583 and the Public Counter read 130 and the machine has been sealed with seal # _____.

Signed:
 Helen D'Amato
 Connie Campbell
 Margaret Tomarsky
 Benjamin Staller

Election Officers
 Please Complete After Closing The Polls
 We the undersigned Election Officers do hereby certify that on the 5th day of FEB 2008 this board under the scrutiny of each member, closed the polls from further voting, obtained this printed record of votes cast on this machine and that after the polls closed, the Protective Counter read 5583 and the Public Counter read 130 and the machine has been sealed with seal # _____.

Signed:
 Helen D'Amato
 Connie Campbell
 Margaret Tomarsky
 Benjamin Staller

chine provided to us had seal number 585 (that is, it is marked with nothing more than the name of the election-supply vendor “INTAB” and the number 0000585). This strongly suggests that Union County orders each batch of new seals starting from 0. This defeats the purpose of numbered and logged security seals.

10.15 **Defeating tamper-evident seals in general.** We have studied seals in detail because, like locks, they are important in the field of computer security. One of the most useful reference works in this area is by Dr. Roger G. Johnston of the Los Alamos National Laboratory of the U.S. Department of Energy. Los Alamos has scientists who work on nuclear weapons and scientists who work on the problem of nuclear proliferation. This laboratory has reasons to study the security and tamper-resistance of seals, because these can be vital in the transport of nuclear materials and in the inspection of nuclear facilities. Dr. Johnston has published several scientific studies of the vulnerability of security seals. In one such study²³ he studied 94 different types of seal, including 13 different designs of plastic seals, including several different plastic strap seals. It is plastic strap seals that are used on the Results Cartridge of the AVC Advantage.

10.16 Dr. Johnston found “how to defeat all 94 seals using rapid, inexpensive, low-tech methods.” He defines, “Defeating a seal consists of opening the seal without any detectable damage or evidence of entry; or opening the seal and repairing any damage and/or erasing detectable evidence of entry; or replacing the entire seal with a counterfeit that will be confused with the original; or replacing relevant parts with counterfeits.”

10.17 All of Johnston’s attacks were low-tech, and can be implemented with tools and supplies that can be carried easily by one person. The median cost of materials and tools to defeat a seal is under \$100. The median time to defeat a plastic seal is two to three minutes.

10.18 The experimental methodology presented by Dr. Johnston in this and other reports appears to be sound.

10.19 We found that we were able to bypass the plastic seal installed by Union County, and remove the circuit-board cover without disturbing the seal. We have shown this on the video that accompanies this report. Furthermore, based on Dr. Johnston’s analysis we conclude that, no matter what form of plastic strap seal

²³ “Vulnerability Assessment of Security Seals,” by Roger G. Johnston, Ph.D. and Anthony R. E. Garcia, technical report LA-UR-96-3672, Los Alamos National Laboratory, 1996.

a county might use, it would not prevent, deter, or even significantly delay a determined attacker from replacing or modifying either the internal software or the removable ballot cartridges of a voting machine.

11 Reverse engineering allows construction of fraudulent firmware even without access to trade-secret source code

11.1 Summary: An attacker would not need Sequoia’s trade-secret Source Code in order to design fraudulent vote-stealing firmware.

In order to construct fraudulent vote-stealing firmware the attacker must understand the legitimate firmware in the voting machine just enough to modify it. One might think this is not possible, because the firmware is a secret. However, the firmware is present in every single AVC Advantage voting machine, and is straightforward to extract and analyze. The attacker would apply *reverse engineering* to analyze the firmware, even without source code.

11.2 “Reverse engineering” is the process of deducing the design of an engineered artifact from the artifact itself. For example, recovering the Source Code from the Firmware would be reverse engineering. Or, recovering the design specifications and behavioral description from the Source Code would be another form of reverse engineering.

11.3 Reverse engineering is commonly done in industry for a variety of reasons: for example, learning how a competitor’s product works, or learning how your own product works when the engineers who built it have left the company and you can’t find the original design documents or source code.

11.4 In our current study, pursuant to the Court’s order, we requested access to Sequoia’s source code. We did this, not because it’s impossible to analyze and hack the firmware without the source code, but because the reverse-engineering process would have added several weeks of time to the analysis. We requested source code in order to expedite this examination.

11.5 In 2007 Appel and students performed a study to quantify how easy it is to hack the AVC Advantage without source code. This kind of hack takes 4 steps:

- Step 1 is to obtain access to the AVC Advantage, to get a copy of the firmware. In Section 8, we described how one could do this illegally; Appel did it legally, by purchasing a used machine.

- Step 2 is to derive source code from firmware by perform “reverse engineering” analysis.
- Step 3 is to prepare a new, fraudulent program; in Section 4 of this report we explain that this took 4 person-days.
- Step 4 is to install the fraudulent firmware into the voting machines, as we describe in Section 4 and showed on the video that accompanies this report.

It is Steps 1 and 2 that we will discuss in this section.

It is easy to legally obtain voting-machines to analyze

11.6 In early January 2007, the county of Buncombe in North Carolina advertised for sale on the Internet auction site govdeals.com several Sequoia AVC Advantage voting machines. There were 136 machines sold, in lots of 10 machines, 4 machines, and 5 machines, for a total of 18 lots. The auctions closed on January 16 and January 26, depending on the lots. Figure 16 shows a screenshot from the govdeals.com site showing that the lots of voting machines all sold to various bidders for prices ranging from \$7 to \$140 per lot. Figure 17 shows a description of the AVC Advantage merchandise. The auction site govdeals.com is, apparently, meant for federal, state, and local governments to sell surplus equipment. Any person can qualify to bid on and purchase equipment through this site.

11.7 Appel purchased one lot of 5 machines, for a price of \$82 for the lot. In registering to bid, he did not have to present any credentials other than his name, address, e-mail, and telephone number. No other questions were asked of him by govdeals.com or by Buncombe county. The government had no information about him or his motives in obtaining the voting machines at any time before or after the auction and delivery of the voting machines to him. He paid for the machines by cashier’s check. He had these machines shipped to Princeton by commercial carrier, where they arrived on February 2, 2007. The machines arrived in operating order, complete with one Results Cartridge and two sets of keys per machine.

11.8 The machines, originally sold to Buncombe County in 1997 for \$5200 each, are physically very similar to the Union County machines, except that they do not contain an audio-kit (daughterboard) and the ROMs are version 5.00D instead of Union County’s 9.00H. Figure 1 shows a photograph taken in February 2007 of one of Appel’s Sequoia AVC Advantage voting machines in his office at Princeton University.



New Bidders Register FREE!

Registered Bidders Login:

User Name: Password:

Feb 8, 2007, 4:25 PM ET S1

[Home](#)

[Site Map](#) [Contact Us](#) [FAQ](#) [Help](#)

SearchResults Closed Items for voting
Items 1 through 10 of 18

Inventory ID	Description ▲	Asset Location	End Date/Time ET	Start/Current Bid
1	Lot of (10) Voting Machines	Asheville, NC	1/16/07 9:45 AM	\$140.00 Bids: 17
10	Lot of (10) Voting Machines	Asheville, NC	1/26/07 4:30 PM	\$32.00 Bids: 9
12	Lot of (10) Voting Machines	Asheville, NC	1/26/07 4:30 PM	\$32.00 Bids: 7
15	Lot of (10) Voting Machines	Asheville, NC	1/26/07 4:00 PM	\$32.00 Bids: 7
17	Lot of (10) Voting Machines	Asheville, NC	1/26/07 4:35 PM	\$32.00 Bids: 7
18	Lot of (30) Voting Machines	Asheville, NC	1/27/07 4:00 PM	\$102.00 Bids: 27
4	Lot of (4) Voting Machines	Asheville, NC	1/16/07 9:50 PM	\$20.00 Bids: 4
5	Lot of (4) Voting Machines	Asheville, NC	1/16/07 9:45 AM	\$20.00 Bids: 6
6	Lot of (4) Voting Machines	Asheville, NC	1/16/07 9:50 AM	\$60.00 Bids: 6
7	Lot of (4) Voting Machines	Asheville, NC	1/16/07 9:50 PM	\$7.00 Bids: 2
<i>There was a page break in the original document that I have suppressed here. -- A. Appel</i>				
8	Lot of (5) Voting Machines	Asheville, NC	1/16/07 9:45 AM	\$42.00 Bids: 5
9	Lot of (5) Voting Machines	Asheville, NC	1/16/07 9:45 PM	\$12.00 Bids: 3
11	Lot of (5) Voting Machines	Asheville, NC	1/26/07 4:35 PM	\$32.00 Bids: 10
2	Lot of (5) Voting Machines	Asheville, NC	1/16/07 9:45 AM	\$82.00 Bids: 13
3	Lot of (5) Voting Machines	Asheville, NC	1/16/07 9:50 AM	\$60.00 Bids: 5
16	Lot of (5) Voting Machines	Asheville, NC	1/26/07 4:35 PM	\$32.00 Bids: 8
13	Lot of (5) Voting Machines	Asheville, NC	1/26/07 4:00 PM	\$112.00 Bids: 22
14	Lot of (5) Voting Machines	Asheville, NC	1/26/07 4:30 PM	\$32.00 Bids: 8

[Previous](#) 1 2

Page 2 of 2

Figure 16: List of AVC Advantage voting machines sold by Govdeals.com in January 2007.



User Name:

[Home](#) [Back](#) [Terms and Conditions](#) [Bid History](#)

Item: **Lot of (5) Voting Machines**

Starting Bid: **\$1.00**

Bid Increment: **\$2.00**

Tax Imposed: **NO**

Auction Ended: **Tuesday, January 16, 2007 at 9:45 AM ET**

Sold Amount: **\$82.00**

Description: **This lot includes: (5) Sequoia voting machines, model AUM, wheelchair accessible, not HAVA compliant (means not audio equipped), paid \$5200.00 new for each one in 1997, maintained on a very strict schedule, framework replaced 5 years ago. Software and Battery chargers not included.**

[Photo Gallery](#)

Quantity: **1 Lot**

Condition: **Good**

Seller Name: **Buncombe County, NC**

Asset: **44 Valley Street**

Location: **Asheville, NORTH CAROLINA 28801**

[Map to this location](#)

Special Instructions: **If you are interested or wish to schedule an inspection, please contact Shirley Jones at (828) 250-4802 or contact by email shirley.jones@buncombecounty.org. Please note all items are sold as is: We believe to the best of our knowledge that the items are in good working order, however Buncombe County makes no guarantees concerning the future operation of these items nor will be held responsible for any subsequent parts or labor that may be needed. Buncombe County reserves the right to reject any and all bids.**

Inventory ID: **2**

Category: **Election Equipment**

Figure 17: *Description of the AVC Advantage machines that Appel purchased through Govdeals.com in January 2007.*

Reverse-engineering translates the AVC Advantage firmware back to source code

- 11.9 In the spring of 2007, Appel advised a team of students at Princeton University, to assess the effort required to reverse-engineer the AVC Advantage.
- 11.10 Joshua Herbach wrote a simulator, a software program running on an ordinary PC. The the firmware can be loaded into this simulator and it will run the firmware as if the firmware were installed in the AVC Advantage voting machine.²⁴ Alex Halderman and Ariel Feldman analyzed the circuit boards and the contents of the ROMs.²⁵
- 11.11 Herbach built the simulator in approximately 3 person-weeks, that is, 25% of his time for 12 weeks. He started with an open-source Z80 simulator, fixed the bugs in it, and then implemented simulation of input/output operations that the Advantage uses to run its memory manager, external lights and buttons, and other devices.
- 11.12 Halderman and Feldman reverse-engineered the circuit boards; this took about 4 person-weeks. Then they used the IdaPro reverse engineering tool to analyze about 35 kilobytes of the firmware; this took about 2 person-weeks. The version 9 AVC Advantage has 320 kilobytes of firmware. We estimate that the reverse-engineering task would take about 25 person-weeks.
- 11.13 We obtained Sequoia’s Source Code, by Court order, about one year after the reverse-engineering study concluded. Therefore, the reverse-engineering experiment was not influenced in any way by seeing Sequoia’s Source Code.

Reverse-engineering is possible even without possession of an AVC Advantage DRE

- 11.14 It would be entirely possible to cheat in an election even without having possession (as we do) of a government-surplus AVC Advantage voting machine. It is straightforward, although illegal, to get a copy of the firmware by tampering with a voting machine while it is left unattended in a public place. (Section 8 describes

²⁴ “Simulating the Sequoia AVC Advantage DRE Voting Machine” by Joshua S. Herbach. Department of Computer Science, Princeton University, May 2007

²⁵ “AVC Advantage: Hardware Functional Specifications” by J. Alex Halderman and Ariel J. Feldman, technical report TR-816-08, Department of Computer Science, Princeton University, March 2008.

how voting machines are left unattended in public places.) One would open the back door, unscrew the 10 screws holding the circuit-board cover in place, pry out the four ROM chips, and put each one in a ROM-reader device for 5 seconds. (We show this device at ¶5.4.) Then he would replace the (unaltered) ROM chips, replace the cover, and close the door. The attacker can then study and reverse-engineer the firmware in the privacy of his own home.

Another reverse-engineering study

11.15 In the summer of 2007, the Secretary of State of California commissioned a “top-to-bottom review” of the hardware and software of the voting machines then in use in California. The review was conducted by several teams of computer-security experts. Most of the experts were from universities (in California, Pennsylvania, New Jersey, and Texas) but some were at private consulting companies.

11.16 One of the explicit goals of the California study was to determine whether an attacker could exploit vulnerabilities in a voting machine *without* access to the source code. Therefore, for each voting machine studied, two separate teams were constituted. The “source code review team” studied the source code to assess its accuracy and security, and the “red team” studied the physical voting machine without access to the source code. On all the voting machines studied, the red team found ways to exploit security vulnerabilities in the voting machines. In particular, the red team was able to extract and analyze the Sequoia AVC Edge²⁶ firmware, and construct malicious versions of that firmware, without access to the source code.²⁷

11.17 **Conclusions.** Keeping the source code secret does not make the AVC Advantage, or any voting machine, secure. The source code is simply a shortcut that enables the attacker to skip the step of reverse-engineering the firmware. The security vulnerabilities we describe could be found by someone without access to the source code.

²⁶They studied voting machines used in California, including AVC Edge; the AVC Advantage is not used in California and they did not study it.

²⁷“Security Evaluation of the Sequoia Voting System: Public Report”, Computer Security Group, Department of Computer Science, University of California, Santa Barbara, July 2007. http://www.sos.ca.gov/elections/voting_systems/ttbr/red_sequoia.pdf

12 Fraudulent firmware can be installed inside the Z80 processor chip

12.1 **Summary: It is possible to physically replace the main computer chip on the motherboard with a fraudulent computer that steals votes.**

12.2 The CPU (central processing unit) chip that “masterminds” the AVC Advantage 9.00 is a Z80 processor, invented in 1976. With today’s technology, it is straightforward to replace the Z80 on the AVC Advantage motherboard with an imitation of a Z80, one that is specially constructed to steal votes instead of running the legitimate firmware from ROMs.

12.3 One way to “hack” the AVC Advantage (or any electronic voting machine) so that it steals votes is to replace the CPU chip with a fraudulent one that does not obey the instructions in the firmware. To do this in 1980 might have required a million dollars, to design a new processor chip and fabricate it in silicon. However, using modern technology it can be done for a few dollars in parts, and a few weeks of time by an engineer trained at the bachelor’s degree level.

12.4 The way to do this is via a *field programmable gate array* (FPGA). This is a commercially available silicon chip that can be programmed to simulate any kind of CPU chip. Programmable gate arrays can be slower than the chips they simulate by a factor of 10 or more. However, modern computer chips are well over 1000 times faster than the computer chips of the Z80 era. Therefore it is easy to program a modern FPGA to simulate an ancient Z80.

12.5 Computer hobbyists have already programmed a Z80 simulation into an FPGA, and published the entire design specification.²⁸ An FPGA chip that can be programmed to simulate the Z80 costs about \$13.²⁹ To have an FPGA chip professionally custom-molded into a plastic chip package that would mimic the Z80 on the motherboard would cost \$40 each, in quantities of 300 or more (or \$60 in quantity 50).³⁰

12.6 The fraudulent processor chip would be built as follows. One would start with the readily available design specification for the Z80 processor, implemented in

²⁸zxgate.sourceforge.net

²⁹Xilinx “Spartan 3” at emwcs.avnet.com

³⁰Quik-Pak IC Packages, Assembly & Prototype Services, San Diego, CA.

- the FPGA. One would install fraudulent vote-stealing firmware, inside the same FPGA.
- 12.7 The attacker would install this fake Z80 in place of the real Z80 on the motherboard. He would not touch the ROM chips that contain the legitimate vote-counting firmware—he would leave them alone on the motherboard. However, the computer program (firmware) in the fake Z80 would choose when to fetch instructions from the legitimate ROMs, and when to ignore those instructions and use its own internal instructions.
- 12.8 The behavior of the voting machine will be the same as if the ROMs were replaced by fraudulent firmware: the machine would cheat in elections, but it would not cheat in circumstances where it is likely to be detected. The fraudulent election program will interact with the voter and with the Results Cartridge in almost the normal way. Except, of course, that it writes the wrong votes into the Results Cartridge and prints the wrong votes (to match) onto the results report printout.
- 12.9 To replace the Z80 processor chip it must be unsoldered from the motherboard. Desoldering tools are widely available, in a range of prices from \$30 and up. Figure 18 shows a high-performance industrial desoldering device that sells for \$649.
- 12.10 This attack requires more work and more sophistication to perform. Instead of taking a week to design a fraudulent ROM chip, it might take several weeks for a person to prepare this attack. However, no new science needs to be invented—all the techniques are well understood, and all the processes and parts are easily affordable.
- 12.11 **Fraudulent processors are of concern to many scientists.** A report from the National Institute of Standards and Technology, used by a committee of the Federal Election Assistance Commission as the basis for a resolution on voting machine standards, explicitly discusses this kind of fraudulent-processor “hack” (under the term “ASIC,” for Application-Specific Integrated Circuit); see paragraph 16.2 of our report for more discussion.
- 12.12 To examine the computer-security implications of fraudulent processor chips, researchers at the University of Illinois built a fraudulent processor chip based on the SPARC computer made by Sun Microsystems.³¹ They write, “Current defense

³¹ “Designing and implementing malicious hardware,” by Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou, in *Proceedings of the First USENIX*



Figure 18: *Desoldering tool uses heat to melt the solder and a vacuum pump to suck it out of the joint. Can be used to remove Z80 processor chip from AVC Advantage motherboard.*

www.howardelectronics.com/edsyn/zd500dx.html

techniques are completely ineffective against malicious processors.” Then they go on to speculate about how, in the future, it might be possible to detect fraudulent processor chips.

12.13 The U.S. Department of Defense is concerned that fraudulent processor chips, fabricated in China and then installed in U.S. military networks, could contain extra fraudulent circuitry. These fraudulent computers could purposely leak secret data that passes through them. Therefore the DoD funds research by the IBM Research Laboratory, among others, to find a way to detect fraudulent processor chips.³² This research being done by IBM is interesting from a scientific point of view, but it is years away from application to a tool that New Jersey election officials could use.

12.14 **Conclusion.** Replacing processor chips with fakes that cheat is a recognized threat, not only in voting computers but in other applications as well.

13 Would anyone go to these lengths?

13.1 It might seem that no person would spend half a year of his time to reverse-engineer the firmware of a voting machine, or design a fraudulent computer chip on an FPGA. However, political campaigns are very high-stakes contests. Candidates for president will spend hundreds of millions of dollars to be elected, and they benefit from thousands of volunteers that spend enormous amounts of time and money to get their candidates elected. Some of these partisans cross the line into unethical or downright illegal tactics. Half a year is not such a lot of time. We have spent far more than that just in explaining the technology issues in voting machines to the public.

13.2 In addition, there is an aspect of “puzzle-solving” that motivates some computer programmers to take on a challenge like this. Some computer hackers spend months developing a clever new computer virus that costs the world millions of dollars and countless hours of inconvenience. Mostly they have done this for the fun of it, not for expectation of reward: new computer viruses appeared year after year before anyone figured out how to exploit them for criminal profit.

Workshop on Large-Scale Exploits and Emergent Threats (LEET), April 2008.

³² “Trojan Detection using IC Fingerprinting,” by Dakshi Agrawal, Selcuk Baktir, Deniz Karakoyunlu, Pankaj Rohatgi, and Berk Sunar. In *IEEE Symposium on Security and Privacy*, 2007.

13.3 Thus, the time required to design a vote-stealing “hack” is not enough to be a substantial deterrent.

14 There is no means to reliably detect fraudulent firmware in AVC Advantages

14.1 We have described methods by which an attacker could install new firmware in the AVC. In general, it is almost impossible to detect this fraud from any external observation of the voting machine.

14.2 We will describe a procedure that an election official could use, in principle, to test the ROM chips. However, this method is fraught with difficulties, which we will explain. Also, this method for testing ROM chips does *not* work for detecting fraudulent Z80 processor chips. **There is no *practical* method that New Jersey election officials could use to detect fraudulent Z80 processor chips.**

14.3 The procedure for examining ROM chips is: Unscrew the circuit-board-cover screws, carefully pry out each ROM chip, insert each ROM chip into a ROM reader device attached to a PC, copy the contents of the ROM to the PC, and compare with a reference standard using a computer program. Then replace the ROMs into the circuit board, screw everything back together, and run the machine through Pre-LAT to make sure that the ROMs were put back in the right places.

14.4 No election officials in New Jersey have ever performed this procedure (based on documents produced by the State of New Jersey in connection with this lawsuit).

14.5 This procedure cannot catch the replacement of ROMs at the polling place while they sit unattended for up to three days before the election.

14.6 This procedure cannot easily be done in the presence of witnesses from the political parties *in such a way that they can trust that the test is being performed accurately and legitimately*. This is because it depends on the software running in the PC that is testing the ROMs. In effect, we are using one piece of software to check on another. **If we were a witnesses to this procedure, even with all our expertise, we would have no way of knowing that the testing software in the election official’s PC is doing what it is supposed to.** An ordinary citizen serving as a witness representing a political party would be in no better position than we would.

14.7 Additionally, using ROM-testing devices could easily contaminate legitimate ROM chips. The PC that is used for testing ROMs may carry a virus. Millions of “innocent” PCs on the internet have been infected by viruses that cause them to do the bidding of those who created the virus.³³ At the very least, an attacker who gained control of the testing computer by means of a virus from the Internet, could install fake testing software that gives a pass to fraudulent ROM chips. At worst, fake testing software can modify the contents of the ROM, to install fraudulent vote-stealing firmware instead of reading and testing it.

14.8 As we explained in paragraph 12.13, there is **no standard method** for detecting fake processor chips, although scientists are pursuing this goal. Even if such a method were to be developed, it would require New Jersey election officials to desolder and remove the Z80 processor chips, which runs the risk of damaging them. (The attacker who is replacing them with fake processor chips does not mind damaging the ones he is removing, in contrast to election officials who would need to test and reinstall them.) **Therefore, fraudulent vote-stealing Z80 processor chips are not practically or reliably detectable.**

15 Many insiders have access sufficient to tamper with AVC Advantage voting machines

15.1 There are many insiders who have sufficient access to voting machines to install fraudulent firmware. These insiders include employees of the Superintendent of Elections: from maintenance logs provided by Camden County, it appears that Camden employs at least 8 election-machine technicians.³⁴ These insiders include private companies who service the voting machines.³⁵ These insiders include the delivery company who delivers AVC Advantage machines to the polling places

³³ Press release, FBI National Press Office, June 13, 2007. “The majority of victims are not even aware that their computer has been compromised or their personal information exploited,” said FBI Assistant Director for the Cyber Division James Finch. “An attacker gains control by infecting the computer with a virus or other malicious code and the computer continues to [appear to] operate normally.”

³⁴ Bates Numbers CAM 0003–000444

³⁵ For example, at least two employees of Election Support & Services, Inc. of Medford, NJ, perform set-up, ballot verification, audio test, and Pre-LAT test for the County of Camden. Letter from ES&S to County of Camden, January 22, 2008; Bates Number CAM 000295.

(and sometimes to the wrong place).³⁶

15.2 In many parts of the 20th century, corrupt political machines (particularly in New Jersey, but elsewhere as well) manipulated elections from the inside, by controlling the election workers. Even in recent decades, there have been several corrupt elected and appointed officials, even in New Jersey.

15.3 In general, we should assume and believe that the people who run our elections are honest. But even so, we permit party challengers to witness the events in the polling place. That is, we strive to achieve elections that are sufficiently auditable and witnessable that the public (and the losing candidate) can trust that the outcome is legitimate without having to trust the individuals who run the elections.

15.4 AVC Advantage machines, which can be hacked either inside or outside the warehouse, cannot achieve this level of trust.

16 The danger of fraudulent firmware is widely recognized by experts

16.1 We have explained that hidden changes to the software (firmware) of a voting machine can *undetectably* change the outcome of an election. Many computer scientists and election experts came to recognize the importance of this problem in the years 1999–2004, by which time it was a well-established scientific consensus.

16.2 The federal Election Assistance Commission (EAC) formulates standards for voting machines (having taken this role over from NASED³⁷ in 2005). In 2006, the EAC’s Technical Guidelines Development Committee (TGDC) asked the National Institute of Standards and Technology (NIST) to draft a report explaining this concept and defining appropriate terms. This report³⁸ was then used as a basis for discussion at a December 2006 meeting of the TGDC of the EAC.

16.3 The report defines the term **software independence**. *A voting system is software-independent if a previously undetected change or error in its software*

³⁶ See footnote 12 on page 28. Also, “Locations of Replacement machines for Presidential Primary:” “the delivery company delivered [two] machines to the wrong place,” Bates Number CAM 0001.

³⁷ National Association of State Election Directors

³⁸ “Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC,” draft report, National Institute of Standards and Technology, November 2006.

cannot cause an undetectable change or error in an election outcome. That is, the votes should be countable (auditable) independent of the behavior of any computer software. This is because (1) software is so complex in general that it is not possible to be confident that it is adding the votes correctly, and (2) it is inherently difficult or impossible to know what software is currently installed inside a voting machine or computer.

16.4 The report explicitly notes that “software” encompasses not only the firmware inside the voting machine, but also other computer chips in the machine; that is, it addresses not only the ROM-replacement “hack” that we discussed in Section 4 but also the fake Z80 processor that we discussed in Section 12.³⁹

16.5 The Technical Guidelines Development Committee of the EAC, at its December 2006 meeting, on the basis of the definitions in the NIST report, adopted a resolution calling for software independence in the next generation of voting systems standards.⁴⁰

16.6 Paperless DRE voting machines such as the AVC Advantage⁴¹ lack this crucial quality of software independence. The results of the election in each precinct are reported at the complete discretion of the program, which is in control of *all* of the records of the votes up until the time of the close of the polls. That means that paperless DREs are *inherently* susceptible to fraud and error.

16.7 **Evidence for consensus.** Experts in computer science who have also developed expertise in election technology have reached an overwhelming consensus that software independence is necessary in voting, and that paperless DREs are unacceptable. We will explain the evidence for this statement.

16.8 The Election Technology Library “is designed to serve as a clearinghouse of information related to election technology” and “has no policy agenda,” according

³⁹ “It should be noted that in [Software Independence], ‘software’ is really means complex technology, which can be software implemented on hardware, e.g., burned into PROMs or built into ASICs. ‘Software independence’ should be interpreted to really mean *complex technology independence*.” — from NIST report cited above.

⁴⁰ Resolutions adopted by the Technical Guidelines Development Committee at the December 4, 5 2006 Plenary Session. <http://vote.nist.gov/AdoptedResolutions12040506.pdf>

⁴¹Of course, the AVC Advantage has a paper printer inside the cabinet, which does not operate while votes are being cast; and the full-face voter-panel is covered by a large sheet of paper on which the names of candidates are printed. By “paperless” we mean that there is no paper ballot for each individual voter, that the voter can verify before casting, and which can be recounted by humans, without software programs interpreting the ballots to them.

to their website.⁴² They publish a *Who's Who in Election Technology*, a “comprehensive list of election technology professionals and those related to election technology” that lists 52 individuals and several organizations. In our examination of their list, we found it to be representative and reasonably comprehensive. Of these 52 individuals, we identified 25 as having education, expertise, and background in computer science or related technology, as opposed to others who are primarily expert in election administration and political science.

16.9 Of these 25 election technology experts, 22 of them⁴³ have joined this consensus that paperless DREs such as the AVC Advantage are unacceptable; either by endorsing the *Resolution on Electronic Voting*,⁴⁴ or by publishing research papers, or both. One of them⁴⁵ has made no public statement one way or the other, perhaps because as Director of NIST he feels it is inappropriate to do so. Only two of them⁴⁶ have made public statements indicating confidence in paperless DREs.

16.10 **More evidence for consensus.** The Association for Computing Machinery (ACM) is the international scientific and professional society for computer science, computer scientists, and computing professionals. It publishes the leading journals and organizes the leading scientific conferences in the field of computer science. The U.S. Public Policy Committee of the ACM recommended, and the ACM adopted, this policy position:

Voting systems should also enable each voter to inspect a physical (e.g., paper) record to verify that his or her vote has been accurately cast and to serve as an independent check on the result produced and

⁴² <http://www.electiontechnology.com>

⁴³ Andrew Appel, Matt Bishop, Matt Blaze, David Chaum, Lorrie Cranor, David Dill, Edward Felten, Harry Hochheiser, Rush Holt, Harri Hursti, David Jefferson, Doug Jones, Rebecca Mercuri, Ronald Rivest, Avi Rubin, Bruce Schneier, Ted Selker, Barbara Simons, Warren Smith, Roy Saltman, David Wagner, Dan Wallach

⁴⁴ “Computerized voting equipment is inherently subject to programming error, equipment malfunction, and malicious tampering. It is therefore crucial that voting equipment provide a voter-verifiable audit trail, by which we mean a permanent record of each vote that can be checked for accuracy by the voter before the vote is submitted, and is difficult or impossible to alter after it has been checked. Many of the electronic voting machines being purchased do not satisfy this requirement. Voting machines should not be purchased or used unless they provide a voter-verifiable audit trail; when such machines are already in use, they should be replaced or modified to provide a voter-verifiable audit trail. Providing a voter-verifiable audit trail should be one of the essential requirements for certification of new voting systems.”

<http://www.verifiedvotingfoundation.org/article.php?id=5028>

⁴⁵ Hratch Semerjian

⁴⁶ Michael Shamos, Brit Williams

stored by the system.⁴⁷

17 Conclusion of Part I

- 17.1 **Creation and installation of vote-stealing firmware in an AVC Advantage is straightforward, and we have demonstrated it. No one approaching an Advantage voting machine in New Jersey—whether a voter, a party challenger, or an election official—can have any justifiable confidence that the machine is legitimately counting the votes.**

⁴⁷ <http://usacm.acm.org/usacm/Issues/EVoting.htm>

PART II

DAUGHTERBOARD AND WINEDS VIRUSES CAN DISENFRANCHISE VOTERS

- 17.2 **Summary: The audio-kit “daughterboard” of the AVC Advantage 9.00 contains its own computer, which is very susceptible to viruses. We have installed new firmware the daughterboard 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.**
- 17.3 In Part I, we described how malicious firmware can be installed on the AVC Advantage motherboard with tools as simple as a screwdriver. In this part, we will describe how fraudulent firmware can be installed in another computer inside the AVC Advantage *using no tools at all*. In fact, because this installation is done *in the ordinary course of inserting an audio-ballot cartridge, it can be done inadvertently by a perfectly honest pollworker*.
- 17.4 In addition, because this fraudulent firmware can then copy itself onto any new audio-ballot cartridge later inserted into the AVC Advantage, the fraud can become a *computer virus* that propagates itself from one AVC Advantage to another.
- 17.5 We have found that such a virus can jump to WinEDS computers, that is, computers used in the election warehouse to prepare new ballot cartridges and to tabulate election results. Such a virus could then change vote data in the election database, and modify the tabulated results. We have found that the WinEDS computers are very vulnerable to hacking from the Internet.
- 17.6 From WinEDS computers, the virus can jump back to other AVC Advantage voting machines.

18 The audio-kit daughterboard is a second computer in the AVC Advantage

- 18.1 The AVC Advantage 9.00 has an “audio kit” containing its own computer. Any voter who wishes to vote by audio instead of on the large printed buttons-and-lights voter panel is permitted to do so. Voters might wish to vote by audio because of vision impairments, mobility impairments, inability to read, or for any other reason—indeed, voters are not required to state the reason they wish to vote by audio.
- 18.2 The audio-kit computer resides on a “daughterboard,” inside the cabinet but separate from the main circuit board of the AVC Advantage (which is called the “motherboard”).
- 18.3 Unlike the motherboard firmware described in Part I, the firmware of the daughterboard does not reside in ROM. It resides in “flash memory”: the flash memory 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.
- 18.4 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 very dangerous. In fact, Sequoia’s design of the daughterboard is in violation of the Federal Election Commission 2002 and 2005 Voting Systems Standards.⁴⁸
- 18.5 Storing firmware in writable flash memory opens the possibility that an attacker can install fraudulent firmware without *any* physical change to the voting machine. In fact, we have demonstrated that this is possible on the AVC Advantage. In this part of the report we describe how a computer virus can spread itself to many AVC Advantage machines. Once installed, the virus can steal votes or selectively disable voting machines.

⁴⁸ “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;

FEC 2005 Voluntary Voting Systems Guidelines, Sec. 7.4.1.

But in fact, we have found that the same flash memory chip on the daughterboard holds both the operating system and election-specific programming.

19 One can install fraudulent daughterboard firmware by inserting a cartridge—even unwittingly

19.1 **Summary:** One can install fraudulent firmware into the daughterboard simply by inserting a cartridge into the slot in the daughterboard. This takes one or two minutes. The person inserting the cartridge does not even need to know that the cartridge is perpetrating a fraud.

19.2 It is easy and straightforward to install fraudulent firmware into the daughterboard memory. There are at least two different ways it can be done.

19.3 **Method 1. Installing firmware by means of a cartridge.** We have used this method to install firmware into the daughterboard, and to remove it again.

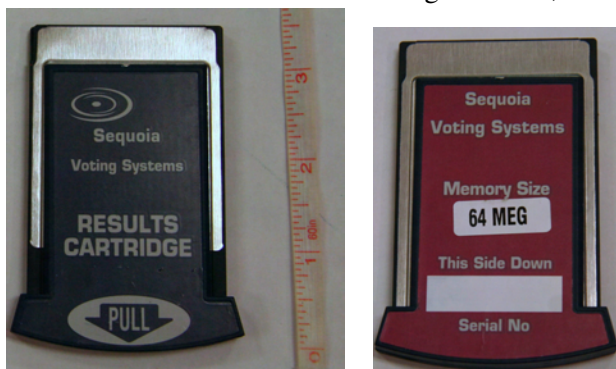


Figure 19: Audio ballot cartridge, front and back. Notwithstanding the text printed on the cartridge, this is not a Results Cartridge.

19.4 The audio-kit has a slot on the top, dimensions about 2.5 inches by 3/8 inches, for the insertion of an Audio Ballot Cartridge. The cartridges that fit in this slot, as provided to us by Union County, NJ, are in the PCMCIA format. PCMCIA cards are a standard on laptop computers; they are about the dimensions of a credit card, but 1/8 of an inch thick.⁴⁹

19.5 The audio-ballot cartridges are labeled “RESULTS CARTRIDGE,” which causes some confusion, because the Sequoia 9.00H also accepts another cartridge called “Results Cartridge,” of dimension 7x4x1 inch, that fits into a different slot. In fact, the small-dimension audio-kit cartridges do not hold “results”; they usually hold audio ballot data, that is, sound recordings of the names of candidates and contests. On other models of Sequoia voting machines, such as the AVC Edge and the ver-

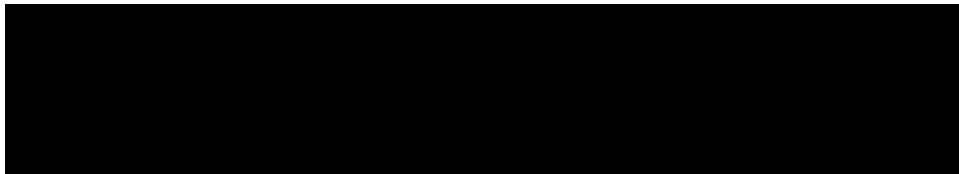
⁴⁹ The Sequoia cartridges are in a plastic packaging that makes them thicker, about 5/16 inch, so they don't fit in a normal *computer* PCMCIA slot unless an extender card is used.

sion 10 AVC Advantage, these PCMCIA-format cartridges do serve to hold results (among other things, as we will explain in Section 61).

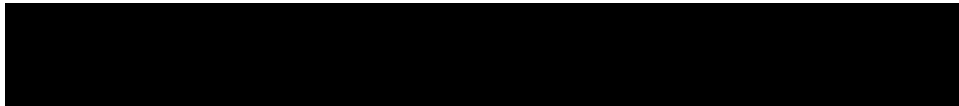
19.6 In fact, PCMCIA-format cartridges can hold any kind of data at all, including audio data, ballot data, and executable programs. The cartridge is formatted as a standard Microsoft FAT file system, just like ordinary computer floppy disks, hard drives, and, in fact, just like ordinary PCMCIA memory cards.

19.7 The daughterboard firmware is stored in a 2-megabyte flash memory, which is also formatted as a FAT file system. This runs a DOS-compatible operating system. When the voting machine is turned on, the operating system executes AU-TOEXEC.BAT, just as on any 1990s-era personal computer that ran the Microsoft operating systems.

19.8



19.9



19.10 In devices that contain firmware in flash memory, where it is desired to be able to update the firmware later, it is a common industrial practice to use an AU-TOEXEC.BAT design similar to what Sequoia has done in the AVC Advantage



At left, a generic PCMCIA memory card inserted into the side of a laptop computer. The Sequoia audio-ballot cartridges are PCMCIA memory cards, but made thicker by being encased in plastic, so they do not fit into the standard slot unless an extender is used, of the type shown at right.

daughterboard. **However, this design makes it extremely easy to install fraudulent firmware into the daughterboard—significantly easier than replacing ROM chips. Therefore this practice is not recommended for security-sensitive equipment that can be accessed by malicious attackers.** Appel has informed New Jersey’s Voting Machine Examination Committee (chaired by Richard Woodbridge, Esq.) of his concern about this problem, in relation to certification of AVC Advantage version 10 machines with printer attachments.⁵⁰

19.11 To install fraudulent firmware in an AVC Advantage 9.00G or H, one has to perform the following steps. *Note that all but the first step are routinely performed by honest election workers in the normal course of preparing AVC Advantage machines for elections.*

1. Prepare a PCMCIA cartridge with new programs in the INSTALL folder. It can be a generic PCMCIA memory cartridge; a cartridge from Sequoia is not needed. This preparation can be done on any ordinary laptop computer.
2. Open the back door of the voting machine, using the key or by picking the lock (see Section 9).
3. Remove any installed PCMCIA cartridge, if any, by simply pulling it out. No seal is used on this cartridge. No screws need to be unscrewed.
4. Insert the new cartridge.
5. Turn on the voting machine. The files will be automatically copied from the cartridge into the daughterboard.

This whole process takes just a minute or two. It is easier than replacing ROMs, because no tools are needed at all.

19.12 Before each election, election workers insert an audio-ballot cartridge into every AVC Advantage voting machine to inform the computer how to pronounce the names of the candidates on the ballot. If an attacker has put fraudulent firmware into the INSTALL folder of the audio-ballot cartridge, then the election worker will then be unwittingly installing that firmware into the AVC Advantage. This means that the attacker never even needs physical proximity to an AVC Advantage voting machine to perpetrate this attack. We will discuss this further in Section 20.

⁵⁰ Letter from Andrew W. Appel to Richard Woodbridge, emailed via Robert Giles, Director, Division of Elections, NJ Department of State, May 27, 2008.
<http://www.cs.princeton.edu/~appel/voting/appel-22may08hearing.pdf>

- 19.13 Even if Sequoia were to fix the very severe vulnerability in its AUTOEXEC.BAT, a second method of installing fraudulent firmware in the daughterboard would still exist. There is no straightforward method of mitigating this second method.
- 19.14 It is a common and necessary industrial practice to provide a means to install firmware into the flash memory of a computer such as the daughterboard. This is because when the daughterboard is first manufactured, its flash memory contains no program that could perform copying via the AUTOEXEC method. Also, such a second method would be necessary if the contents of flash memory gets scrambled by hardware or software failure, so that the AUTOEXEC method no longer works.
- 19.15 To use this second method, one would have to unscrew 5 screws to open the sheet-metal box containing the daughterboard, and one would plug the daughterboard into special equipment. In 1999 this equipment (Compulab 486Base) was available for \$30.⁵¹ This vulnerability cannot be mitigated.

20 Vote-stealing computer viruses can infect AVC Advantage and WinEDS

- 20.1 **Summary: Not only is it easy to install fraudulent firmware in the daughterboard. Worse yet, there is a very severe vulnerability to firmware viruses that propagate through audio-ballot cartridges. We have demonstrated the feasibility of a virus that propagates from AVC Advantage voting machines onto a WinEDS computer, carried on the cartridge. A single virus can propagate onto all the WinEDS computers and the AVC Advantage voting machines used in a county or state. This means that an attacker can install fraudulent firmware without needing physical access to voting machines.**
- 20.2 A computer virus is a program that can copy itself from one computer to another, either through computer networks or through removable media such as cartridges. In addition to merely copying itself, the virus may also have a *payload* that performs some malicious act, such as stealing money via fraudulent financial transactions, forwarding spam e-mail, or stealing votes inside election firmware.
- 20.3 We have found that a virus can propagate through the AVC Advantage to other AVC Advantage machines, from AVC Advantage machines to WinEDS comput-

⁵¹ "Peewee PC sports a pint-sized price," Electronics Design News, August 19, 1999. <http://www.edn.com/index.asp?layout=article&articleid=CA46087>, fetched August 25, 2008

ers, from WinEDS computers to other WinEDS computers, and from WinEDS computers to AVC Advantage machines.

20.4 The WinEDS software, sold by Sequoia, is used by county election workers to prepare ballot definitions and to tabulate votes. WinEDS runs in an ordinary desktop or laptop PC running the Microsoft Windows operating system.

20.5 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 the polling places. After the election, the cartridges are removed from the machines and transported back to county election workers, who then use the WinEDS software to extract the election results and cumulate the results from all the precincts.

20.6 Propagation happens as follows:

1. When an “infected” audio-ballot cartridge (that is, one containing the virus) is inserted into an AVC Advantage voting machine, the virus propagates into the internal flash memory of the (audio-kit) daughterboard.
2. After that time, the virus resides in the internal memory of the daughterboard. If any uninfected cartridge is later installed into that voting machine, the virus copies itself onto that cartridge. That cartridge is now infected.
3. When an infected audio-ballot cartridge is inserted into a WinEDS computer (e.g., to prepare audio-ballots for the next election), the virus copies itself into the Microsoft Windows operating system on that computer, by a mechanism we will describe in Section 22.
4. After that time, when an uninfected cartridge is inserted into the WinEDS computer, the virus will copy itself into the cartridge, thus infecting the cartridge.
5. Also, while the virus resides on the WinEDS computer, it can copy itself onto other WinEDS computers on the same network.
6. 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 Internet surfing. See Section 23.4.

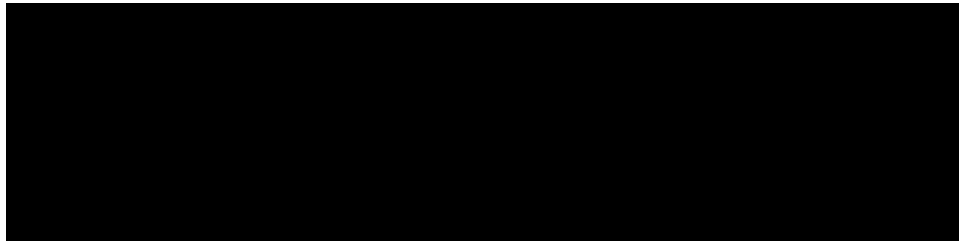
20.7 Like any computer virus, the vote-stealing virus has two parts: the *propagation* part, which copies the virus from one computer to another, and the *payload*, which accomplishes the attacker's goals. The payload of a personal-computer virus might steal financial data, or be a platform for sending spam. A voting-machine virus's payload changes vote data, either in the voting machine during elections, or in the election management system (WinEDS). In the next two sections, we will describe propagation; then we will describe the harm the virus's payload can cause.

21 Viruses can propagate through the AVC Advantage

21.1 **Summary: The design of of the audio kit and its cartridge interface causes a very severe security vulnerability: the ability to virally propagate fraudulent software from one voting machine to another.**⁵²

21.2 Although the attack propagates through audio-ballot cartridges, it works even if no voters ever use the audio-voting feature.

21.3



⁵² A similar design flaw was found in 2006 on Diebold Accuvote machines by Hursti and by Feldman et al., who also demonstrated how an attacker can use this vulnerability to propagate vote-stealing viruses. A similar design flaw was found on the Sequoia AVC Edge in 2007 by Blaze et al.

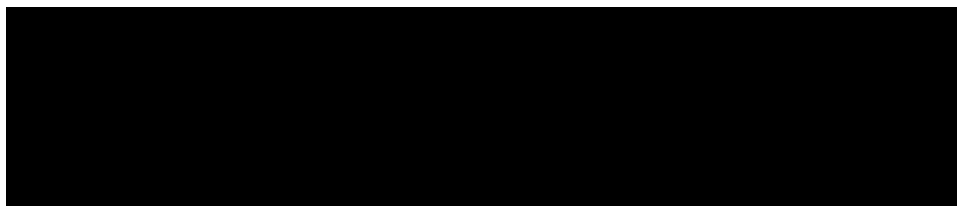
“Diebold TSx Evaluation / Security Alert: May 11, 2006 / Critical Security Issues with Diebold TSx” by Harri Hursti. <http://www.blackboxvoting.org/BBVreportIIunredacted.pdf>;

Security Analysis of the Diebold AccuVote-TS Voting Machine, by Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, in *Proceedings 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*, August 2007.

“Source Code Review of the Sequoia Voting System” by Matt Blaze, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, and Ka-Ping Yee. Report commissioned by the Secretary of State of California, released July 20, 2007, http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf

21.4 The fraudulent SUBSYS.EXE program does not need to limit itself to audio voting, as we will explain in Section 24. It is a computer program with complete control of what the daughterboard does.

21.5



21.6 To verify experimentally that all of this works as we have described it, we wrote a program and copied into an audio-ballot cartridge using an ordinary desktop PC. Then we inserted the audio ballot cartridge, and verified that the AVC Advantage installed our program as firmware in the daughterboard. We verified that our program took control of the daughterboard and copied itself into an audio-ballot cartridge. These are all the steps that a virus would need to take.

21.7 One can start the propagation of vote-stealing viruses through WinEDS and AVC Advantage machines very easily, with access to *any one* of the following:

- A Sequoia audio-ballot cartridge that will be used in some future election.
- An unattended AVC Advantage voting machine, with or without the audio-ballot cartridge installed.
- An unattended WinEDS computer.
- A web site that a user of the WinEDS computer visits.
- Any computer on the Internet that can send a message to the WinEDS computer, if that computer is configured to accept such connections (as Union County's machine is; see Section 23.6).

21.8 **Conclusion:** An attacker can easily inject a virus into the WinEDS/Advantage system that infects all the AVC Advantage machines in a county or a state.

22 Viruses can propagate through WinEDS computers

22.1 **Summary:** Viruses can easily propagate through WinEDS either from the Internet or through audio-ballot cartridges. One virus can propagate onto all

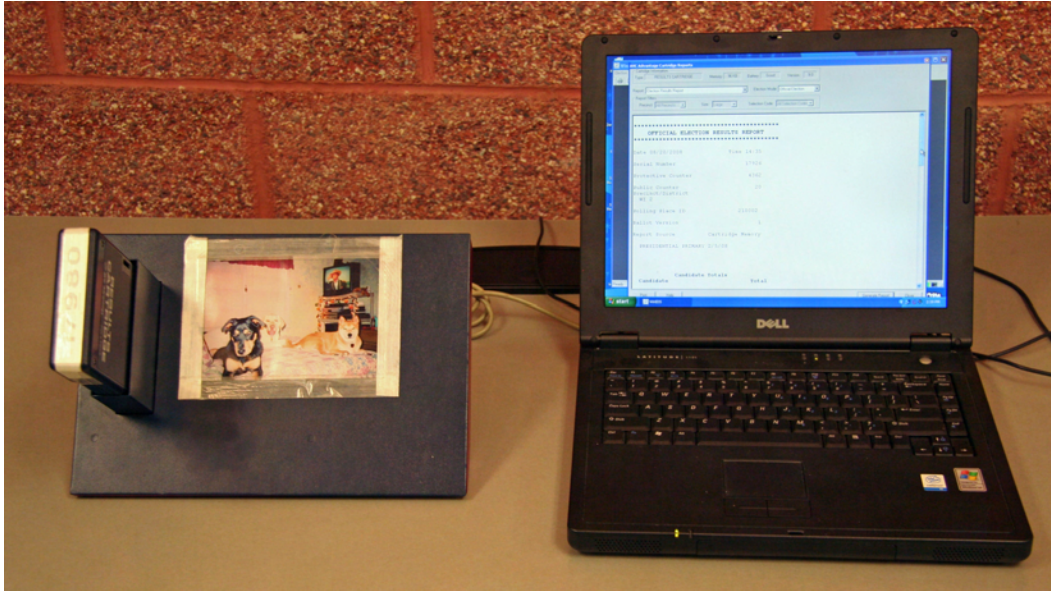


Figure 20: At left, Results Cartridge reader/writer; at right, WinEDS computer

the WinEDS computers and AVC Advantage voting machines used in a county or state. This is a very severe vulnerability.

22.2 The WinEDS software runs on ordinary personal computers running Microsoft Windows. Union County, New Jersey provided to us for examination one computer with the WinEDS software installed. The computer is a Dell Latitude 110L laptop computer running Microsoft Windows XP SP3 and with WinEDS 3.1 installed. The computer is identified in the “computer description” of its “system properties” as “warehouse laptop 1.” Therefore we will assume it is one of several laptop computers that Union County uses in the warehouse in which it also stores its AVC Advantage voting machines. WinEDS computers are used by New Jersey counties not only in warehouses storing voting machines, but in other locations as well.⁵³

22.3 **The computers that run WinEDS in Union County are severely vulnerable to viruses from cartridges and to attacks from the Internet,** as we will explain in this section and the next. As there is there is no reason believe that the Union County computers are in any way different from voting-machine warehouse com-

⁵³ In a telephone discussion (August 2008) with James J. Vokral, Administrator, Middlesex County Board of Elections, Appel learned that Middlesex uses WinEDS computers in its election warehouse in Edison, NJ, as well as in the Board of Elections office in New Brunswick, NJ.

puters used in other counties in New Jersey, our conclusions generalize to the entire State.

22.4 The WinEDS computer is equipped with a reader for large-format Results Cartridges; this reader connects to the computer by a USB port. Small-format audio-ballot cartridges connect into the standard PCMCIA port of the laptop computer, using a standard PCMCIA extender card.

22.5 When a PCMCIA flash memory card (such as an audio-ballot cartridge) is plugged into the PCMCIA port of a standard Microsoft Windows laptop computer, the Windows 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 will presume that other election-warehouse computers in Union County and other counties are configured similarly.

22.6 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 Microsoft Windows computer. On Microsoft 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.

22.7 In Microsoft Windows, when removable media such as PCMCIA or CD-ROM is inserted and automounted, Windows normally searches it for files such as AUTORUN.INF which cause a program from the removable media to be executed as a Windows application. This is the case on the Union County computer.

22.8 It is well known to hackers and to computer-security experts that the Autorun feature is a way that viruses can be propagated.⁵⁴ This feature means that the PC (unsafely) runs an arbitrary program that is stored on any cartridge inserted into the PC. If this program is a virus the audio-ballot cartridge, it will easily infect the WinEDS computer when that cartridge is inserted. Such insertion normally occurs before an election, for the purpose of copying the audio-ballot files into hundreds of audio-ballot cartridges for all the county’s voting machines.

⁵⁴ Even if Autorun were to be disabled, the Automount feature of Windows sometimes contains exploitable vulnerabilities that permit malicious software on insertable media, such as PCMCIA cartridges, to take control of the host PC and install viruses.

- 22.9 Once the virus propagates onto the WinEDS computer, it can do many things:
1. Cause WinEDS to fraudulently miscount votes, when it accumulates the results from different precincts;
 2. Cause WinEDS to write fraudulent ballot definitions into (large-format) Results Cartridges;
 3. Propagate itself into other audio-ballot cartridges, either within the county or in a different county, and thereby infect other AVC Advantage voting-machine daughterboards;
 4. Propagate itself through the Internet, or through County or State internal networks, to other WinEDS computers. These WinEDS machines are routinely connected to the Internet already. Even if that were not the case, as the State of New Jersey moves towards a centralized voter-registration database, the election computer networks of the counties will be inevitably connected to each other or to a State network. This increases the risk that viruses can spread throughout the State.

22.10 **Ineffectiveness of antivirus.** Although the WinEDS computer used by Union County is equipped with an antivirus program,⁵⁵ this kind of antivirus provides no useful protection against a specialized vote-stealing virus. The reason is that antivirus programs work by recognizing *known* viruses, and are ineffective against *new* viruses. When a personal-computer virus propagates around the world to millions of PCs, the makers of antivirus software eventually notice it, and rush to modify their antivirus software to detect the new virus. However, if a virus propagates just to a few dozen machines in the internal network of state or county election officials, then the makers of antivirus software will never see it. Thus they will not be able to update their antivirus program to detect and remove the vote-stealing virus.

23 WinEDS computers have severe security vulnerabilities and are routinely connected to the Internet

23.1 **Summary: Vote-stealing viruses can propagate into WinEDS computers from the Internet. Union County's WinEDS computer, and the WinEDS election-management program and data on it, is severely vulnerable to attack from the**

⁵⁵ Symantec AntiVirus v10.0.2.2000, updated June 25 2008 (delivered to us 1 July 2008)

Internet. The general security configuration of the machine is wide open. In addition, there is an enormous amount of casual Internet browsing by election employees. This means outsiders can interfere with preparation of the ballots, can modify the results as they are added up, and change the data stored in the database.

- 23.2 WinEDS runs on a standard Windows PC; the Union County system that we studied runs Windows XP release SP3 with a normal complement of programs like Microsoft Office, Internet Explorer 7 (IE), Windows Media Player, and so on.
- 23.3 Any system has security vulnerabilities, and both Windows and IE are known to have problems. The FEC Guidelines require that if a computer used to manage election information also includes browsers, compilers, database systems and the like, they are governed by the requirements as well, unless the software can be disabled or removed when voting system functions are enabled.⁵⁶
- 23.4 In general, security-sensitive computers should not be used for extensive casual web-browsing, because untrustworthy web sites can cause spyware and viruses to be downloaded onto the computer. However, the Union County machine has been used extensively for browsing on the web, using Internet Explorer. The list of “Temporary Internet Files” maintained by IE shows a large number of web sites visited, for mail, shopping, personal banking, streaming music, pictures, and checking news and sports results. Only a small fraction relate to the official Union County web site, ucnj.org. Each of these visits typically triggers a host of downloaded images and tracking information from advertising sites like DoubleClick, Tacoda, Advertising.com, and so on. The Temporary Internet Files folder maintained by IE contains well over a thousand such temporary files related to casual web-surfing, with dates over a period of years, including periods immediately before and after the February 2008 election and even a visit to a banking site on election day.
- 23.5 At least one of the frequently-used online services, AOL’s AmpX music streaming service, is known to have serious vulnerabilities because of buffer overrun errors. This has been known for several years. Symantec describes this threat as having “High” severity, and observes that “A successful attack would corrupt process memory, allowing arbitrary code to run in the context of the client application...”⁵⁷

⁵⁶ VVS, Section 4.1.3

⁵⁷ Symantec Corporation, http://www.symantec.com/avcenter/attack_sigs/s50125.html, visited August 23, 2008. Symantec is a well respected maker of antivirus and other security software.

That is, the attacker using the AmpX security vulnerability would produce a malicious music stream. When a user of the WinEDS computer listens to that music, the malicious music stream would install a virus on the WinEDS computer. Then the attacker could do practically whatever he wants on Union County's WinEDS computer, including modifications to the WinEDS vote database or the WinEDS vote-counting program.

23.6 Computers running the Microsoft Windows operating system communicate with the outside world through a huge variety of "services" and "protocols." Each of these constitutes a vector through which attackers on the Internet can insert malicious software into the computer.

23.7 Computers that handle information whose integrity needs to be protected should have their operating-system services configured to minimize the number of attack vectors. However, the Union County computer has a large number of services automatically enabled and running, including SQL Server, Universal Plug and Play, Net Logon, and Remote Registry. Each of these is a potential vector for an attack on Windows and/or WinEDS. The Windows firewall is disabled as well. A port scan of the machine reveals several TCP ports and a dozen UDP ports open.

23.8 One common vector that Internet scammers use to infect PCs with malware is by e-mail attacks. Opening a bogus e-mail attachment can cause a malicious program to run on your computer. The PC we examined is apparently not used for e-mail. But it may be routinely installed on the same network at the voting-machines warehouse as other PCs that are used for e-mail. Viruses can easily hop from machine to machine in the same local network.

It is extremely difficult to truly secure the WinEDS computers

23.9 Sequoia provides to its customers "Computing Infrastructure Hardening Guidelines"⁵⁸ that describe "the necessary steps to assist clients in securing their information systems infrastructure."

23.10 These steps are supposed to show how jurisdictions like Union County can make their Windows computers secure enough to run election management software on. This document describes a very long, very intricate sequence of steps. Some of the steps in the hardening process, like editing the Windows Registry, have the potential to disable the machine. Many of them imply a level of expertise

⁵⁸"Computing Infrastructure Hardening Guidelines," Release Version 2, Sequoia Voting Systems, June 2008.

that would be scarce even in a sophisticated computing environment (e.g., Step 98: “Enable IPsec to Protect Kerberos RSVP Traffic”).

23.11 It would be difficult for a county to comply with these guidelines: they require a high level of sophistication to appreciate and apply consistently and correctly. Even according to Se “System administrators should be highly skilled in the appropriate technologies of Windows administration and security”⁵⁹

23.12 Based on our examination of Union County’s warehouse WinEDS computer, Union County has not even come close to complying with these guidelines, and in fact has left open a variety of security holes. Even according to Sequoia, “This guide is not adequate to even begin to protect the infrastructure if the network is allowed to be connected to external networks.”⁶⁰ But Union County has routinely connected its computer to the Internet, and we found other ways in which the guidelines were not followed.

23.13 Even if a county did fully comply, vulnerabilities would remain. Sequoia says, “ ... This Guideline provides only a portion of the information needed to fully protect the jurisdiction’s election computing infrastructure.”⁶¹

23.14 In addition, following these guidelines to the letter risks disabling some of the necessary functionality of WinEDS or other legitimate election-management applications.

23.15 In conclusion, WinEDS is highly vulnerable to tampering, and there is no simple way to make it invulnerable. The cost of doing so would be prohibitive: it would require the counties to have information security officers with substantial expertise, and would require substantial time and constant vigilance by these officers, and would require substantial training of users (election workers).

23.16 Once a virus or Internet attack has infected either WinEDS computers or AVC Advantage voting machines, it can change votes and selectively disenfranchise voters, as we will explain in Section 24.

23.17 **On WinEDS computers,** malicious software can change ballot definitions (before elections) and change vote data (after elections). These changes will not

⁵⁹ *Id.*, “Step 5” (the document is unpaginated.)

⁶⁰ *Id.*, “Step 5”

⁶¹ *Id.*, “Step 5”

always be detectable by auditing, especially the kind of ballot manipulation that we describe in Section 43.

24 The daughterboard can steal votes or selectively disable voting machines

24.1 In addition to the Z80 computer on the AVC Advantage motherboard, the AVC Advantage version 9.00 contains a second computer, called the daughterboard, which is used in audio voting.

24.2 On AVC Advantage voting machines, fraudulent firmware in the daughterboard

1. can steal the votes of blind voters, or of any voters who use audio voting;
2. can selectively cause voting machines to fail on election day in precincts chosen by the attacker (see Section 24).

24.3 On the version 9 AVC Advantage, the daughterboard does not directly write votes to the Results Cartridge. The motherboard controls the Results Cartridge, and communicates with the daughterboard via messages sent through a cable.⁶² When a voter votes using audio, the daughterboard presents the ballot aurally to the voter, and communicates candidate selections to the motherboard.

24.4 Audio voters use an input device that is connected to the daughterboard, not the motherboard. Thus it is very easy for fraudulent daughterboard firmware to steal the votes of audio voters, simply by conveying different candidate choices to the motherboard. **The votes of disabled voters are even more at risk, on the AVC Advantage, than the votes of those who use the full-face voter panel.**

24.5 In addition, the attacker can cause voting machines to fail in a selected set of precincts. For example, if he disables a dozen or two voting machines in heavily Democratic election districts across the state, then long lines of voters may form, and some voters may leave the polling place before voting. **The significance of doing this attack via a daughterboard virus is that a single person can disable voting machines in hundreds of precincts that he chooses, without ever going near any of those machines.**

⁶² A three-wire RS-232 serial connection.

24.6 To do this, the attacker then programs an audio-ballot virus, replacing the audio-voting software on the daughterboards of all AVC Advantage voting machines in New Jersey.

24.7 On election day, when each machine is turned on, one of the first things that the motherboard does is to send a message to the daughterboard saying (paraphrase) “load the audio ballot,” and the daughterboard normally responds saying (paraphrase) “OK.” However, the fraudulent daughterboard software responds with a different message, either one of the following:

- “Cannot load ballot.” Then the AVC Advantage (motherboard) will display an error message on the Operator Panel, and the election cannot start.
- A specially crafted message that triggers the buffer overrun bug described in Appendix B. This causes the machine to reboot, in an infinite loop, or for as many repetitions as the daughterboard chooses.

In either case, the AVC Advantage will fail to start up on the morning of election day, or will be delayed for a chosen number of minutes.

24.8 The audio-ballot cartridge loaded in the daughterboard contains the name and number of the election district in which the machine will be used. Thus the daughterboard firmware has enough information for an attack on specific precincts. This allows a selective denial of service to specific demographic groups.

24.9 This general means of manipulating elections is well understood. In Ohio in the 2004 Presidential election, “the misallocation of voting machines led to unprecedented long lines that disenfranchised scores, if not hundreds of thousands, of predominantly Minority and Democratic voters.”⁶³ Selective disabling, instead of misallocation, could produce a similar result.

25 No genius required for daughterboard attacks

25.1 The daughterboard virus is a very elementary attack. Virus programming is not much taught in schools, but unfortunately there are many practitioners of it

⁶³ *What went wrong in Ohio: The Conyers Report on the 2004 Presidential Election*, ed. by Anita Miller. Produced at the request of Representative John Conyers, Jr., by the Democratic staff of the House Judiciary Committee, 2005.

nonetheless. There tens of thousands of known computer viruses.⁶⁴

- 25.2 For this particular virus programming, not even a bachelor's-degree level of skill is necessary. The daughterboard is an Intel-486-compatible computer running a DOS operating system—just like the hardware and software of the IBM PCs from about 1990. Millions of PC users gained familiarity with its scripting tools that would be helpful in creating viruses for the AVC Advantage daughterboard.

Reverse-engineering the daughterboard firmware

- 25.3 We found that it is also possible to reverse-engineer the daughterboard firmware.⁶⁵ The daughterboard computer is made by Compulab. We were able to find documentation for this computer on the Internet. Compulab sold this computer for many applications, not just voting machines, and development tools are available for it. Using these development tools, an attacker could extract the firmware and reverse-engineer it. Then, using the results of this analysis, he could devise fraudulent firmware of the kind that we described in Section 24.

26 The motherboard is vulnerable to malicious daughterboard firmware

- 26.1 Election workers prepare ballots for the AVC Advantage on WinEDS computers at the election warehouse, or at the board of elections, or other locations. The electronic ballot definition loaded into the Results Cartridge specifies not only the names of the candidates, but several other options about the election. In preparing a ballot definition for the AVC Advantage, one can choose the option to disable audio voting. The (large-format) Results Cartridge with this option setting is then loaded into the (motherboard of the) of the AVC Advantage. This tells the motherboard not to use the daughterboard.
- 26.2 One might hope that disabling audio voting would make the motherboard immune to harmful effects from a daughterboard virus. Unfortunately, this is not the case. Because of a mistake Sequoia made in programming the motherboard

⁶⁴ "A-Z Listing of Threats and Risks," Symantec, Inc.

http://www.symantec.com/business/security_response/threatexplorer/azlisting.jsp

⁶⁵ Note that in order to perform the ROM-replacement hack that is described in Part I of this report, the attacker does not need to know anything at all about the internals of the daughterboard or its firmware.

firmware, the AVC Advantage is vulnerable even if the ballot definition says not to use audio voting.

26.3 The programming error is known as a “buffer overrun,” and it occurs in the part of the motherboard program that reads input from the daughterboard. A deliberately malicious message from the daughterboard to the motherboard can trigger this bug, causing the Z80 computer on the motherboard to restart.

26.4 When the AVC Advantage is first turned on, the Z80 motherboard computer attempts to communicate with the daughterboard *even if audio voting is disabled*. A malicious message from the daughterboard can cause a restart, and then (as the power-up sequence runs again) to restart again, in an infinite loop. If this occurs in a polling place, the voting machine will not be usable.

26.5 The AVC Advantage can be made immune to daughterboard viruses only by removing the audio kits. This removal is not difficult, and could be done by a county election technician in a few minutes.

26.6 Even so, removing the audio kits is problematic for two reasons. First, it means that the AVC Advantage will not be usable by certain disabled voters without a person to assist them, which means that the Advantage machines would not be HAVA-compliant. Second, it cuts off the upgrade path to a voter-verified paper ballot since Sequoia’s VVPAT printer (in its version 10 AVC Advantage) is connected through the audio kit and not directly to the Z80 motherboard.

27 Security vulnerabilities in WinEDS 3.1

27.1 **Summary: The WinEDS election-management software is known to be insecure, based on studies done by the State of California. In our examination we noticed some of the same weaknesses in WinEDS that were previously reported elsewhere.**

27.2 WinEDS is an “election data system” used for preparing ballot definitions for Sequoia voting machines before elections, and for cumulating results from Sequoia voting machines after elections.

27.3 In the summer of 2007, the Secretary of State of California commissioned a “top-to-bottom review” of the hardware and software of the voting machines then in use in California. A team led by Professor Matt Blaze of the University of Penn-

sylvania examined the source code of several Sequoia products, including WinEDS and the AVC Edge voting machine. Blaze did not study the AVC Advantage, because it is not used in California.

27.4 Blaze’s team found many security vulnerabilities in WinEDS,⁶⁶ such as: “WinEDS creates administrator-level database accounts for all users; ... does not encrypt or authenticate database communication; ... does not remove database access for deactivated users; ... changes account usernames incorrectly; ... does not encrypt password change requests; ... retrieves the default password in the clear on every login; ... places the password suffix in a password entry field; ... displays the password suffix when resetting passwords; ... changes the password for the administrator incorrectly; ... lets any user export data from the database; ... Data Wizard’s import function does not work; ... does not validate a format string read from the database; ... accepts negative vote totals from the database; ... fails to check some function return codes; ... contains many small buffer overflows; ... trusts the list of precincts for which a Results Cartridge claims to report votes ... [and several more]”

27.5 It was not necessary for us to repeat the entire California study of WinEDS, as that study was conducted in a scientific manner by top computer-security experts, and we agree with their conclusions. But we will comment here on a specific insecurity that we observed experimentally in WinEDS that is specifically relevant to the security of the AVC Advantage voting machine. The California study describes it as “Integrity checking of Results Cartridges by WinEDS is not adequate to detect tampering” and “WinEDS fails to check the integrity of election results.” We found that one can change the vote totals and/or audit trail in a Results Cartridge, and WinEDS will not notice anything amiss. We will describe this further in Section 40.

28 Conclusion of Part II

28.1 **AVC Advantage voting machines and WinEDS vote-tabulation software are both severely vulnerable to viruses that can alter election results.** We have demonstrated the feasibility of creating a computer virus that propagates from AVC Advantage machines to each other, and to WinEDS computers. Such a virus can

⁶⁶ “Source Code Review of the Sequoia Voting System” by Matt Blaze, Arel Cordero, Sophie Engle, Chris Karlof, Naveen Sastry, Micah Sherr, Till Stegers, and Ka-Ping Yee. Report commissioned by the Secretary of State of California, released July 20, 2007, http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf, pages 43–56.

carry payloads that modify votes inside the AVC Advantage, and modify election and vote databases in WinEDS. The virus can also be programmed to erase itself from voting machines just before the polls close, so as to avoid detection after the fact.

- 28.2 The WinEDS system is very vulnerable to of cheating and manipulation. An attacker could access the WinEDS computer either physically (inside the voting-machine warehouse) or remotely (from the Internet). Internet attacks are feasible by all the means that ordinary Windows PCs are successfully attacked every day on today's Internet: Internet viruses, websites containing spyware, e-mail phishing, port scanning, and viral propagation through audio-ballot cartridges.

PART III

USER-INTERFACE INACCURACIES AND INSECURITIES CAN DISENFRANCHISE VOTERS

- 28.3 The user interface—the physical and logical design of how the computer interacts with the human user—of the AVC Advantage is flawed in several ways that can: cause votes not to be counted; allow pollworkers to collude with voters to perpetrate vote fraud; and cause other problems.
- 28.4 The consequence, as we demonstrate in the video that accompanies this report, is that voters can be disenfranchised either unintentionally or maliciously.

29 How we vote in New Jersey

- 29.1 In most of New Jersey, the normal mode of voting is as follows.⁶⁷ A voter approaches a table where election-board workers sit with pollbooks. The pollbooks contain the names, addresses, and signatures of all voters registered in this election district (precinct). There are two election-board workers at this table, one from each political party. At the same table there may also be challengers (pollwatchers) representing the candidates or the parties. The voter tells the board worker her name and address, and signs the poll book in the space provided. The voter also signs a “Voting Authority” ticket, which is a piece of paper approximately 4 inches square, taken from a bound pad of 100 tickets. Each ticket has a serial number, as does the stub remaining in the booklet when the ticket is removed at the perforations. In some counties the voter also prints her name on the Voting Authority ticket. The pollworker removes the ticket from the pad and gives it to the voter.
- 29.2 Then the voter waits in line for a voting machine. There may be several voting machines serving the same precinct. When she reaches the front of the line, she hands her ticket to an election-board worker who is standing next to the voting

⁶⁷ Polling place procedures in this sections taken generally from “Official Instructions for the District Board of Elections,” Middlesex County Board of Elections, Revised Jan 2008; Bates Number *Middlesex 1048*; from “Official Instructions for Members of the District Boards of Elections, Presidential Primary Election – February 5, 2008,” Mercer County, Bates number MERCER 004642; and from personal observation of polling place procedures in Mercer County.



Figure 21: A small portion of the voter panel, without the printed paper ballot overlay.

machine. He takes this ticket; in some counties (e.g., Mercer) but not others (e.g., Union), he threads this ticket on a string of tickets attached to the machine.⁶⁸ In this way one can reconstruct exactly which voters voted on each voting machine, and in which order.

29.3 Then the operator (the election-board worker at the voting machine) presses the green “Activate” button on the operator panel of the AVC Advantage voting machine. (If it is a primary election, he presses another button first; see section 56.5.) This causes the machine to be activated, i.e., to be ready to accept votes. The AVC Advantage indicates this in three ways: it emits a barely audible chirping sound for 1/4 second; it turns on the fluorescent light on the inside of the top panel of the machine, illuminating the inside of the booth; and (optionally) it lights a green X next to the name of each contest to be voted. This last option is enabled in Mercer County and disabled in Union County (at least in the February 5, 2008 presidential primary).

29.4 The voter panel, dimensions 38x28 inches, has 42 rows and 12 columns of buttons, each about half-inch square. Just 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. Thus, 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 and the mylar.

⁶⁸ In general, we have found it remarkable how different counties in New Jersey have such different procedures for using the same voting machines. They use a different format of voting authority, they use different ballot-definition options, they have different procedures for announcing in-precinct election results to the public; different procedures for communicating these results to party challengers; different practices with regard to emergency ballots; and so on.

29.5 The Z80 computer in the AVC Advantage can at any time read buttons and illuminate lights. However, the control firmware for the Z80 does not actually interpret these buttons to indicate votes unless the machine has been activated by the operator.

29.6 So, 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.

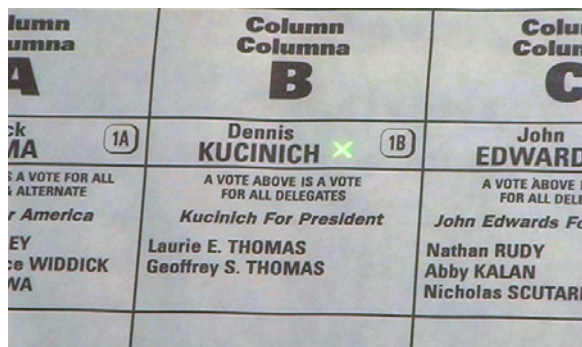


Figure 22: Green X appears by selected candidate

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.

29.7 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.

29.8 Write-in votes are cast by a process described in Section 36.



Figure 23: Cast Vote button

29.9 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.

29.10 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. At the same time the machine emits a chirping sound, and the little LCD display under the voter panel changes to read “VOTE RECORDED THANK YOU”.



Figure 24:
*VOTE
RECORDED
THANK
YOU*

29.11 At a time when 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.⁶⁹

30 AVC Advantage falsely indicates votes are recorded, when they are not

30.1 **Summary: The AVC 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 AVC Advantage is not activated, then it will give three different kinds of visual feedback that the vote is recorded, even though it did actually record the vote at all. Even though no vote is recorded:**

- **the Advantage lights the X by each selected candidate button,**
- **it illuminates the Cast Vote button when pressed,**

⁶⁹This is the behavior when the ballot description programmed into the Results Cartridge specifically prohibits “blank ballots.” This is the setting used by Union County in its 2008 presidential primary election.

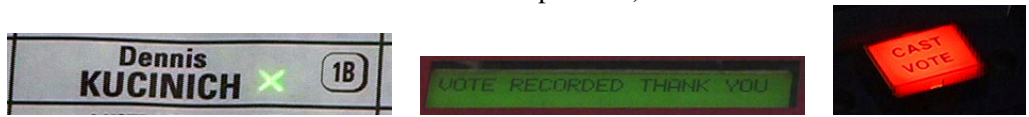
- and it displays “VOTE RECORDED THANK YOU” on the LCD panel visible to the voter.

30.2 This behavior can cause voters to believe that they have voted when in fact they have not voted. The average voter is not intimately familiar with the modes of behavior of the AVC Advantage. If the voter presses a button and a green X lights up by that button, and the voter presses Cast Vote and the Cast Vote button lights up and the LCD display says “VOTE RECORDED,” then the voter can easily believe that her vote has been recorded.

30.3 This behavior, which we found in our examination of the AVC Advantage voting machine, is consistent with experiences reported by voters in certifications filed with the Court.⁷⁰

30.4 This behavior is consistent with the evidence of a 1% lost-vote rate in Pennsauken election district 6, Camden County, where there were 283 Democratic voting-authority stubs but only 279 or 280 votes cast; see Figure 36.

30.5 If the voter enters the booth when the operator has *not* pressed Activate on the Operator Panel, then the AVC Advantage will not count votes. But the AVC Advantage gives three different visual cues that can easily mislead the voter into believing her vote was counted. Even if the operator has not pressed Activate, the AVC Advantage behaves as follows. If the button for a candidate (e.g., “John Smith”) is pressed, then the green X by the candidate’s name is illuminated for about one full second. For one second, the LCD display under the voter panel displays the message “Voter Panel E13” (where in place of E13 there is whatever the row-column letter-number pair corresponding to the button pressed); then the LCD displays “VOTE RECORDED THANK YOU” continuously. (This happens whether or not the Cast Vote button is then pressed.)



30.6 When the machine is in this unactivated state, the Cast Vote button is normally dark. But if pressed, it glows red for about 1 second. A voter may easily interpret this illumination to mean that a vote has been cast—but no vote has been cast.⁷¹

⁷⁰ Certif. of Stephanie Harris, October 1, 2004; Certif. of Glenn Cantor, October 17, 2004

⁷¹ Sequoia is aware of this behavior. According to the AVC Advantage Operator Manual, “The system allows the Voting Switches and the Cast Vote Switch to be tested when the machine is in the

30.7 This design leads to the possibility of vote fraud by election-board workers. The operator simply fails to activate the machine for some voters. Because DRE gives three different types of visual indications that a vote has been cast, many voters will be misled into thinking their votes have been recorded, when they have not.⁷²

30.8 Even though the vast majority of pollworkers are good citizens, with this design flaw there is still the very real danger that a pollworker will inadvertently fail to press the Activate button correctly. In this case, many votes can be lost because of the bad design of the AVC Advantage, which gives extremely misleading feedback through its user interface when not activated.

31 Pressing an option switch deactivates the Advantage so that no votes are recorded

31.1 **Summary: An inadvertent or deliberate button-push by the operator can cause the AVC Advantage not to record votes.**

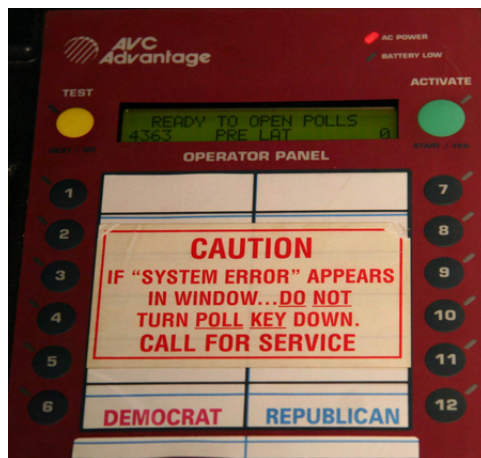


Figure 25: *Operator Panel*

Voter Inactive mode. To test the switch, press it (it will light) and the switch name will be displayed in the Voter Panel LCD.” This description is incomplete: the Operator Manual does not describe the behavior we observed, which is that the LCD display shows “VOTE RECORDED THANK YOU”. Regardless of the original reason for this design, in practice it causes confusion and can disenfranchise voters.

⁷² A corrupt pollworker even has “plausible deniability” in this fraud. If some voters understand that (because the overhead light in the booth is not lit) the machine has not been activated, they will protest. In that case, the election worker can simply apologize for failing to press the Activate button, and activate the machine for this voter.

- 31.2 In a primary election, after the pollworker activates the voting machine by pressing one party's button (e.g., 6-DEM or 12-REP) followed by Activate, he can deactivate the machine by pressing the *other* party's button (12-REP or 6-DEM, respectively).
- 31.3 This behavior leads to inadvertent or deliberate disenfranchisement of voters. First, the pollworker may inadvertently deactivate the machine, and the voter may not notice since the symptoms will be the same as in Section 30.
- 31.4 Second, this behavior permits a vote fraud by a corrupt board worker, or an unintended denial of the franchise by an inexperienced or tired board worker. The operator first presses DEM or REP then Activate, as usual. This causes the chirping noise that signals that the machine is activated to accept votes, as we will describe in Section 32. Then he immediately presses REP or DEM (respectively). *This causes no sound*, but deactivates the machine. The voter's votes will not be recorded.
- 31.5 Unlike the case where a corrupt pollworker deliberately fails to press the Activate button, this method of fraud is even harder for voters or other witnesses to detect, because the AVC Advantage makes its normal vote-Activation chirping noise.

32 Sound on activation is not an effective signal for voter, pollworkers, or witnesses to determine when votes are cast

- 32.1 **Summary: The AVC Advantage makes a sound when the machine is activated for a voter to vote. It makes the same sound when the voter presses the Cast Vote button. This sound is 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). Furthermore, using the same sound for both signals invites confusion and fraud.**
- 32.2 One method of vote fraud that is over a century old is this: The voter puts more than one ballot into the ballot box; or a pollworker puts ballots into the ballot box

when no voter is near. Or, with a voting machine, the pollworker allows the voter to vote several times; or the pollworker votes several times when no voter is near.

32.3 To defend against this kind of fraud, ballot boxes for paper ballots are put in full view of many witnesses, for example, in view of the pollworkers and pollwatchers sitting at the registration desk. Some ballot boxes are equipped with a lever that opens the slot to accept ballots; whenever this lever is pulled, a bell rings. Thus, everyone in the room is aware of every time a ballot is inserted into the ballot box.

32.4 Similarly, the lever-action machines used in New Jersey throughout most of the 20th century make a fairly loud and prolonged noise when the voter switches the “cast vote” lever. In addition, the machines used from 1961 to 2003 in Mercer County automatically closed a curtain when the machine was activated, and opened this curtain when the voter switched the “cast vote” lever. This was a visual indicator to anyone in sight.

32.5 The AVC Advantage emits a chirping sound when the operator activates the machine for voting, and the same chirping sound when the voter presses Cast Vote.



If this sound were effective, it could prevent collusion between the voter and the operator, of the kind where the operator repeatedly activates the machine and the voter repeatedly votes. The sound, if effective, would also prevent the operator, at times when no voter is near, from activating the machine and then voting himself.

32.6 Pollworkers and party challengers sitting at the sign-in table should be vigilant to out-of-the-ordinary activity in the polling place. But the AVC Advantage provides no visual signal (visible from that distance) that a vote has been cast. And its aural signal (the chirping noise) is not loud enough to be reliably heard from several feet away, where the pollworkers and challengers are sitting. This is especially true in polling places that are large rooms (such as school gymnasiums), sometimes with more than one election district (each with two Advantage machines), with difficult acoustics, where there will be a cacophony of chirps as several voting machines are activated and voted. Since 2004, we have heard from many voters that they did not hear the chirping sound.

32.7 Furthermore, exactly the same chirping sound is made for the Activate function and the Cast Vote function. This needlessly causes additional confusion, especially

when there are several AVC Advantage machines in the same room.

32.8 Finally, the Advantage makes no sound at all if it is deactivated, accidentally or intentionally, by the pollworker.

32.9 In summary, the AVC Advantage's inadequate aural signals cause confusion, prevent the detection of fraud, and permit fraud.

33 The AVC Advantage's lack of feedback leads voters to undervote

33.1 **Summary: The full-face buttons-and-lights design of the AVC Advantage does not give adequate feedback to a voter who may have forgotten to vote in some of the contests on the ballot.**

33.2 Computer scientists study user interface design, so that their computer programs can better "understand" and carry out the intent of the user. User-interface issues are also important in voting machines and ballot design, where both computer scientists and social scientists study these issues.

33.3 Professor David Kimball, a political scientist, recently studied the undervote rates in the 2006 New Jersey general election.⁷³ He found that the AVC advantage has a very high undervote rate on public questions, about 29%. He found that the undervote rate increased for voters with lower incomes.

33.4 In our examination, we found several reasons that can explain the high undervote rate of the AVC Advantage.

33.5 The AVC Advantage does not have a video screen for communication to the voter, to alert the voter that he has forgotten to vote in certain contests. Thus, the voter may be inadvertently disenfranchised.

33.6 In our examination of the AVC Advantage we have studied all the mechanisms by which Sequoia and election officials attempt to remind voters not to undervote. In doing so they attempt to overcome the inherent inexpressiveness of the AVC Advantage's user interface. In our opinion these mechanisms do not succeed. We describe this in detail in Appendix I.

⁷³ "Voting Equipment and Residual Votes on Ballot Initiatives: The 2006 Election in New Jersey." David Kimball, University of Missouri-St. Louis, February 28, 2007

34 Voter can't tell which primary is activated

34.1 **Summary: The AVC Advantage gives inadequate information to voters in primary elections about which ballot is activated. This feature of the machine may interact with the primary-election “option-switch” bug to disenfranchise voters.**

34.2 In a primary election, the voter hands to the pollworker a Voting Authority ticket that informs the pollworker which party's primary the voter is eligible to vote in.

34.3 Inside the booth, *there is no indication*, on the full-face preprinted ballot, of which party's primary is activated.⁷⁴ Therefore, the voter is presented with two complete primary ballots on the same panel, the Democratic and the Republican primary, with no visual prompt indicating which one to vote in.

34.4 This is particularly a problem in connection with the option-switch bug (see Section 56). In that situation (which occurred on 37 machines in 8 counties on February 5, 2008), the computer program in the AVC Advantage presented the wrong party's primary ballot to the voter. The lack of visual indication of which primary was enabled may have contributed to the confusion, on the part of both voters and pollworkers, and thus contributed to the disenfranchisement of those voters.

35 Pollworker can see who the voter votes for

35.1 The purpose of a privacy curtain, and other technological measures to protect the secret ballot, is to protect voters from being coerced to vote a certain way, and to prevent vote buying. The AVC Advantage does not provide effective voter privacy.

35.2 In normal use of the AVC Advantage machine,⁷⁵ an election-board worker presses a button on the Operator Panel to activate the machine for each voter. The Operator Panel is on the side of the machine, towards the rear.

⁷⁴ From our examination of Union County's AVC Advantage machines as they were set up for the Presidential Primary election of February 5, 2008.

⁷⁵ unless the voter-smart-card activation option is installed, which it is not in New Jersey. The AVC Edge voting machine also uses smart-card activation. Studies commissioned by California and Ohio found security vulnerabilities associated with smart-card activation, such as the possibility that a voter could use a hacked smart card to vote repeatedly.



Figure 26: *Peeking through the slot at the position of the voter's finger. Here, the pollworker can see that the voter is voting for a candidate at the left side of the full-face ballot. This shows more clearly in the video that accompanies this report.*

35.3 In principle, the voter has privacy in the act of voting because the AVC Advantage has side doors and a top panel that unfold to form a voting booth. A curtain shields the voter from the rear.

35.4 However, there is an open slot on each side where the top panel joins the back of the machine. These slots are 8 inches by 1/4 inch, at each side of the machine, about 54 inches from the floor. A poll worker of average height (anyone at least 64 inches tall) can easily see through a slot to where the voter's finger is pressing the buttons to select candidates. This can be done by standing in a normal position and attitude at the Operator Panel.

35.5 Looking through the slot, it is fairly easy to tell the horizontal position of the voter's finger, i.e., which column is the candidate voted for. It is somewhat more difficult to tell the vertical position, i.e., which row the candidate is in. Since, in New Jersey, each contest is laid out as one horizontal row,

1. Where there are few races on the ballot, such as the presidential primary of February 5, 2008, the poll worker can tell how each voter voted.
2. If the voter votes the contests from top to bottom (as most voters presumably do), it's often possible to tell whether they're voting a straight party ticket, and for which party.

35.6 A corrupt pollworker can combine this fraud with the one we describe in Section 31: he can deactivate the AVC Advantage as soon as he sees the voter's finger aiming for a candidate that the pollworker does not favor.

36 Can't undo write-in vote, in violation of FEC guidelines

36.1 **Summary: A voter cannot undo a write-in vote after pushing ENTER but before casting a vote. The consequence of this user-interface problem is that the AVC Advantage may fail to record the intent of the voter. If the voter discovers, after entering a write-in vote, that she has placed this write-in in the wrong contest on the ballot, there is no way for her to correct this contest and vote her true intent in this contest.**

36.2 The FEC guidelines for voting machines: section C.8.e says “A means for correcting a vote response should be readily available. For non-paper based systems, this should be built into the design of the system.”⁷⁶

36.3 On the AVC Advantage, write-in votes are cast as follows. For some contest, the voter selects a “candidate” marked “Personal choice.” Then she uses an alphabetic keyboard below the voter panel to type a name, with feedback from an LCD display below the voter panel. After typing the letters, she presses “ENTER” on this keyboard.

36.4 While the machine is activated, a voter can select a candidate by pressing the button for that candidate. If she changes her mind, she can deselect the candidate by pressing the button again. This causes the X by that candidate to go out, and she can now select a different candidate for that contest.

36.5 However, if the voter has selected “Personal choice” for a given contest, then after pressing “ENTER”, it is not possible to deselect the “Personal choice” selection, or to change the write-in vote. This appears to be a violation of the FEC guidelines.

37 Procedures for fleeing voter leave opportunities for violating the privacy or integrity of the ballot

37.1 **Summary: If a voter leaves the booth without pressing Cast Vote on the AVC Advantage, then the procedure for pollworkers to follow is very clumsy. The procedure is difficult to follow while respecting the voter's privacy, and leaves opportunities for changing votes.**

⁷⁶ VVS 2002, Appendix C, Section C.8, paragraph e.

37.2 This issue slightly impairs the accuracy of the AVC Advantage in recording the voter's intent, and slightly impairs the security against pollworker manipulation. However, we judge this issue to be of somewhat less import than the others that we discuss in the body of this Report. Therefore we have relegated a discussion of this issue to Appendix J.

38 Conclusion of Part III

38.1 The full-face buttons-and-lights design of the AVC Advantage user interface has an inherent design weakness: it is unable to give certain kinds of feedback to the voter. In particular, really effective feedback about undervotes is difficult to achieve, and there is an inherent possibility for confusion about whether the machine is activated.

38.2 However, even given that inherent limitation, Sequoia has made certain avoidable design mistakes that greatly increase the risk that the intent of the voter will not be recorded. The behavior of the machine when not activated is inexcusable: pushing a button lights the green Xs even when no vote is being recorded. The machine is too easily deactivated either inadvertently or surreptitiously before the voter has a chance to vote. And there is a voter-privacy violation that could have been avoided with a better physical design.

38.3 These flaws have the effect of disenfranchising voters, either inadvertently (with no malicious intent on the part of pollworkers) or on purpose. Thus, they compromise both the accuracy and the security of the AVC Advantage.

PART IV

DESIGN ERRORS AND PROGRAMMING BUGS MAKE THE AVC ADVANTAGE INSECURE

38.4 The attacks that we describe in Parts I and II are so deadly because they succeed even if every election worker is honest and because they are undetectable by audits.

38.5 In our examination of the source code, we found many other design flaws that an attacker could exploit in order to steal votes. In contrast to the attacks described above, the vulnerabilities that we will describe in this section: may require cooperation from a dishonest election worker; could in principle be detected by well designed audit methods; or could compromise “only” the privacy of the ballot instead of stealing votes.

39 Vote data is not electronically authenticated, making it vulnerable to tampering

39.1 **Summary: In its promotional literature, Sequoia claims the Advantage is using “cryptographic” means to guarantee authenticity, integrity and confidentiality of votes. This is simply not true.**

39.2 Sequoia’s promotional literature⁷⁷ makes many claims about the use of “cryptographic signatures” to validate the integrity of vote data. Indeed the Source Code has many mechanisms that purport to ensure the authenticity, integrity and confidentiality of votes. **The mechanisms that Sequoia uses are completely inadequate for this purpose.**

39.3 “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. We will use this standard term of art as it is used by computer scientists, and as specified by the National Institute of

⁷⁷“AVC Advantage Security Overview,” Sequoia Voting Systems, Inc., 2004.

Standards and Technology.⁷⁸

- 39.4 A digital signature *algorithm* authenticates a data file by applying the *signer's* secret key to produce a *signature*. The signature is a short string of just a few dozen characters. Only someone in possession of the key, someone who intends to authenticate this data, can produce this signature string. Therefore the signature string *proves* the authentication of this data.
- 39.5 One could imagine using digital signatures to authenticate votes coming from a voting machine, in such a way that only this voting machine could have produced this vote data. **But Sequoia did not design the AVC Advantage to do this.**
In our examination of Sequoia's Source Code, we found that,
- 39.6
- **There is no use of digital signatures (or “cryptographic signatures”) at all.**⁷⁹ There is not a single piece of data or firmware that is protected against deliberate fraud by the use of digital signatures.
- 39.7
- Hash functions are weaker than digital signatures—they can detect *accidental* data changes but not deliberate falsification. **In the AVC Advantage, no hash functions at all are used to protect actual vote data.** The ballot-image file and the candidate totals stored in Results Cartridges and in internal memory are not protected by any kind of overall hash function or checksum. This makes it very easy for an attacker to change ballot images and candidates totals in Results cartridges.⁸⁰
- 39.8
- **Some of the hash functions used are even too weak to protect reliably against inadvertent data modification.** Some kinds of data in the AVC Advantage are protected by “CRC” (cyclic redundancy check) hash functions, which are adequate to catch inadvertent changes to data. But other kinds of data, such as the contents of ROMs, are protected by a naive “checksum” computed by simply adding up the bytes. This method has been obsolete for forty years,⁸¹ since it fails to catch even inadvertent errors reliably.

⁷⁸ *Digital Signature Standard*, Federal Information Processing Standards, Publication 186-2, National Institute of Standards and Technology, January 27, 2000.

⁷⁹ There is some use of SHA-1 in Technician Cartridges, but the Technician Cartridge feature is disabled.

⁸⁰ Each individual ballot image has a checksum. This is a much weaker defense against fraudulent or accidental change than using an overall hash signature on the whole file. This is because individual ballot images can be duplicated, checksum and all, without detection.

⁸¹ Peterson, W. W. and Brown, D. T. (January 1961). “Cyclic Codes for Error Detection”, Proceedings of the IRE 49:228.

39.9 In conclusion, any “authentication” that the AVC Advantage performs is useless against deliberate fraud. In all cases where we examined an attack on vote data or firmware, either there was no authentication mechanism or we were easily able to defeat whatever mechanism was present.

40 Manipulating Results Cartridges

40.1 **Summary: Results Cartridges are used for transmitting the ballot definition to the AVC Advantage, and transmitting the election results from the AVC Advantage to a WinEDS computer. It is easy to physically and electronically manipulate Results Cartridges, either to turn them into other types of cartridges, or to change the votes in them. Results cartridges are *very insecure* against tampering with the votes stored inside.**

40.2 The AVC advantage uses data cartridges, called “Results Cartridges,” which are about the size of a VHS tape. The data in the cartridge is organized into a simple file system. There is no protection (either via hardware or via cryptography) against reading and writing the data in the cartridge.

40.3 The cartridge contains the ballot definition as well as the votes cast. At the close of the polls, the Results Cartridge is normally removed from the AVC Advantage by a pollworker. Then the cartridge is put into a zipper-bag, sealed, and sent back to election officials for tabulating in WinEDS.

40.4 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.

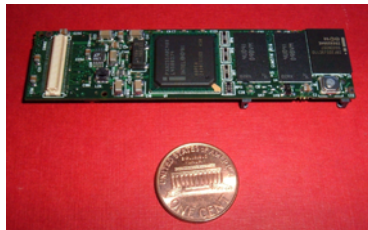


Figure 27: *Tiny computer, sold for \$99 by gumstix.com, that could be the “brains” of a cigarette-pack size device to alter the contents of Results Cartridges*

40.5 It is possible to make a simple device that changes the votes in a Results Cartridge. This device could be as small as a package of cigarettes. One would plug



Figure 28: *Nonfunctional mock-up of a device, in a cigarette pack, to alter the contents of Results Cartridges.*

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.



Figure 29: *(nonfunctional mock-up)*

40.6 This could be done at any of the following times:

- 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 (stowing the curtains, attending to the other AVC Advantage in the same precinct, etc.).
- By a person who transports the cartridge to county election officials for tabulation.
- By a person who removes the cartridge from the bag before tabulating in WinEDS.

40.7 As we explained above in Section 39, no means of cryptographic signature or authentication protects the vote data in the Results Cartridge from modification. Sequoia claims, in its AVC Advantage Security Overview,

“After polls are closed, the AVC 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.”⁸²

However, this is not true, for two different reasons:

1. Sequoia does not use true cryptographic signatures. 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*. The AVC [Advantage] calculates a checksum that does not have this property; that is, anyone (such as the WinEDS program) that can check the authenticity of a Results Cartridge also has enough information to forge a fake one. This information is identical in all AVC Advantage machines and in all WinEDS installations, so that anyone with access to a single one of these has the ability to forge a Results Cartridge as if it came from any other.
2. The checksum protects the ballot definition, *but no checksum at all protects the election results!* Therefore, candidate totals can be changed without knowing anything about checksums.

40.8 In summary, once a Results Cartridge leaves the voting machine, it is *immediately* susceptible to modification of vote data.

41 Some NJ County Clerks use the less trustworthy source of data in tabulating official election results

41.1 **Summary: Sometimes the AVC Advantage prints different vote totals on its printer than are stored electronically in its Results Cartridge. The paper reports are less susceptible to fraud and error (although they are still susceptible). In case of disagreement, County Clerks should rely on the paper printout in their tabulation of official election results. However, some Clerks unwisely use the electronic data instead of the printed data.**

41.2 Sections 40, 46, 47, 48 explain how the data in Results Cartridges are vulnerable to fraudulent manipulation. Therefore the paper results-report printouts made

⁸²AVC Advantage Security Overview, Sequoia Voting Systems, page 9

by the AVC Advantage, immediately when the polls close, in the presence of witnesses, and signed by those witnesses, is more trustworthy. Section 57 explains how, when the AVC Advantage loses votes because of hardware failure, the paper results-report printouts are more likely to be accurate than the Results Cartridges.

41.3 Even the paper results-report can be fraudulently changed by election-stealing firmware inside the voting machines, as described in Parts I and II of this report. Here we are talking about sources of fraud and error other than that kind of hacking.

41.4 When there is a disagreement between the paper and the Results Cartridge, the paper record should be considered more reliable, in the absence of specific other evidence. However, unfortunately, election officials often ignore the paper records entirely, and rely entirely on the electronic data.

41.5 This is true even in a case where there is a specific “red flag” indicating the unreliability of the data in the Results Cartridge. In Camden County, when a Results Cartridge failed in a way that we describe in Section 57, the County Clerk apparently used data that was extracted (by other than the usual means) from this partially failed cartridge, *even though this data disagreed with the paper printout from the machine signed by witnesses.*

41.6 An extremely conscientious County Clerk will review the paper records to compare them with the electronically transmitted numbers. This is what Joanne Rajoppi, Clerk of Union County, did in February 2008, which led her to discover the party-affiliation error made by AVC Advantage machines (described in Section 56).

41.7 However, to the extent that Ms. Rajoppi’s exemplary practice is not widespread among the County Clerks of New Jersey, errors and fraud in Results Cartridges will influence official election results.

42 The Advantage can print a paper report from a fraudulent Results Cartridge

42.1 Suppose someone fraudulently changes votes in a Results Cartridge, using the method we describe in Section 40. He can then change the paper results-report printout as well, so that no discrepancy is noticed, using the following method.

42.2 We have found that one can reinsert the Results Cartridge into the voting machine and print a phony results report from it. To do this, one inserts the Results Cartridge into the Auxiliary report of the AVC Advantage. Then one selects from a menu on the Operator Panel to “print report from Results Cartridge.”

42.3 A dishonest pollworker could perform this manipulation. He would print an extra fraudulent Results Report, which would then match exactly the (fraudulent) contents of the Results Cartridge. If the other pollworkers are not paying attention, they would not notice the extra buttons he pressed on the voting machine to accomplish this.

42.4 One might think that an alert and honest pollworker might notice the extra manipulation of the voting machine performed by the dishonest one. However, some pollworkers have less experience with exactly how the machine works,⁸³ and what technical procedures are supposed to occur at the closing of the polls.

42.5 Also, there are other distractions while the polls are being closed. In fact, Middlesex county explicitly recommends that pollworkers perform other tasks at the very time the results report is printing! Middlesex’s pollworker manual instructs, “While the results are printing, begin closing the front of the machine. Remove privacy curtain and return it to the storage tube. Unlatch the top privacy panel and fold down. Fold in the side privacy panels, lock the door with the yellow key, and remove the key.”⁸⁴

42.6 Furthermore, pollworkers print several copies of the results report.⁸⁵ It would thus be possible for a pollworker to make the original, legitimate copy disappear and have all the witnesses sign the report printed from a manipulated cartridge.

43 One can confuse the AVC Advantage with a fraudulent ballot definition that yields two votes for one button

43.1 A cleverly designed ballot definition can cause a single button on the voter

⁸³Based on Appel’s observations of pollworkers in two different precincts as they closed the polls in November 2004 in Princeton, NJ. In one precinct the head pollworker was clearly very experienced and knew exactly what she was doing; in the other, the pollworkers made some procedural mistakes.

⁸⁴ From page 34 of “Official Instructions for the District Board of Elections,” Middlesex County Board of Elections, Revised Jan 2008; Bates Number *Middlesex 1048*.

⁸⁵ “When all reports are printed, if more are needed, push the BLUE PRINT MORE BUTTON. Note: You MUST use the Blue Print More Button to produce another copy of the Results Tape to post for the public to see.” —*Id.*

panel to add two votes for a candidate, or to have an invisible button add extra votes. The trick is to abuse the “endorsement” feature of the AVC Advantage. Even though “endorsement” is not practiced in New Jersey, that does not prevent an attacker from taking advantage of its existence in the AVC Advantage.

43.2 Endorsement is used principally in New York, where (for example) the same candidate can run on the Democratic Party ticket and on the Liberal Party ticket. Thus, the candidate appears twice on the ballot, once in each party column.

43.3 In the electronic format of 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 fact, this ballot-definition data structure is so complex that it is very vulnerable to fraudulent manipulation. **However, the AVC Advantage does not thoroughly check the ballot-definition data structure to make sure it is well-formed.** For example, the ballot definition can have candidates in nonexistent contests, and the voting machine will not notice.

43.4 The AVC Advantage printer permits special printer control characters such as “cancel printing of this entire line.” The firmware in the AVC Advantage unwisely permits these control characters to be present in candidate names, contest names, and voting-machine serial numbers. In combination with the complex ballot definition structure, this leads to two different security vulnerabilities, as we will explain here and in Section 46.

43.5 By manipulating these data structures, one can design a ballot definition that plays the following trick: it puts John Smith on the ballot at two different locations, one in the expected place, and one invisible. It is easy to make a button invisible, since all the buttons are behind the paper overlay on the voter panel, and they



Figure 30: *Buttons behind paper ballot on voter panel*

become “visible” only by the fact that the printed paper has an indication of which button-positions are meant to be pressed. The tricky ballot definition also needs

to manipulate the way the results report is printed, which can be done with printer control codes that suppress printing of lines containing the duplicate candidate names.⁸⁶

43.6 Whenever a new ballot definition is fed into *any* voting machine, the machine should check the ballot definition for “sanity” and well-formedness. Ballots structured in ways unanticipated by the programmer can lead to hacks, of which the two-votes-for-one that we describe here is just one example.

43.7 Even though the AVC Advantage does have some checks for ballot sanity, we found others that were missing. The complexity of the ballot definition format in the AVC Advantage leaves it potentially vulnerable to this kind of attack.

43.8 **Conclusion.** The AVC Advantage’s failure to perform sufficient “sanity checks” on the the ballot definition constitutes a security vulnerability.

44 Results Cartridges can be easily converted into other kinds of cartridges and used for fraud

44.1 Sequoia makes many types of cartridges that have the same size, shape, and appearance to Results Cartridges: Consolidation Cartridges, Technician Cartridges, Program Cartridges, Simulation Cartridges, Audit-trail Transfer Cartridges, and so on. These cartridges were designed in the early 1980s before flash memory was invented. They have (typically) 96 kilobytes of static RAM, and two AA batteries to maintain enough power to preserve the data in the RAM.

44.2 We found that it is easy to convert a Results Cartridge into any of the other types. We cut certain traces (printed wires) on the circuit board of the Results

⁸⁶ The fraudulent ballot design is constructed with the following technical details.

- 1) Build multiple candidates as endorsement ring.
- 2) Leave last of the instances in the ring to be part of the race one wants to manipulate.
- 3) Change the other instances to be members of a nonexistent race (which omits those from reports).
- 4) Make the other instances to point to switches already in use (for example in other races).
- 5) Manipulate the party description field to contain combination control characters (like “cancel line”) to omit the extra lines on report caused by endorsement reporting.

Then, if a voter pushes the candidate’s button, the candidate gets a vote—but also one can bind the “invisible” button to award a second vote. The “invisible” button can even be made the same button as another legitimate candidate in the race. For example gubernatorial candidate A can be bound to get a second vote from every voter who votes for state-senate candidate C. This will not affect the votes tallied in the senatorial race; it will just generate extra votes for Governor.

Cartridge, and installed a 24-pin header for repluggable jumpers. This took about 15 minutes. Depending on the pattern of jumpers, we were able to make any of the different cartridge types.

44.3 In the next few sections we will describe ways to fraudulently manipulate elections using these other types of cartridges.

45 Early Voting Cartridges permit fraud in States that use them

45.1 **Summary: The AVC Advantage contains an Early Voting feature. This mechanism is insecure, and subject to manipulation and fraud. New Jersey does not currently permit Early Voting on AVC Advantage machines. Because of these insecurities, New Jersey should not adopt Early Voting on the AVC Advantage.**

45.2 The AVC Advantage permits early voting, as follows. On each of the early voting days, a pollworker unfolds the voting machine and inserts an Early Voting cartridge. Voters cast their votes. At the end of the day, the pollworker removes the Early Voting cartridge. Thus, the cartridge contains several sessions of early voting data.

45.3 States that use Early Voting are subject to many severe vulnerabilities in this process, especially the following: In contrast to the process at the end of an ordinary election day, where a “results report” is printed out by the voting machine and witnessed, no results report is printed at the end of each early voting session. This results report, when it exists, can serve as an important check to detect manipulation of cartridges after they leave the voting machine. If an attacker changed the data in an Early Voting cartridge, no one could detect it.

46 Manipulating Consolidation Cartridges

46.1 **Summary: There is a mechanism for consolidating the votes of several AVC Advantages in a precinct into one cartridge. This mechanism is insecure, and subject to manipulation and fraud. To the extent that counties in New Jersey do use this mechanism, they open vulnerabilities for fraud.**

46.2 The AVC Advantage has the ability to do polling-site consolidation. That is, if there are several AVC Advantage machines in the same precinct, the totals from these machines can be accumulated at the polling place, immediately after the close

of the polls, so that only one set of Candidate Totals is reported for the whole precinct.

46.3 On the AVC Advantage the process uses a Consolidation Cartridge that looks just like a large-format Results Cartridge. (In fact, we easily converted one of Appel's own Results Cartridges to a Consolidation Cartridge by a simple rewiring.) After the close of the polls, a blank Consolidation Cartridge is inserted into the Auxiliary port of the first AVC Advantage in the precinct. This first voting machine writes its candidate totals to the cartridge.⁸⁷ Then the cartridge is removed, and inserted into the next AVC Advantage. This second voting machine *adds* its candidate totals to the cartridge. As the cartridge is inserted into each subsequent machine, the totals are similarly accumulated.

46.4 There are two ways an attacker could manipulate this process to steal votes:

1. Start with a Consolidation Cartridge that is not blank, but contains *negative votes* for candidate A and an equal number of *positive votes* for candidate B. Then, when legitimate votes are added from the voting machines, the negative votes will cancel out some of the legitimate votes for candidate A, leaving only positive totals. Because of the balance of negative and positive votes, all the totals will be consistent with the public counters, i.e., with the number of voters who voted on the machines. When the Consolidation Cartridge is inserted into WinEDS, the WinEDS system will read the candidate totals (and will not check the ballot images, even if they are present).⁸⁸

One might think that the voting machine would reject a Consolidation Cartridge with negative votes. But in fact it does not. This is very dangerous. The Consolidation fraud works by adding votes. If one can only add positive votes, then one risks being detected, because the vote total will exceed the number of voters. But if one can add negative votes to one candidate and an equal number of positive votes to another, then one can avoid detection.

2. One could use a handheld device, as described in Section 40.5, to change votes in the Consolidation Cartridge, just as in a Results Cartridge.

⁸⁷Optionally, depending on a setting in the ballot definition, the voters' ballot images are also copied to the Consolidation Cartridge.

⁸⁸To complete this attack, it is useful to suppress from the printer paper "consolidation report" any mention of the voting-machine serial number from which the fraudulent negative-and-positive votes were loaded into the Consolidation Cartridge. This can be done by putting a suppress-print-line control character into the ASCII string that holds the serial number of this voting machine, as we describe in ¶43.4. Of course, this "voting machine," used to prepare the fraudulent Consolidation Cartridge, need not be a real AVC Advantage; and ordinary personal computer or a cigarette-pack-sized handheld device will do.

46.5 In summary, Consolidation Cartridges allow many opportunities for stealing votes.

47 Wireless access to Results Cartridges opens avenues to manipulation

47.1 **Summary: Inexpensive and readily available technology would permit an attacker to make a fake audio-ballot cartridge that can be radio-controlled from several feet away. This is bad for the AVC Advantage 9.00, and disastrous for the version 10 Advantage.**

47.2 As discussed in Section 19.4, the audio-ballot cartridge of the Sequoia AVC Advantage 9.00 is a PCMCIA card that plugs into the daughterboard, also known as the “audio kit processor.” The AVC Advantage model 10 uses the same hardware architecture, but on that machine the daughterboard is called the “main processor” and the PCMCIA card is called the “Results Cartridge.”

47.3 This PCMCIA card is used for audio ballot files (on the version 9 machine) and for ballot definitions, audit trails, and election results (on the version 10 machine). But it is also used for loading software updates into the daughterboard processor.

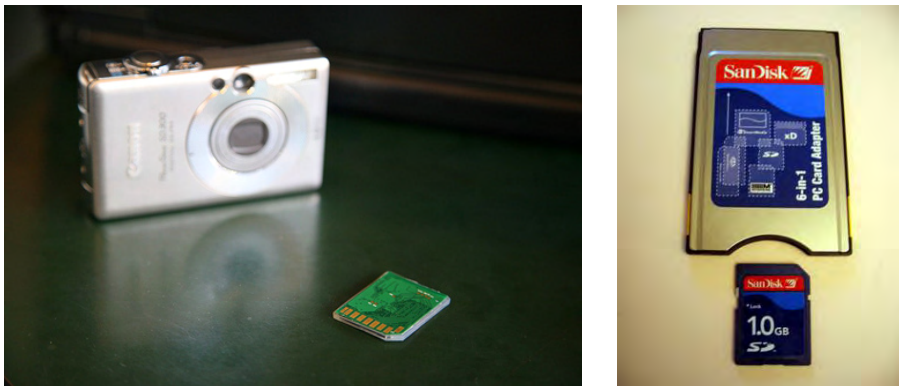


Figure 31: At left, Eye-fi card designed for digital cameras. At right, adapter that converts Eye-fi card (or any SD-compatible camera card) to PCMCIA format. Photo at left by Scott Beale, laughingsquid.com, Creative Commons license: attribution / noncommercial / no-derivative-works. Photo at right from www.universmobile.net

47.4 Although Sequoia's audio-ballot cartridge is the size of a credit card, inside it is actually a much smaller "Compact Flash" card of the kind that plugs into digital cameras. Sequoia encases the cartridge in a plastic casing that obscures this arrangement. When I plug the audio-ballot cartridge into the PCMCIA card slot of a Microsoft Windows computer, the card identifies itself as SanDisk SDCFJ-32 or SDCFJ-64 Compact Flash.⁸⁹

47.5 One can easily purchase⁹⁰ a Wifi-enabled compact flash card, brand-name "Eye-Fi." One uses this card in a digital camera, in place of the standard SD flash-memory card. Then one can use a Wifi-enabled computer or cell-phone to download/upload picture files from/to the digital camera. To enable compatibility with existing digital-camera operating systems, the SD card presents (to the slot it's plugged into) the appearance of a perfectly ordinary SD card. However, files from the SD card can be read or written remotely even while the digital camera is in operation, and the camera is completely unaware of this activity.

47.6 SD-format flash memory cards are much smaller than PCMCIA cards, and an SD-to-PCMCIA adapter is readily available. It would be very easy to make a fake Sequoia PCMCIA cartridge that contains a radio-enabled SD card, but looks identical to the real thing.

47.7 Therefore it is easily possible, with very little technical skill, to produce fraudulent Audio Ballot Cartridges (for the Advantage model 9) or Results Cartridges (for the model 10) that can be modified remotely from a distance of several feet from the voting machine. The attacker can be a pollwatcher or election-board worker (if he wishes to perform the attack before the polls are opened) or a voter (if he wishes to perform the attack while the polls are opened).

47.8 This mechanism can be used to modify audio-ballot files on the version 9 machine, so that disabled voters are presented with a fraudulent set of choices. This mechanism can be used to modify ballot-definition files and election-results files on the version 10 machine.

47.9 This mechanism can also be used to entirely replace the program in the daughterboard with a fraudulent program that steals votes. See Section 19.

⁸⁹The capacity of the card is variously 32 megabytes or 64 megabytes.

⁹⁰ www.eye.fi, \$79.99

Wireless access to version 9 results cartridge

- 47.10 The large-format Results Cartridge of the version 9 AVC Advantage does not contain a Compact Flash; instead it contains (typically) 96 KB of static RAM, with two AA batteries to power the RAM continuously so that it does not forget the contents.
- 47.11 The cartridge is 7x4x1 inches in dimensions, with room to spare inside the (opaque plastic) case. It would be a simple exercise, suitable for an undergraduate student of electrical engineering or computer science, to design a fraudulent Results Cartridge containing a Wifi-enabled compact flash. This would permit manipulation of ballot data and election results, either while the Results Cartridge is installed in the AVC Advantage or after its removal.

48 Fraudulent intelligent Results Cartridges could steal votes

- 48.1 **Summary: Another way to steal votes in the AVC Advantage is to make a “smart” Results Cartridge that fools the motherboard computer.**
- 48.2 A standard Sequoia Results Cartridge (the large-format cartridge from the version 9 machine) contains 96 KB of static RAM, with two AA batteries to power the RAM continuously so that it does not forget the contents, and 8 bits, set by hard-wired jumpers, to indicate the cartridge type (4 bits) and the memory size (4 bits). When this cartridge is plugged into the AVC Advantage motherboard through the Results port, the Z80 accesses the memory by doing input/output instructions.
- 48.3 It would be a simple exercise, suitable for an undergraduate student of electrical engineering or computer science, to design a fraudulent Results Cartridge containing a computer. Such a computer could easily simulate a normal Results Cartridge when “talking to” the Z80 or to the WinEDS system that collects election results from it. However, the program in this cartridge-resident computer could easily manipulate election results or ballot definitions.
- 48.4 This attack does not require any access to the internal circuitry of the AVC Advantage voting machine. To replace a Results Cartridge when the machine is turned off, at most requires picking the lock and defeating a seal. See Section 10. However, election insiders can insert fraudulent intelligent Results Cartridges into the election process without any access to the AVC Advantage voting machine at all. This can be done when Results Cartridges are being programmed with ballot

definitions, when they are being read to extract results after an election, when they are stored in warehouses, when they are being manufactured, or at other points.

48.5 These fraudulent cartridges are not easily detected by pollworkers, because they have the same appearance as ordinary cartridges.

48.6 The computer program in such a cartridge can be programmed to steal votes in election after election with no human intervention. The Results Cartridge contains enough ballot data to tell which candidates are Republican and which are Democratic, what offices they are running for, and the date of the election. Thus it can be programmed to generically steal a few votes, only in presidential elections (for example), from one party's candidate to the other.

48.7 Unlike the ROM replacement described in Part I of this report, the vote-switching Results Cartridges can be detected by a careful audit of the paper results printouts. The paper results printout is (usually) printed from the AVC Advantage's internal memory, which would not be affected by vote-switching in the cartridge. Therefore this attack is most dangerous when County Clerks are inattentive or when political parties have insufficient resources to send pollwatchers to witness and record copies of the printed results, and compare them with published precinct-by-precinct result totals.

48.8 Designing such cartridges would require several weeks of effort by someone with bachelor's-level training in electrical engineering. Once designed, they could be produced in quantity.

49 Electronically stored "ballot images" compromise privacy of the ballot

49.1 **Summary: In its internal memory and Results Cartridges, the AVC Advantage stores a record of every ballot cast. This list of ballots is shuffled to (attempt to) preserve voter privacy. The shuffling algorithm is inadequate, and list can be unshuffled, revealing each voter's ballot in the original sequence.**

49.2 The secret ballot was introduced over a hundred years ago to combat vote-buying and voter coercion. But even as late as the mid 20th century, voter coercion (via violation of the secret ballot) was still taking place in cities such as Jersey

City.⁹¹

49.3 Because the sequence of voters who use a voting machine is observed by witnesses (pollworkers and party challengers), if one could learn the exact sequence of ballots cast, then one could learn how each voter voted. Therefore, any record of all the ballots that preserves this sequential order compromises privacy. It is for that reason that one would not want to use a reel-to-reel mechanism for recording voter-verified paper ballots, for example.

49.4 As each voter completes her ballot by pressing Cast Vote, the AVC Advantage stores an electronic record of that ballot as a “ballot image.” The Advantage keeps one copy of the list of ballot images in its internal memory, and it writes the other copy to the Results Cartridge.⁹²

49.5 If the ballot images were stored in sequential order, then one could learn how each voter voted. Therefore Sequoia has written the AVC Advantage software to shuffle the order of the ballot images in the internal memory (and in the Results Cartridge) so that the order is obscured.

49.6 We have found a procedure that can be used to learn the unshuffled order of ballot images, and therefore learn the votes of every voter. It requires knowing the exact time each voter pressed the “cast vote” button, to the nearest two seconds.

49.7 Our attack works in four stages, as follows.

1. *Record the sounds coming out of the voting machine.* An election-board worker carries a pocket-size digital voice recorder. He sets it down unobtru-



Figure 32: *Digital voice recorder, \$100*

sively on the voting machine, behind the little speaker that makes the chirping noises. The chirps made when Cast Vote is pressed are recorded, along

⁹¹Personal eyewitness report of Ed Kessler, told to Appel in 2004. In the 1930s Mr. Kessler accompanied his father to the polling place in Jersey City and watched as some voter showed their completed ballots to pollworkers before depositing them into the the ballot box.

⁹² Each ballot image is a string of bits, one bit for each active ballot position in this election, packed into a few bytes. For example, in the presidential primary of February 5, 2008, with 7 Democratic and 7 Republican candidates, each “ballot image” occupies 5 bytes.

with other ambient sounds. After the election, the audio file can be uploaded to a computer for automatic processing, which will separate the chirps from the noise, and calculate the exact time at which each voter voted.

2. *Extract the ballot images.* Anyone can walk up to the AVC Advantage after an election, when it is unattended, and use menus on the Operator Panel to write a copy of the ballot images to a cartridge.
3. *Run another election.* Inside the memory of the machine is the 32-bit random “seed” of the random number generator. To undo the shuffling, it is sufficient to know the value of the seed either before or after the election. One procedure for learning the seed is this. While the machine is unattended, turn it on and install a fresh ballot definition by inserting a fresh Results Cartridge into the Results port. Cast a known sequence of votes. The machine will write to the Results Cartridge an audit trail, shuffled using the algorithm described above.
4. Bring the audio-recording, the ballot-image cartridge, and the Post-LAT Results Cartridge to a computer, and upload the data. A specially prepared computer program analyzes all the data, and unshuffles the ballot images. This program is not as simple to write as the vote-stealing firmware we have described: writing the program would be a project of several months for a computer-science graduate student. The computer-science analysis behind this program is described in Appendix D.

Listening for the sounds the machine makes was the basis for a known attack on voter privacy in the days of lever machines. The lever machines used by New York State in the 20th century permitted voting a straight party ticket by pulling a single lever, and this was easy to distinguish (from voting a split ticket) by listening from outside the booth.⁹³

50 Conclusion of Part IV

50.1 Vote data in Results Cartridges is not authenticated by digital signatures. Therefore, 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. Or, the Results Cartridge can be manipulated before the polls open to install a ballot definition that confuses the AVC Advantage and permits fraud.

⁹³E-mail message from Douglas A. Kellner, co-chair, New York State Board of Elections, August 6, 2008.

Other kinds of cartridges (Early Voting cartridges, Consolidation cartridges) can also be manipulated to steal votes. The shuffling of the individual voters' ballots is reversible, permitting attacks on the secrecy of the ballots.

PART V

INSUFFICIENTLY RIGOROUS DESIGN AND CERTIFICATION PROCESSES LEAVE THE FIRMWARE VULNERABLE

51 Sequoia's sloppy software practices can lead to error and insecurity

51.1 **Summary:** In many places, the Source Code of the AVC Advantage does not follow best software engineering practices. We found many places where the Source Code and is violation of the specific technical rules for Source Code of the FEC Voting System Standards for election software. Violations of these practices and rules increase the chances that programmers will make mistakes, and the chances that these mistakes will slip through review and certification processes. Mistakes in the program can either directly miscount votes or can open security vulnerabilities that allow attackers to steal votes.

51.2 The AVC Advantage version 9.00H software consists of almost 130,000 lines of source code (including comments and empty lines) in over 700 source files. Somewhat over 25,000 lines are in Z80 assembly language and the rest are in C. If comments and blank lines are excluded, the corresponding numbers are approximately 38,000 and 12,000 lines respectively. This source code contains comments describing myriad changes from 1987 through October 2005, by at least a dozen different people.

51.3 The AVC 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 a significant number of 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.

51.4 The code suffers from, among other infelicities, 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. We give specific examples in Appendix E.

51.5 **Violations of FEC guidelines.** According to comments in the source files, at least one third of the source files were revised, mostly in 2001, to satisfy FEC standards.⁹⁴ However, these changes appear to have been done incompletely, and many parts of the source code are in direct violation of the standards.

51.6 For instance there are about fifty occurrences of the explicitly prohibited ”do ... while (FALSE)” construct. The FEC standards prohibit this manner of phrasing a computer program, because it leads to a program that is harder to understand, both by those who write the program and those, such as examiners and certifiers, who have to read it. Hard-to-understand programs are more likely to mask errors, insecurities, and vulnerabilities in the logic of the program. Many of the other FEC rules have a similar aim—make the logic of the program easier to understand and less prone to design flaws—and Sequoia’s Source Code breaks many of these other rules as well.

51.7 **Other ways in which the programming style increases the probability of error.** 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 language⁹⁵ makes it harder for compilers and other automatic tools to help catch programming errors. Standard library routines for tasks like memory allocation, copy and comparison are written from scratch, presumably for efficiency, but this can lead to confusion and potentially to errors.⁹⁶ 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 a problem as well, since it is much harder to work with than is a higher-level language.

51.8 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 such as the FEC

⁹⁴ presumably the Voting System Standards of 2002 and the similar Voluntary Voting System Guidelines of 2005

⁹⁵That is, function prototypes are written in 1970s style.

⁹⁶ For example, the order of arguments differs between the standard function `memset` and the Sequoia equivalent `memfill`; there are two functions called `fsize`, one the usual standard library version and one a version for the internal AVC file system.

coding standards. This is a serious problem, because errors in the program can miscount votes or open security vulnerabilities that permit fraud.

52 Wyle Laboratories examines firmware only superficially

52.1 **Summary: Our analysis of the Wyle Laboratories ITA reports, in conjunction with the actual Sequoia AVC Advantage Source Code, shows that the ITA reports are not very useful for ascertaining the security or reliability of the voting machine.**

52.2 Many states, in their decisions about whether to certify voting machines for use, rely on reports from a so-called independent test authority (“ITA”). In this section we will show that the sections of these reports that assess the *voting-machine firmware* are inadequate to provide meaningful guarantees of the security of the voting machines. From a technical point of view, New Jersey should not rely on such reports to assess the security of voting machines proposed for certification.

52.3 In this section we will evaluate the quality of the ITA reports on the AVC Advantage voting-machine firmware. In the next section we will explain why it is important to do so.

52.4 The Sequoia AVC Advantage models 9.00G and 9.00H were examined by Wyle Laboratories, an ITA, in Huntsville, AL. Wyle’s report on this examination⁹⁷ says that Wyle performed “in-depth source code review and functional tests” of the Advantage firmware. “The source code was reviewed to ensure it followed the recommended programming guidelines as contained in the FEC standards.” (page 18)

52.5 Wyle’s ITA report is inadequate in two ways.

- Sequoia did not provide to Wyle, and therefore Wyle did not examine, several firmware components installed in the AVC Advantage voting machine. One of components that Wyle did not examine⁹⁸ was extremely significant,

⁹⁷ Test Report 48761-03: Change Release Report of the AVC Advantage DRE voting machine (Firmware version 9.00G), April 27, 2004; page 5.

⁹⁸We know this in two ways. First, the written Wyle report includes a “file manifest” that lists every file that they did examine. Second, the way in which Sequoia responded to the Court’s order to provide all of their firmware was to have Wyle Laboratories prepare a disk of all the firmware they examined. As we will explain in Section 54, this disk did not contain some firmware components that Sequoia later provided to us, and that we confirmed are present in the AVC Advantage.

because it was the pathway for the voting-machine virus that we explained in Sections 19–21. This component is the AUTOEXEC.BAT. Indeed, Wyle did not report on this problem.

- On the firmware components Wyle did examine, their report is too superficial and perfunctory to be meaningful. The firmware would not be in compliance with the FEC 2002 standards, as we will describe.

52.6 Attachment B of the Wyle report on the Advantage 9.00G/H is about 70 pages long and is entitled “Source Code Reports Review and File Listings.” It reviews the AVC Advantage version “MainBd 10.1.1 IOBd 1.5 software” as of January 30, 2006. The document claims to include information from Revision 8.09D through Revision 10.1.1/1.5. There is no mention of 8.09 in any of the Sequoia code we have access to, but 8.00 is from December 1997 and 8.10 (originally called 8.1) is May 2001. Another comment in the report says that the assessment of version 8.00D through 9.00A is contained in Wyle Report 44733-07, which we obtained later through Court Order.

52.7 The attachment lists the names of files that were changed from each version to the next; typically there are a handful to a few dozen. The comparison between versions 9.00G and 9.00H is accurate in its list of files that have changed, as we can determine since Sequoia provided those two versions to us.

52.8 For a few of these files in a few of the versions of the software, the 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.

52.9 Only a small number of the comments ever suggest that the examiner at Wyle did anything more than skim through the program, *pro forma*. Appendix E gives specific technical support for this conclusion. Either the Wyle examiner does not have proper training in software engineering and computer security and so does not know what to look for; or he is not looking in enough depth to find the problems that are there; or both.

52.10 What this means is that the ITA software examination process permits errors and security vulnerabilities to slip through the certification process. Such vulnerabilities include the ones in the AVC Advantage that we describe in Sections 3, 19–21, 24, 26, 39, 40, 43, 45, 46, 49, 51, 56, and 57.

Wyle's report on the version 10 AVC Advantage is also inadequate

52.11 The criteria that Wyle uses for its examination of the version 10 AVC Advantage⁹⁹ are specified in the 2002 FEC Voting Systems Standards. The technical Source Code rules in those standards are not very specific nor likely to be very effective. Even if Wyle followed those rules to the letter, the report would not be very useful in assessing the security of the voting machines. However, it appears that Wyle does not even follow those rules in its report.

52.12 The transition from 9.00H to X.1 appears to have involved a significantly larger number of changed files; almost 130 are listed as changed. However the report says "half of the files [are] brand new", which is inexplicable. First, 9.00H has over 700 files; 130 files is less than 20 percent, not half. Second, many of the filenames listed are identical to names in 9.00H. Perhaps it is their contents that are different. In that case, one would have expected more substantive commentary on the changed code.

52.13 We believe that either the examination is simply too superficial, or that once some file has been deemed acceptable it is not examined again unless it changes and even then only the changed parts are examined.

53 New Jersey officials neglected to read the ITA reports, and thus had no opportunity to notice how their inadequacies

53.1 We do not know whether the State of New Jersey relied on Wyle's ITA report, or any report from any ITA, in certifying the AVC Advantage 9.00G or H for use in New Jersey. In response to Plaintiffs' request to the Defendant for all ITA reports in the possession of the State of New Jersey, that describe any version of AVC Advantage, the Defendant produced only some reports on version 10 AVC Advantages, and none for version 9 or earlier. The Defendant asserted that these were all the ITA reports that they had on the AVC Advantage.¹⁰⁰

53.2 Either the AVC Advantage 9.00 was put into use in New Jersey without being certified by State election officials; or it was certified without any New Jersey official examining the ITA reports. Suppose it is the case that the AVC Advantage 9.00 was purchased and put into service in New Jersey based, in part, on Sequoia's

⁹⁹ Test Report 51884-08: Hardware qualification testing of the Sequoia AVC Advantage DRE voting machine (Firmware version 10.1.5, April 12, 2006).

¹⁰⁰ Statement by Donna Kelly to the Court, July 2008.

assurance that this voting machine had received ITA approval in January 2006 (that is, the voting machine got its “NASED number”). **Then the failure of New Jersey officials to read Wyle’s ITA report deprived these officials of the opportunity to observe how inadequate the ITA examinations are as assessments of the security of voting-machine firmware.** If, on the other hand, the State of New Jersey had had a computer-security expert involved in the certification process, he would have wanted to see this report. An expert would have made the observation that Wyle’s examination of the firmware is so superficial that it cannot be relied upon as a basis for certifying that the firmware of the AVC Advantage is secure.

54 Sequoia does not keep track of what firmware is installed in its DREs

54.1 **Summary: Sequoia does not appear to keep track of what firmware is installed on its AVC Advantage voting machine. This is a serious problem for a product in which fraudulent firmware can steal elections.**

54.2 Sequoia Voting Systems complied in a very haphazard way with a Court Order to deliver its voting-machine Source Code and Firmware. In the process, we learned that Sequoia apparently does not keep good track of what firmware is in its own voting machines. The firmware is supplied from a wide variety of sub-contractors and suppliers. Many of the components, Sequoia has not examined or inspected.

54.3 Any one of these components could contain,

- an innocent programming error that an attacker can exploit to insert vote-stealing firmware; or
- malicious firmware that steals votes.

To the extent that Sequoia does not have tight control over what firmware is installed, Sequoia leaves avenues for the installation of vulnerable or malicious firmware *during the manufacture of the voting machines.*

54.4 **Evidence that Sequoia does not keep good track of what is installed in the AVC Advantage.** In March, 2008 the Court ruled that it would enforce a subpoena for materials including the following:

“... 4. For each Sequoia AVC Advantage DRE Voting machine supplied pursuant to Requests No.2 and No.3 above: The complete source

code (in electronic form), including libraries and all related technical documentation, for all the software (or firmware, as the case may be) in the voting machine, complete with all configuration files and build tools. Your production pursuant to this Request must be such that would allow the recipient to reproduce the binary images currently loaded into the voting machines in use in New Jersey, and sufficient to enable the building and execution of modifications to the software made for testing and analysis purposes.”

54.5 **We will describe the haphazard and disorganized way in which Sequoia complied with this request, to support our conclusions that Sequoia did not have a well-organized inventory of what firmware is in its AVC Advantage voting machine.**

54.6 On May 20, 2008 the Court issued an order for Sequoia to produce these items for examination. On June 20, 2008, the Court issued a modified order—but not modified with respect to what materials should be produced. Thus, Sequoia had several months to prepare its production of Source Code, Firmware, and Build Tools by the Court-ordered delivery date of June 30, 2008.

54.7 On June 30 Sequoia supplied a CD-ROM created by Wyle Laboratories labeled “9.0G Source and Firmware, 9.0H Source and Firmware, Wyle Job No. T55627-01.”¹⁰¹ This disk contained

- The complete firmware for the motherboard Z80.
- The source code for the motherboard Z80, *except* for the sources to certain library files for which only the linkable object code was present. This library was later identified as coming from Greenleaf Software, Inc. of Richardson, TX.
- The source code and firmware for a file SUBSYS.EXE which is the voting program that runs on the daughterboard.
- No build tools (e.g., compiler).
- No source code or firmware for the operating system on the daughterboard computer, which appeared to be a 1990s-era DOS-compatible operating system.

¹⁰¹Recall that we are using the term “firmware” to indicate the compiled program as it is loaded in the voting machine; Wyle’s label also uses the word in that sense.

- No configuration files (“Execution Environment”) for the daughterboard, such as CONFIG.SYS or AUTOEXEC.BAT that would be expected to be present.

54.8 We brought these omissions to Sequoia’s attention, and after some delay they provided on July 14 a CD-ROM created by Wyle Laboratories labeled “Sequoia Advantage 9.0G & 9.0H / Source Code, Compiler, and Reports / Wyle Job No. T55023W-013.” This repeated much of the earlier material, but also contained the Build Tools for the motherboard only, that is, the Lattice C compiler and associated makefiles. However, still missing were:

- Build tools (e.g., compiler & makefiles) for daughterboard.
- Source code and firmware for the operating system on the daughterboard computer.
- Execution Environment for the daughterboard, (CONFIG.SYS, AUTOEXEC.BAT, etc.).

54.9 We brought these omissions to Sequoia’s attention, and after some delay they told us on July 14 that they had assembled the missing components and were preparing to send them to us. In a telephone telephone conversation that day between Appel and Mr. David Allen, V.P. of Development for Sequoia Voting Systems, Inc., Mr. Allen said that Sequoia had not previously had the files in its own possession, but had just finished gathering them from Sunrise Labs, a company that had built the daughterboard under contract to Sequoia. However, during this conversation Mr. Allen told Appel that CONFIG.SYS and AUTOEXEC.BAT were not among the files that he had gathered. Mr. Allen said he would again contact Sunrise Labs to obtain these missing files.

54.10 On July 16 Sequoia delivered a disk that they described as the missing operating-system and execution-environment components. It contained,

- Execution Environment for the daughterboard, (CONFIG.SYS, AUTOEXEC.BAT, etc.).
- Some operating-system components in Firmware form:
 - Certain components from Datalight ROM-DOS 5.0SU.
 - Certain components from Datalight ROM-DOS version 6 or 7: HIMEM.SYS.

- Certain components from Microsoft MS-DOS 6: MEM.EXE, MODE.COM, and MOVE.EXE.
- A component from an unidentified source, NJRAMDX.SYS.

However, the BIOS components of the operating system were missing (IBMBIO.COM and IBMDOS.COM). Mr. Allen said that they did not have this component, because it was preinstalled on the daughterboard by the manufacturer of the daughterboard processor.

54.11 We were able to extract the BIOS from the daughterboard of an AVC Advantage belonging to Union County, and found that it was from General Software, Inc.

54.12 In summary, the firmware on Sequoia's AVC Advantage voting machine is an assemblage of components from Sequoia itself and no fewer than 6 different vendors (Sunrise, Datalight, Microsoft, IBM, General Software, and one unknown). Furthermore, it appears that before we engaged in them in the process of submitting their entire firmware for examination, Sequoia did not have any organized records of what firmware was in their own voting machine, and had never examined the BIOS components of the operating system. To this day, Sequoia claims it does not have Source Code for any of the operating systems components running in the daughterboard.

54.13 Therefore, Sequoia has no effective way of knowing whether they have installed tainted firmware in the AVC Advantage. This is a serious problem for a product in which fraudulent firmware can steal elections.

55 Conclusion of Part V

55.1 Sequoia's sloppy software practices can lead to error and insecurity. Such programming errors can miscount votes and permit fraud. Wyle's ITA reports are not rigorous, so that programming errors and security vulnerabilities can and do slip through the ITA examination process. New Jersey officials who certify voting machines do not sufficiently examine even these inadequate ITA reports.

PART VI

COMPUTER-PROGRAMMING ERRORS HAVE ACTUALLY DISENFRANCHISED NJ VOTERS

55.2 Certain county clerks, and others, noticed inconsistencies in the printed paper results reports from New Jersey's Presidential Primary election of February 5, 2008. We have found that these were caused by two distinct design flaws or programming errors in the AVC Advantage voting machine. As a consequence of these flaws, voters were disenfranchised.

55.3 A *bug* is a computer-programming error that causes the program to operate incorrectly. Needless to say, a bug in a computer program that counts votes is a serious issue.

56 Primary election party-affiliation bug disenfranchised voters

56.1 **Summary: A programming error in the AVC Advantage caused at least 37 and likely more primary voters to be given the wrong party's ballot to vote. This was noticed because the results-report printouts from the machines were internally inconsistent—the number of votes cast in each primary did not match the number of voters in that primary. A stray option-switch button-press can interact with the programming error to cause the problem observed in 37 different AVC Advantage voting machines in the 2008 Presidential Primary. The problem is significant because it caused voters to be disenfranchised by denying them the ability to vote in their own party's primary. In addition, it wrongly permitted them to vote in the other party's primary.**

56.2 In the New Jersey Presidential Primary of February 5, 2008, anomalies were noticed on 38 different voting machines in 8 counties.¹⁰² Our examination shows that one of these machines¹⁰³ experienced an error that is qualitatively different

¹⁰² An OPRA (Open Public Records Act) request to all counties for copies of results-report printouts that exhibited anomalies yielded the following results: Bergen (4 machines), Burlington (1), Camden (1), Cape May (4), Gloucester (2), Hudson (16), Ocean (1), Union (8).

¹⁰³Machine serial number 25249, in Pennsauken election district 6, Camden County

from all the others. We discuss this error separately, in Section 57. Here we discuss the other 37 machines.

- 56.3 In a primary election, the AVC Advantage counts
- The number of voters from each party that voted on the machine (each voter permitted to vote only for a candidate from her own party); and
 - The number of votes each candidate received; and
 - The total number of ballots cast on the machine.

The firmware of the machine (the computer program) is supposed to make sure that each voter votes only for a candidate in her own party's election.

- 56.4 The anomaly was that 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. On other machines, the number of votes for Republican candidates exceeded the number of Republican voters. The results report printed by the machine was inconsistent with itself.

- 56.5 **How primary elections work on the AVC Advantage.** Before approaching the voting machine, the voter signs the pollbook at the sign-in table. The voter receives a paper ticket called a "voting authority." The voter then approaches the voting machine. She hands the voting authority ticket to a pollworker standing next to the voting machine. In a general election, the pollworker would take the ticket and press the green "Activate" button on the Operator Panel of the voting machine.¹⁰⁴

- 56.6 The procedure is slightly different in a primary election. The voter may vote either in the Republican primary, or the Democratic primary, but not both.¹⁰⁵ However, each AVC Advantage can accept ballots of either party. When the voter enters the booth, all the candidates of both parties would be shown, in two separate rows. The AVC Advantage does not have the capability to show only the candidates for just one of the parties at a time, because the "display" is just a large paper sheet

¹⁰⁴ Sources of information for first three paragraphs of this section: Mercer and Middlesex pollworker manuals; Sequoia AVC Advantage Operator Manual; and from personal observation of election procedures in Mercer county.

¹⁰⁵To simplify the discussion, we assume that only these two parties are holding primary elections, as was the case in the 2008 New Jersey Presidential Primary.

preprinted with candidate names in such a way that they are placed by the appropriate buttons under the paper.

- 56.7 Only one party's ballot is enabled for each voter, using the following process. Depending on the voter's registered party affiliation, she receives either a Republican or a Democratic voting authority. These are colored differently to avoid confusion in the next step. In a primary election, the pollworker must first tell the machine which party's ballot to activate. He does this by pressing an extra button before pressing Activate.

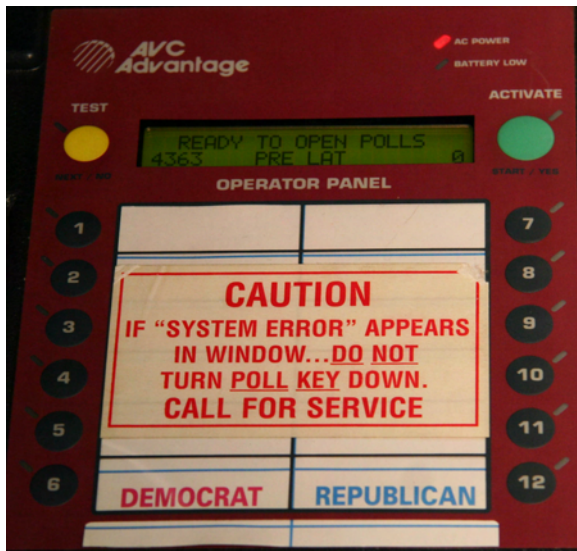


Figure 33: *Operator Panel*

- 56.8 The Operator Panel of the AVC Advantage has an alphanumeric display, 14 buttons, and 16 red lights. A yellow button is labeled "Test", a green button is labeled "Activate", and 12 buttons are labeled 1 through 12, in two columns. (See Figure 33). The numbered buttons are called "option switches." Depending on the ballot definition programmed into the Results Cartridge, these option switches perform certain functions in an election. (Outside of an election, they also serve other purposes.) The panel has a plastic window under which a paper sheet may be inserted to label the functions of the buttons.¹⁰⁶

- 56.9 As the ballot definition used by Union County for the 2008 Presidential Primary election was configured, the lower-left option switch, number 6, selects the

¹⁰⁶ From our examination of AVC Advantage voting machines.

Democratic primary, and the lower-right option switch, number 12, selects the Republican primary. As the voting machines were used in the polling place, the paper label sheet had the word DEMOCRAT printed by switch 6, and REPUBLICAN by switch 12. Switches 1–5 and 7–11 were unlabeled.

56.10 So, when a voter approached the voting machine and handed a voting authority labeled DEMOCRAT to the pollworker, the pollworker was supposed to press 6, then Activate. Conversely if the voter hands in a REPUBLICAN voting authority and the pollworker is supposed to press 12-then-Activate.

56.11 The results report printed by AVC Advantage serial number 17627 in Ward 3, District 2 of the municipality of Hillside in Union County on February 5, 2008 is shown in Figure 34. The candidate totals are

- (Democrats) Obama 182, Kucinich 0, Edwards 0, Biden 0, Richardson 0, Clinton 179 (this adds up to 361)
- (Republicans) Giuliani 1, Thompson 0, Romney 13, McCain 40, Paul 3, Huckabee 4 (this adds up to 61)

56.12 In this results report, the number of Democratic voters is listed as 362, and the number of Republican voters is listed as 60. There are more votes than voters in the Republican primary! This should be impossible.

56.13 Also, there are more voters than votes in the Democratic primary. In some kinds of elections this situation should be possible, because voters are not compelled to select a candidate in every contest. But in this election, Union County's ballot definition required each voter to cast exactly one vote in the primary election: the Cast Vote button had no effect if the voter had not chosen a candidate. Thus, it should have been impossible to have 361 Democratic votes by 362 Democratic voters.

56.14 The record of how many voters were enabled to vote in the Democratic primary, and how many in the Republican primary, is called the "Option Switch Totals" as it is printed on the Official Election Results Report. The record of how many votes were cast for each candidate is called the "Candidate Totals". In principle, the Candidate Totals for the Democratic candidates should add up *exactly* to the Option Switch Totals for button number 6, labeled 1-DEM in the printout; and similarly for the Republican candidates and the Republican option-switch total. But on this printout there are erroneous and inconsistent numbers, as we have explained.

Date 02/05/08 Time 8:02 PM
 Serial Number 17627
 Protective Counter 5531
 Public Counter 422
 Precinct/District HI 3-2
 Polling Place ID C70332
 Ballot Version 1
 Report Source Internal Machine Memory
 PRESIDENTIAL PRIMARY 2/5/08

Candidate	Candidate Totals	Total
***	0-DEM	***
*	President 15th delegate A1	(1)
218	BARACK OBAMA	182
E12	DENNIS KUCINICH	0
F10	JOHN EDWARDS	0
G10	JOE BIDEN	0
H13	BILL RICHARDSON	0
I13	HILLARY CLINTON	179
J10	Personal Choice	0
***	1-REP	***
X	President A2	(1)
924	RUDY GIULIANI	1
E24	FRED THOMPSON	0
F24	MITT ROMNEY	13
G24	JOHN McCain	40
H24	RON PAUL	3
I24	MIKE HUCKABEE	4
J24	Personal Choice	0

Write In Votes
 No Write In Votes In Memory

Option Switch Totals

1	UNUSED	0
2	UNUSED	0
3	UNUSED	0
4	UNUSED	0
5	UNUSED	0
6	3-DEM	362
7	UNUSED	0
8	UNUSED	0
9	UNUSED	0
10	UNUSED	0
11	UNUSED	0
12	1-REP	60
Total		422

Election Officers

Please Complete After Closing The Polls
 We the undersigned Election Officers do
 hereby certify that on the Feb
 day of 5 2008 this board
 under the scrutiny of each member,
 closed the polls from further voting,
 obtained this printed record of votes
 cast on this machine and that after the
 polls closed, the Protective Counter
 read 5531 and the Public Counter read
 422 and the machine has been sealed
 with seal # 011742.

Signed:

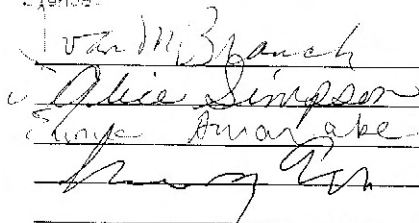


Figure 34: Results report tape from
 Ward 3, District 2 of the municipality of
 Hillside in Union County, Presidential
 Primary election of February 5, 2008.

- 56.15 This discrepancy was noticed by the Union County Clerk, Joanne Rajoppi. She then examined results reports printed by other voting machines in Union County and found several more such discrepancies. She alerted the county clerks of other counties, and they found dozens more similar discrepancies. These county officials then requested the Attorney General to conduct an investigation into the cause.
- 56.16 Subsequently, Sequoia Voting Systems sent a memo entitled, "To: AVC Advantage Customers using series 9.0 firmware," dated March 4, 2008, containing Sequoia's explanation of how this anomaly arose. It explains that a software-programming error, a bug, was triggered when the pollworker pressed *a different button than 6 or 12* on the operator panel. Sequoia makes the claim that, notwithstanding the incorrect "option-switch totals," the votes were added correctly. **What Sequoia leaves out is that this programming error disenfranchised voters, by denying them the ability to vote in their own party's primary.**
- 56.17 If the election worker, on being handed a voting authority labeled DEMOCRAT, presses the 6 button, then presses an unlabeled button (1-5 or 7-11), then Activate, the software bug caused the machine to behave as follows. The red light next to operator-panel button 6 would stay illuminated. The option-switch total would count as 6; but the Republican ballot would be enabled on the voter panel, and the machine would accept votes only for Republican candidates.
- 56.18 It would be 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; then attempting to correct the problem by pressing Activate leads to the sequence 6-7-Activate.
- 56.19 In other counties, where button 6 was assigned to REPUBLICAN and button 12 to DEMOCRAT, the pattern was reversed as to party. A voter would hand a Republican voting authority to the pollworker; the pollworker would press 6-X-Activate (where X is any button 1-5 or 7-11). Then the voter would find that only Democratic candidates could be voted for, but the option-switch total counted as Republican.
- 56.20 One might think that the voter would complain to the pollworker that the machine was not working properly. This may have happened, perhaps far more than 37 times. In that case, there is a way for the pollworker to deactivate the AVC Advantage and reactivate it for the right party. In any case we know that 37 voters did not successfully complain, and ended up voting in the wrong primary election.

- 56.21 In our examination of the Source Code of the AVC Advantage, we found a software bug consistent with Sequoia's explanation in their memo of March 4, 2008. This bug almost certainly caused most of the anomalies noticed in results reports printed on February 5, 2008. However, one machine demonstrated an anomaly that cannot be explained this way; see Section 57.
- 56.22 **Loss of the franchise and unauthorized votes.** It is important to consider what this means. In Union County, for some particular voter, a pollworker pressed the option switch for Democratic and did *not* press the option switch for Republican. Then he inadvertently pressed another button, neither Democratic nor Republican; then he pressed Activate. This means that almost certainly he had been handed a voting authority labeled DEMOCRAT. The voter, however, was not able to vote in the Democratic primary, as was her right. Furthermore, the voter then cast a ballot in the Republican primary, which she was not permitted to do by law, and this vote was recorded and counted.
- 56.23 Appendix C gives a more technical explanation of Sequoia's computer-programming error that led to the disenfranchisement of voters.

57 Hardware malfunctions can disenfranchise voters

- 57.1 **Summary: Hardware errors in the AVC Advantage can cause votes to be lost. When a Results Cartridge fails, the voting machine indicates an error. But it is not possible for either the voter or pollworkers to determine whether or not the vote was recorded. This occurred in the 2008 Presidential Primary, and can occur in general elections as well.**
- 57.2 The AVC Advantage is supposed to have a double-redundant storage for votes: it is supposed to record votes in an internal memory as well as in a removable Results Cartridge, in case a hardware failure during an election causes one memory to be lost.
- 57.3 However, there is a design flaw in the AVC Advantage. If one of these memories fails while a voter is in the booth, it is not possible to know whether that voter's vote has been recorded (in the other memory). Therefore, even the most knowledgeable and alert pollworker would have no way of knowing whether to permit the voter to use a different voting machine to cast her vote.

57.4 This situation actually arose in the February 5, 2008 primary election. An AVC Advantage voting machine in the town of Pennsauken in Camden County¹⁰⁷ experienced an anomaly that cannot be explained by the “option-switch bug” explanation (experienced by 37 other machines on that day). On this DRE, the public counter printed as 29, meaning that 29 voters have voted on this DRE in this election. The results report printed by the AVC Advantage at the close of the polls showed the following tally:

- (Democrats) Clinton 14, Obama 7, Richardson 0, Edwards 0, Kucinich 0, Biden 0
- (Republicans) McCain 5, Paul 2, Giuliani 0, Huckabee 0, Romney 2, Thompson 0

This adds up to 30 votes. Thus, the number of votes recorded exceeds the number of voters; this should not happen. The option switch totals are DEM 20, REP 9, adding up to 29.

57.5 According to our examination of the AVC Advantage source code, this error *cannot* be caused by the “option-switch bug” described in Section 56. Therefore it must have a different cause.

57.6 In our examination of the source code and in our examination of the behavior of an actual machine¹⁰⁸ we have identified the following source of error.

57.7 After the voter presses Cast Vote, the AVC Advantage does the following book-keeping, in this order:

1. Play the chirping sound and wait for it to complete.
2. Write a “ballot image” (a few bytes that record a 1-bit in each voted-for position, and a 0-bit in each unvoted ballot position) to the internal memory and to the Results Cartridge. The internal memory is a battery-backed memory on the motherboard; the Results Cartridge contains a small circuit board with a battery-backed memory.
3. If the voter cast write-in votes, store them in the internal memory and in the Results Cartridge.
4. Add this voter’s votes to the candidate totals, and write the updated candidate totals to the internal memory and the Results Cartridge.

¹⁰⁷Machine serial number 25249, in Pennsauken election district 6, Camden County

¹⁰⁸AVC Advantage serial number 17926, owned by Union County, NJ.

5. (If in a primary election) Add 1 to the option-switch totals for the selected option switch, both in the internal memory and in the Results Cartridge.
6. Add 1 to the public counter, which maintains a count of the total number of votes cast during the election.
7. Add 1 to the protective counter, which maintains a count of the total number of votes ever cast on this machine.

57.8 If the machine is interrupted during this process, then the first few steps will complete, but not the rest. An error message will appear on the operator panel, and the machine will not accept any more votes.

57.9 The “interrupts” that cause the Cast Vote process to suspend include,

- Failure of communication to the Results Cartridge (whether or not audio voting is in progress);
- Failure of communication to the audio-voting keypad (when audio voting is in progress).

In our experiments, we deliberately caused these failures of communication by unplugging the Results Cartridge or the audio-voting keypad just after casting the vote. The results are shown in Figure 35. Depending on how exactly when the Results Cartridge fails (or is disconnected),

- The list of ballot images disagrees with the candidate totals (this error is not observable from the results-report printout alone, but can be seen by WinEDS in the Results Cartridge); or
- The candidate totals disagree with the option-switch totals; or
- The candidate totals and option-switch totals agree, but disagree with the public counter.

57.10 We presume that, in Pennsauken (Camden County) on February 5, nobody yanked out a Results Cartridge from the back of the machine just as a voter pressed Cast Vote. However, an electrical failure in the Results Cartridge or in the socket of the Results port could also cause this problem.

57.11 There were two Advantage machines in Pennsauken district 6 that morning, #25574 and #25249. It must be the case that some component of machine #25249

```

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
OFFICIAL ELECTION RESULTS REPORT
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Date 02/05/08          Time 8:01 PM
Serial Number          25249
Protective Counter     655
Public Counter         29
Precinct/District     Pennsauken Dist 6
Polling Place ID      270006
Ballot Version        1
Report Source          Internal Machine Memory

Presidential Primary
County of Camden
February 5, 2008

Candidate Totals
Candidate              Total
xxx 1-DEM              xxx
* US President        (1)
D7 Hillary Clinton    14
E7 Barack Obama       7
F7 Bill Richardson    0
G7 John Edwards       0
H7 Dennis Kucinich    0
I7 Joe Biden          0
xxx 1-REP              xxx
* US President        (1)
D17 John McCain       5
E17 Ron Paul          2
F17 Rudy Giuliani     0
G17 Mike Huckabee     0
H17 Mitt Romney       2
I17 Fred Thompson     0

Write In Votes
No Write In Votes In Memory

Option Switch Totals
1 1-DEM                20
2 UNUSED               0
3 UNUSED               0
4 UNUSED               0
5 UNUSED               0
6 UNUSED               0
7 1-REP                9
8 UNUSED               0
9 UNUSED               0
10 UNUSED              0
11 UNUSED              0
12 UNUSED              0
Total                  29

Election Officers
Please Complete After Closing The Polls
We the undersigned Election Officers do
herby certify that on the 5
day of Feb 2008 this board
under the scrutiny of each member,
obtained the polls from further voting,
cast on this machine and that after the
polls closed, the Protective Counter

```

(a)

```

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
OFFICIAL ELECTION RESULTS REPORT
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Date 01/29/08          Time 1:19 PM
Serial Number          17926
Protective Counter     4047
Public Counter         4
Precinct/District     WI 2
Polling Place ID      210002
Ballot Version        1
Report Source          Internal Machine Memory

PRESIDENTIAL PRIMARY 2/5/08

Candidate Totals
Candidate              Total
xxx 1-DEM              xxx
* President 12th delegeate (1)
A1
D13 BARACK OBAMA      1
E13 DENNIS KUCINICH   0
F13 JOHN EDWARDS     0
G13 JOE BIDEN         0
H13 BILL RICHARDSON   0
I13 HILLARY CLINTON   2
J13 Personal Choice   0
xxx 1-REP              xxx
* President            (1)
A2
D24 RUDY GIULIANI     0
E24 FRED THOMPSON     0
F24 MITT ROMNEY       0
G24 JOHN MCCAIN       2
H24 RON PAUL          0
I24 MIKE HUCKABEE    0
J24 Personal Choice   0

Write In Votes
No Write In Votes In Memory

Option Switch Totals
1 UNUSED              0
2 UNUSED              0
3 UNUSED              0
4 UNUSED              0
5 UNUSED              0
6 1-DEM               3
7 UNUSED              0
8 UNUSED              0
9 UNUSED              0
10 UNUSED             0
11 UNUSED             0
12 1-REP              2

```

(b)

```

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
OFFICIAL ELECTION RESULTS REPORT
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Date 01/29/08          Time 2:13 PM
Serial Number          17926
Protective Counter     4070
Public Counter         5
Precinct/District     WI 2
Polling Place ID      210002
Ballot Version        1
Report Source          Internal Machine Memory

PRESIDENTIAL PRIMARY 2/5/08

Candidate Totals
Candidate              Total
xxx 1-DEM              xxx
* president 12th delegeate (1)
A1
D13 BARACK OBAMA      2
E13 DENNIS KUCINICH   0
F13 JOHN EDWARDS     0
G13 JOE BIDEN         0
H13 BILL RICHARDSON   0
I13 HILLARY CLINTON   2
J13 Personal Choice   0
xxx 1-REP              xxx
* President            (1)
A2
D24 RUDY GIULIANI     0
E24 FRED THOMPSON     0
F24 MITT ROMNEY       0
G24 JOHN MCCAIN       2
H24 RON PAUL          0
I24 MIKE HUCKABEE    0
J24 Personal Choice   0

Write In Votes
No Write In Votes In Memory

Option Switch Totals
1 UNUSED              0
2 UNUSED              0
3 UNUSED              0
4 UNUSED              0
5 UNUSED              0
6 1-DEM               3
7 UNUSED              0
8 UNUSED              0
9 UNUSED              0
10 UNUSED             0
11 UNUSED             0
12 1-REP              2

```

(c)

Figure 35: Three results-report printouts from AVC Advantage machines demonstrating inconsistencies.

(a) An official report, signed by election board workers at the polling place, from Camden County on Feb. 5, 2008. The candidate totals exceed the public counter.

(b) A report that we produced (July 12, 2008) on AVC Advantage #17926 owned by Union County; the candidate totals exceed the public counter.

(c) A report that we produced (July 12, 2008) on AVC Advantage #17926 owned by Union County; the candidate totals exceed the option-switch totals.

failed on the 30th ballot cast, at or before 8:20 a.m., and then no more ballots were cast on that machine on February 5th. Then Camden County delivered a replacement AVC Advantage, #25690, to this polling place.¹⁰⁹

57.12 The Results Cartridge failed to capture vote data. Camden County's log¹¹⁰ states, "Cartridge was loose."

57.13 Other evidence hints that the Results Cartridge of this machine failed. Since this information was relayed to us at third or fourth hand, we will take it as suggestive but we will not rely on it in making our conclusions.¹¹¹ An examination of the original Results Cartridge in its original state would help clarify how exactly this voting machine failed. This cartridge, although requested in a subpoena, has not been made available to the Plaintiffs or to our team.

57.14 Some evidence hints that, even though the Results Cartridge failed, Camden County was able to read some information from it. A one-page report¹¹² apparently printed by WinEDS, perhaps from this Results Cartridge, indicates votes of

- (Democrats) Clinton 14, Obama 6, Richardson 0, Edwards 0, Kucinich 0, Biden 0
- (Republicans) McCain 5, Paul 2, Giuliani 0, Huckabee 0, Romney 2, Thompson 0

¹⁰⁹ Records of replacement machines delivered to precincts, Bates Number CAM 0001-0002, CAM 000297-000299.

¹¹⁰ "2008 Presidential Primary Machine Report", Bates Number CAM 000450, as follows: Pennsauken 6; 25249; 8:20 AM; System error 31; Could not be cleared. CHECK UPON RETURN. Cartridge was loose. Once pushed in, error cleared."

¹¹¹ E-mail from Deputy Attorney General Jason Postelnik to Penny Venetis, July 30, 2008: "Due to the issue that machine # 25249 experienced on Feb. 5, the ballot cartridge reader, in conjunction with the WinEDS software, could not read this voting machine cartridge. This meant that its results information was not uploaded onto the server and was not saved. The results from that cartridge had to be manually entered into WinEDS from the election results report retrieved using the cartridge utility function." In this e-mail Mr. Postelnik appears to be conveying information given to him by the Camden County Superintendent of Elections. We find the last sentence suggestive of many possibilities. **If the cartridge could not be read at all, then it would not have been possible to retrieve anything from it "using the cartridge utility function" of WinEDS. We suppose it is possible that the cartridge could be partially read but not completely read, so that normal uploading into WinEDS failed, but one of the Cartridge Utility functions did work. In this case, examination of the cartridge in its original state would shed some light on the general accuracy of cartridge data.**

¹¹²Bates Number CAM 000301

This adds up to 29 votes. **If this information is from the Results Cartridge, then the Results Cartridge does not agree with the printed results report from the machine (signed by witnesses), listing 7 votes for Obama and 30 votes overall.**

57.15 We analyzed the election totals reported by the Camden County Clerk for this precinct.¹¹³ Figure 36 summarizes the printouts from the results tapes, along with the totals reported by the Clerk.

57.16 In that table, the boxed pair indicates an inconsistency produced, we conclude, by a failure of the voting machine or the Results Cartridge, probably the Results Cartridge.

57.17 The doubly-boxed pair in the table indicates an inconsistency. The results report signed by witnesses in the polling places add up to 95 votes for Obama, but the Clerk reports 94 votes for Obama. The County Clerk has subtracted one vote for Barack Obama. Apparently he was relying on the data extracted from the failed Results Cartridge, as we described in ¶57.14.

57.18 In summary, when the AVC Advantage experiences a hardware failure, voters are disenfranchised. Next we will explain how a design flaw in the AVC Advantage contributes to this disenfranchisement.

How voters are disenfranchised by Results Cartridge failures

57.19 When an AVC Advantage fails in the Cast Vote process, it is impossible *at that time, before the close of the polls*, to know whether the last vote has recorded in the machine's internal memory, or in the Results Cartridge, or both, or neither.¹¹⁴ This can only be deduced later, after the polls are closed and the results are printed (and the Results Cartridge has been extracted).

57.20 But it is *essential* to know whether to permit the voter to recast the vote (on another voting machine). If the vote has already been recorded in the Results Cartridge, then the voter must not cast another vote, or else she will have voted twice.

¹¹³ A document obtained by OPRA (Open Public Records Act) request from the Clerk of Camden County, listing precinct-by-precinct totals for all Democratic candidates in the Presidential Primary of February 5, 2008.

¹¹⁴ we conclude this from our examination of the source code, and from experiments performed on an AVC Advantage machine.

	#25574	#25690	#25249	Tape Total	Reported by Clerk	Results Cartridge	Voting Authorities
Clinton	86*	81*	14*	181	181 [†]	14	
Obama	45*	43*	7*	95	94 [†]	6	
Richardson	1*	1*	0*	2	2 [†]	0	
Edwards	1*	0*	0*	1	1 [†]	0	
Kucinich	0*	0*	0*	0	0 [†]	0	
Biden	0*	1*	0*	1	1 [†]	0	
DEM	133*	126*	20*			20	
TOTAL	133	126	21	280	279 [†]	20	283 [‡]

Figure 36: *Inconsistent data from Pennsauken 6, in Camden County.*

Tape Total is the sum of number reported by the voting machines on their printed paper results-report tapes signed by witnesses.

Results Cartridge is the data that *may have been* extracted from the Results Cartridge of #25249; the evidence is ambiguous; see ¶57.14 and footnote 111.

DEM is the “option-switch” total printed on the results reports, that is, the number of voters the machine reports in the Democratic primary.

The asterisk* indicates data printed onto paper results reports (by the voting machine whose serial number is given at the top of the column) and signed by witnesses.

The dagger[†] indicates data reported by the County Clerk as the official election results for this precinct (3 voting machines cumulated together).

The double-dagger[‡] is the number of DEMOCRAT voting authority slips collected in this precinct; copies delivered by Donna Whiteside, Assistant County Counsel, Camden County, August 8, 2008.

All numbers without *[†][‡] we calculated from the raw data* in the same row or column.

The boxed pairs should agree with each other, but do not; see ¶57.16–57.17.

Even aside from the one lost vote on the malfunctioning AVC Advantage, there appears to be an undervote of 3 votes. There are 283 voting authority stubs, but only 279 or 280 votes. See Section 30.

If the vote has not already been recorded, then the voter must be permitted to cast another vote.

57.21 The behavior of the AVC Advantage when a Results Cartridge fails constitutes a design flaw. The design of the machine makes it impossible to know whether the vote has been recorded. This risks disenfranchising voters, or erroneously permitting voters to vote twice.

57.22 **Usefulness of optical-scan ballots.** A widely used form of Voter-Verified Paper Ballot is the optical-scan ballot. In places where precinct-count optical scanners are used to satisfy the requirement for a voter-verified paper record of each vote cast, the confusion about “did the machine record a vote?” can be entirely avoided, because the ballot was physically marked by the voter herself, and physically deposited (through the optical scanner) into the ballot box by the voter, in the presence of witnesses. There is no doubt about whether the ballot is in the ballot box.

58 Conclusion of Part VI

Anomalies noticed by County Clerks in the New Jersey 2008 Presidential Primary were caused by two different design errors on the part of Sequoia. The “option-switch error” was caused by a computer-programming bug in the firmware of the AVC Advantage, that had the effect disenfranchising voters by presenting the wrong party’s primary ballot to them. The error that occurred in Camden county was a design error in the firmware, that causes the AVC Advantage not to accurately report whether or not a vote has been recorded. As we explained, this also has the effect of disenfranchising the voter.

PART VII

DIFFERENT VERSIONS OF THE AVC ADVANTAGE HAVE DIFFERENT VULNERABILITIES

58.1 The AVC Advantage has been produced in many versions since it was introduced in the 1980s. These version differ in what firmware is loaded into their ROMs. In this part we explain what machines we examined, and how these machines relate to other machines that have been used, or might be used, in New Jersey.

59 Advantage versions 9.00G and 9.00H have identical vulnerabilities

59.1 In July and August 2008 we examined source code, firmware,¹¹⁵ and the physical hardware of the Sequoia AVC Advantage direct-recording electronic voting computer. The machines and software¹¹⁶ that we examined were version 9.00H of the AVC Advantage series, dated October 5, 2005.¹¹⁷ The State of New Jersey provided to us two voting machines owned by Union County, New Jersey, containing the 9.00H firmware. Therefore we studied primarily the 9.00H version of the software/firmware. Version 9.00G and 9.00H differ only slightly in their firmware, so our conclusions apply to both versions. Most New Jersey counties use version 9.00H but Hudson and Mercer counties have version 9.00G machines.¹¹⁸

59.2 *Versions of the AVC Advantage both before and after 9.00H differ significantly in vulnerability to hacking and in other respects. See Sections 60, 62, and 61. Unless stated otherwise, conclusions in this report about the security and accuracy*

¹¹⁵ In this document we use the term “firmware” to mean executable object code installed in ROM or in Flash memory on the voting machine.

¹¹⁶ In this document we use the term “software” to encompass source code and executable object code.

¹¹⁷ Sequoia provided to us version 9.00G and 9.00H of both the software and firmware, with source code missing for some components. A file within the source code, which lists the software revision history, indicates a date for 9.00G of January 19, 2004, and a date for 9.00H of October 5, 2005; some files of the audio subsystem are dated October 20, 2005.

¹¹⁸ Statement of Assistant Attorney General Donna Kelly to the Court, July 22, 2008.

of the AVC Advantage should be taken to apply only to versions 9.00G and 9.00H, and not to earlier or more recent versions.

60 The AVC Advantage has changed a great deal in successive versions

60.1 **Summary: The AVC Advantage has had many substantial firmware rewrites since its introduction in the 1980s. The hardware, from 1984 to 2002, had just a Z80 (motherboard) computer. Since 2003 it also has a more powerful daughterboard computer. The version 9 machine currently in use in New Jersey uses the daughterboard just for audio voting. In the version 10 machine proposed for use in New Jersey, the daughterboard is the “main processor.”**

60.2 The AVC Advantage was first produced in the 1980s, perhaps as early as 1984, and has been a product of Sequoia since about 1987. Throughout the 1990s and to the present, Sequoia has continued software development. Between 1994 and 2003 the size of the firmware more than doubled: this is a very significant change. **Different version numbers (e.g., 5.00, 6.00, etc.) of the AVC Advantage are significantly different voting machines that differ in their security, accuracy, and reliability.**

60.3 New Jersey statutes prescribe that any voting machine used in the state must be examined by a committee and approved by the chief election official. However, NJSA 19:53a-4 reads, “When such device has been improved, or any improvement or change which does not impair its accuracy, efficiency, or ability to meet such requirements shall not require a reexamination or reapproval thereof.”

60.4 We am not lawyers, and we will not attempt to interpret the exact legal meaning of this sentence. However, we can say as technical experts that each of the changes made between major version numbers¹¹⁹ of the AVC Advantage (e.g., from version 5 to version 8, or version 8 to version 9) are substantial enough that they can be expected to affect or impair the accuracy, efficiency, or ability to meet the technical requirements imposed by NJSA 19. We will give some examples in the next two sections of this report.

¹¹⁹ For this analysis, and for the table in ¶60.5, we are relying on a “version history” summary that we found in the Source Code of the version 9.00H AVC Advantage, provided to us for examination. For information on AVC Advantages versions 10.x, we are relying on reports from Wyle Laboratories.

60.5 The following table demonstrates that the AVC Advantage firmware is a moving target: it differs substantially in functionality from year to year.

Version	date	notable added features
5.00	1994	multiple ballots
6.00	1995	post-QAT
7.00	1996	expanded option switches; early voting
8.00	1997	dozens or hundreds of bug fixes and minor changes
8.00A	1998	mostly documentation changes
8.00B	1998	bug fix
9.00	2003	FEC modification requests; audio voting
9.00C	2003	bug fixes; update to FEC coding standards
9.00D, E	2003	
9.00F, G	2004	
9.00H	2005	a few changes related to audio voting and/or FEC requirements
10	?	Daughterboard computer now “main CPU”
10.5	?	Voter-verified paper ballot?

Although some of these changes have rather cryptic names (e.g., “Post-QAT”), the main point is that there have been many changes to the computer program: different AVC Advantage models use different methods to handle ballots and count votes.

60.6 In approximately 2003, Sequoia added the audio voting feature, to accommodate disabled voters who cannot use the full-face visual interface. This was a major change, because the 1976-vintage Z80 computer used in the 1980s design is not powerful enough to handle audio. Therefore Sequoia added an “audio kit” containing a second processor to drive the headphones used by disabled voters. The audio kit comprises a daughterboard (inside the cabinet) containing a second computer, and a hand-held unit containing yet a third computer.

60.7 The daughterboard processor is much more powerful than the Z80: it is an AMD Elan SC400 processor (Intel 486 compatible) with 2 megabytes of flash memory and 8 megabytes of RAM.

60.8 The Z80 motherboard communicates with the daughterboard via a three-wire connection that implements the RS-232 serial protocol. The motherboard (containing the Z80) is directly connected to the voter panel, the operator panel, and the results cartridge; the daughterboard has no direct connection to these devices. In addition, the daughterboard can connect to an external I/O device, the “Audio Voting Assembly.”

- 60.9 The Audio Voting Assembly is a black plastic box that the disabled voter can hold in his or her hand, and into which one plugs the headphones or other devices. It has several user-interface buttons and contains a DSP (digital signal processor chip) that plays PCM (pulse-code modulation) audio files sent to it by the daughterboard computer.
- 60.10 In version 9, which we examined, the Z80 is considered the main computer, and the audio-kit daughterboard contains a smaller “granddaughterboard” with a 486-compatible processor. The source code refers to the audio kit as the “subsystem.”
- 60.11 Starting from version 10 (also known as D10), the Intel 486-compatible processor on the daughterboard is considered the “main processor,” while the Z80 on the motherboard is relegated to the role of “I/O processor.”¹²⁰ From our examination of version 9.00H, we can say that this characterization (“main” 486, “I/O processor” Z80) does not apply to version 9. In the version 9 AVC Advantage, the motherboard Z80 is clearly the main processor, and the 468-compatible daughterboard just handles audio ballots. The software changes to move the “main” functionality of the machine from the motherboard to the daughterboard are likely to be very substantial, and this change introduces severe security vulnerabilities; see Section 61.
- 60.12 **Conclusion.** From a technical point of view, each version of the AVC Advantage is sufficiently different that one cannot examine one of these versions and from that draw conclusions that a different version securely and accurately counts the votes. Therefore we believe that each version of the AVC Advantage should be separately examined for security and accuracy before it is used.

61 Version 10 AVC Advantage is extremely vulnerable to fraud

- 61.1 **Summary: The new Sequoia AVC Advantage, version 10, has very similar hardware to the version 9, but the firmware has been completely overhauled. Evidence shows that the firmware has not just been modified, but is mostly new. Because most of the functionality is now on the daughterboard, and the daughterboard is less secure than the mother board, this model should be considered significantly more vulnerable to fraud than the version 9 machines.**

¹²⁰“Hardware Qualification Testing of the Sequoia AVC Advantage DRE Voting Machine (Firmware Version 10.1.5),” Wyle Laboratories, Report No. 51884-08, April 12, 2006.

61.2 Sequoia’s successor to the version 9 AVC Advantage is called the “AVC Advantage D10.” This is the only version of the AVC Advantage to which Sequoia is able to attach its proposed voter-verified paper ballot printer. Mr. Cramer of Sequoia testified before this Court in 2006 that the new printer does not attach directly to the Z80 motherboard; instead, it attaches through the daughterboard. All of the different prototype Advantage-with-ballot-printer machines that Sequoia has provided to the state for testing, or to the New Jersey Voting Machine Examination Committee, are version 10 AVC Advantage machines. The Wyle Laboratories reports that Sequoia has provided to the State in connection with these Advantage-with-ballot-printer machines describe it as version 10.

61.3 A Wyle Laboratories report¹²¹ on one version of the D10 characterizes its internal architecture as follows,

- **“Main CPU:** This is an embedded AMD Elan SC400 based system, running ROM-DOS. It contains 8 MB of DRAM, 2 MB of Flash ROM (used for application program storage, ballot definition, and vote data storage), a PCMCIA slot (used for the results cartridge), a battery backed real time clock, and a serial port for communication with the I/O Board.
- **“I/O Board CPU:** This is the original Z80 CPU. With firmware version 10, it manages I/O devices and communicates via a dedicated serial port with the Main CPU. It contains program ROM, system ROM, configuration ROM, time and date clock, backup batteries, timers and counters, speaker (beeper), and additional circuits for self-monitoring, connecting the other assemblies, and controlling AVC power consumption.”

61.4 This hardware configuration is almost the same as the *hardware* configuration of the version 9 model. However, the large-format battery-backed results cartridges (plugged into the Z80 motherboard) are no longer used. Instead, the PCMCIA cartridge that plugs into the daughterboard computer (which is now the “Main CPU”) is now called the “Results Cartridge.” In the version 9 model, this PCMCIA cartridge was used primarily for audio ballot files and for installing new software into the daughterboard computer.

61.5 Although the hardware is much the same, the software configuration is very different: Sequoia has migrated much of the election functionality to the Intel-486-

¹²¹ Hardware qualification testing of the Sequoia AVC Advantage DRE voting machine (Firmware version 10.1.5), Wyle Laboratories, report number 51884-08, April 12, 2006.

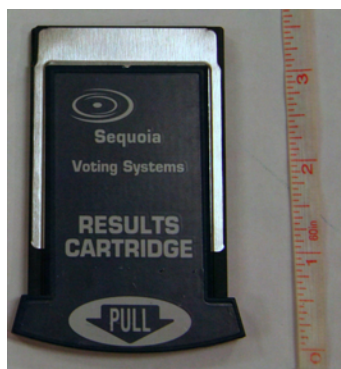


Figure 37: *This cartridge, used only for audio ballots on AVC Advantage 9.00, is used as a Results Cartridge on AVC Advantage 10.*

compatible daughterboard computer. The Wyle ITA report on this machine, in the section on the firmware, says,

“The Sequoia AVC Advantage X.1 was a significant change from 9.00H.1 with half of the files being brand new.

“No change log was supplied.”¹²²

The significance of “no change log” is this: When making modifications to a piece of software, it is standard industry practice to keep a change log—not just for outside examiners, but for the use of the engineers developing the software. If one considers some piece of software to be mostly or completely new, one might discard the change log. Therefore we conclude that the Sequoia engineers consider the AVC Advantage version 10 to be a *new* voting-machine control program, not principally a modification of an old one.

61.6 The architecture of the D10 model is a cause for concern, because the control program for the “Main CPU” is kept entirely in flash memory. In contrast to the version 9 AVC Advantage, in which some of the most dangerous attacks required the use of a screwdriver (to physically replace ROMS), in the D10 the virus attacks described in section 20 will be able to install vote-stealing programs directly into the main processor, where they have direct access to all vote data.

61.7 This is a severe vulnerability, and the AVC Advantage D10 model should be considered extremely insecure, pending a detailed study of that machine. This design is also in violation of FEC standards.¹²³

¹²²*Id.* (Wyle 51884-08), p. B-27

¹²³ See footnote 48 on page 57

61.8 **The severe insecurities in the AVC Advantage version 10 are significant because the version 10 is the only upgrade path that Sequoia proposes for added voter-verified paper ballots (VVPAT) to the AVC Advantage.**

61.9 On May 22, 2008 the New Jersey Voting Machine Examination Committee, chaired by Mr. Richard Woodbridge, held a hearing on the AVC Advantage model D10 DRE with voter-verified paper ballot printer. Appel attended this hearing. Mr. Woodbridge made it clear that this was not a certification hearing for the AVC Advantage voting machine itself, but only for the printer attachment.

61.10 In a letter of May 27, 2008 to Mr. Woodbridge, Appel explained the risk, in the D10 version of the Advantage, of viral propagation of fraudulent firmware. He explained that the design change to the AVC Advantage between version 9 and version 10 are very substantial. He explained that this change does “impair the accuracy” of the AVC Advantage. For that reason he urged Mr. Woodbridge to hold a full certification hearing on the AVC Advantage D10 voting machine, not just on the printer attachment.

61.11 The basic information in Wyle’s report on the AVC Advantage D10 (¶61.3) was enough for Appel to be able to deduce the existence of this problem and alert Mr. Woodbridge. (His conclusions have been strengthened by the subsequent examination we made of the AVC Advantage 9.00.) The fact that the Wyle examiners did not report on the security vulnerabilities caused by this design is evidence of the inadequacy of ITA reports. The fact that Mr. Woodbridge did not notice this problem, in reading the Wyle report on the D10, is evidence of the inadequacy of the current examination/certification process in New Jersey.

61.12 On June 25, 2008, Mr. Woodbridge’s committee recommended to the Secretary of State the approval of the AVC Advantage model D10. They did so without performing a certification examination of the voting machine, but only of the printer attachment. No certification examination or hearing on the entire D10 machine, not just on its printer, has been done in New Jersey.

62 Version 8 AVC Advantage is vulnerable to fraud in some ways that version 9 is not

62.1 **Summary: Mercer County owns 50 of the version 8 AVC Advantage machines. These earlier models of the AVC Advantage, before version 9, are vul-**

nerable to fraud in certain ways that do not apply to the version 9 machine.

62.2 Most of Mercer County’s AVC Advantage machines are version 9.00G. In addition, Mercer County has 50 version 8.00 AVC Advantage machines that are used as backup spares during elections and for high school elections.¹²⁴ It is our understanding that backup spares are used in real elections, especially as replacements for machines that fail in the polling places.¹²⁵

62.3 We examined version 9.00H AVC Advantage machines, source code, and firmware. From the source code we can make inferences about version 8.00 AVC Advantage machines, and prior versions. The evidence for these inferences includes

1. Revision histories and change logs;
2. Vestigial, inactive program code;
3. Inconsistencies between comments and code, providing evidence of previous functionality in the code.

From this evidence we conclude the following.

Execution from Program RAM permits fraudulent firmware to be easily installed

62.4 In version 8 and before, insertion of a “Program Cartridge” into the Auxiliary Port would cause Z80 executable code to be transferred to Program RAM, and then this Program RAM could be mapped to the Z80 program address space and executed. A comment in the Source Code dated April 23, 2002 (i.e., after version 8, during the development of version 9) indicates the removal of this functionality. In the program code itself, we find some vestigial remainders of this functionality, such as the designation of certain numbers as “Program RAM bank numbers”.

62.5 Execution of programs from RAM constitutes a serious security vulnerability. It can permit vote-stealing firmware to be installed simply by plugging a Program Cartridge into the Auxiliary Port. Appendix F describes how the version 8 AVC Advantage was designed to permit execution of programs in RAM from “program cartridges.”

¹²⁴Statement of Assistant Attorney General Donna Kelly to the Court, July 22, 2008.

¹²⁵As is the practice, for example, in Camden County; Bates Number CAM 0001–0002.

62.6 Therefore, we conclude that Version 8 (and prior) releases of the AVC Advantage are potentially *severely vulnerable* to the installation of vote-stealing software *simply by inserting a cartridge into the Auxiliary Port, without removal of the circuit board cover.*

The ability to reprogram ballots on the version 8 AVC Advantage constitutes another security vulnerability.

62.7 In normal use, a county uses the EDS or WinEDS program to program ballot definitions into Results Cartridges; then these Results Cartridges are inserted into the AVC Advantage voting computers.

62.8 However, in version 8 and prior, it was possible to program ballot definitions into Results Cartridges directly from an operator-panel menu of an AVC Advantage machine. This may have provided a way to manipulate elections, and was criticized by election security experts. This feature of the AVC Advantage was removed, apparently in 2001, and is no longer present in version 9.

63 Conclusion of Part VII

63.1 The AVC Advantage has been produced in many versions. The firmware—the computer program that decides how to count the votes—functions significantly differently from one version to another. The accuracy of one version may be therefore quite different from the accuracy of another version. 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. New Jersey should not use any version of the AVC Advantage that it has not actually examined with the assistance of skilled computer-security experts.

PART VIII

CONCLUSIONS AND RECOMMENDATIONS

64 New Jersey should not continue to use the AVC Advantage 9.00, because it is insecure

64.1 **Summary: Paperless DREs in general, and the AVC Advantage in particular, lack the crucial quality of “software independence.” Therefore, the choice of election results in each precinct is entirely at the discretion of the computer software/firmware, and not independently checked. Therefore they cannot be trusted to count the votes.**

64.2 In Section 16 we explained the scientific consensus, with which we concur, that paperless DRE voting machines are inherently susceptible to fraud because they lack *software independence*. That is, how the votes are recorded and counted depends on the software (firmware) inside the DRE machine, and is not independently checkable.

64.3 Not only is the AVC Advantage 9.00 (used throughout New Jersey) *inherently* susceptible to fraud and error because it is a paperless DRE, but we found in our examination that it is particularly and specifically susceptible. In this report we have explained those specific vulnerabilities.

64.4 This makes the AVC Advantage unsafe for use in elections: it cannot be trusted to count the votes legitimately.

65 New Jersey should immediately remove the Audio Kits

65.1 **Summary: The audio kits are grossly insecure, making it easy to steal the votes of disabled voters. Their insecurity makes the rest of the machine less secure as well.**

65.2 As we explained in ¶24.4, on the AVC Advantage 9.00 the votes of disabled voters are even more vulnerable (to theft by computer virus) than the votes entered on the full-face voter panel. Therefore, with great respect for the rights of disabled

citizens to be accommodated, but with particular concern for the protection of the *votes* of disabled voters, we recommend that New Jersey remove the Audio Kits from all its AVC Advantage voting machines.

- 65.3 Removing the Audio Kits is a simple and immediate matter. Even after they are removed, the AVC Advantage will have severe insecurities and sources of inaccuracy. However, removing the Audio Kits also removes the possibility of viral propagation of fraudulent firmware.
- 65.4 Removing the Audio Kits can be done safely as little as one month before an election. Counties will have to set one option differently in their ballot-definition programming: the option to enable/disable audio ballots. If the audio ballot is disabled, then the motherboard will not even attempt to communicate with the audio kit.
- 65.5 Even so, removing the Audio Kits is problematic for two reasons. First, it means that the AVC Advantage will not be usable by certain disabled voters without a person to assist them, which means that the Advantage machines would not be HAVA-compliant. Second, it cuts off the upgrade path to a voter-verified paper ballot since Sequoia's VVPAT printer is connected through the audio kit and not directly to the Z80 motherboard.

66 There is a way to safely use computers to count votes

- 66.1 Software independence does not mean that computers (and computerized voting machines) cannot be involved in elections. It means that any calculations done by the computers must be verifiable independently of the computer program. In fact, it is reasonable and often desirable to have computers involved in elections, as long as software independence can be achieved.
- 66.2 The *only* currently available technology that combines computer technology with software independence is the *voter-verified paper ballot*. That means an individual paper record of each vote cast, seen and verified by the voter at the time the vote is cast, collected in a ballot box so that it can be recounted by hand if necessary.
- 66.3 Not every precinct must be recounted by hand. Only a very small statistical sample of precincts or ballots needs to be audited, just to defend against the possi-

bility of systematic, widespread fraud or error in the computer-counting firmware. A New Jersey law passed in 2008 now requires just this kind of audit.

66.4 Combining a computer count of the ballots with a hand audit gives the best of both worlds. Because the modalities of fraud or error are very different for computer software/firmware and for hand counting, each kind of count will serve as a check on the other. Someone who wishes to cheat will have to ensure that a fraudulent firmware miscount comes out exactly the same as the fraudulent paper recount, and this is not easy to accomplish.

66.5 None of what we say in this section would come as news to the New Jersey Legislature, which in 2005 passed a law requiring voter-verified paper ballots and in 2008 passed a law requiring statistical audits of those ballots. For the reasons discussed throughout this report, those laws should be implemented immediately in order to protect the votes of New Jersey voters. Not only is the AVC Advantage 9.00 noncompliant with those laws from a technical point of view, but it is substantively insecure, as we have explained in this report. Therefore we recommend that the AVC Advantage be replaced with a more secure technology, as we will explain in the next section.

67 Forms of voter-verified paper ballots

67.1 Voter-verified paper ballots are available in three forms, using currently available technology: hand counted paper ballots; optical-scan ballots counted by computer; and paper ballots automatically printed by DRE voting machines.

67.2 **It is the overwhelming consensus of those computer scientists who have studied voting technology that the most trustworthy, robust, and reliable form of voter-verified paper ballot is the precinct-count optical-scan ballot.** We will explain what this means, and why this is.

67.3 An optical-scan ballot is a paper ballot printed with contests and candidates. The voter fills in an oval (or connects an arrow) by the candidates she chooses. In “central-count optical scan,” the voter then deposits the ballot into a ballot box. At the close of the polls, the ballot box is taken to a central location where a high-speed optical scanner counts the ballots for many precincts.

67.4 In contrast, in “precinct-count optical scan” the voter feeds the optical-scan ballot directly into a scanning machine. This machine counts the ballot and de-

posits it into a ballot box. Immediately at the close of the polls, the election results for that precinct are printed by the scanning machine. The sealed ballot box full of optical-scan ballots is available for hand recounts, which can be done to audit the count made by the scanning machine.

- 67.5 Optical-scan voting has very significant advantages over DREs equipped with paper-ballot printers:
- 67.6 • The more voters actually examine and verify the choices written on their paper ballots, the more useful a statistical audit is. There is quite a bit of doubt about how closely voters examine the paper ballots printed for them by DRE machines after they make their choices electronically. In contrast, voters who filled out an optical-scan form *made the marks themselves*, which means they are much more likely to know what marks are there.
- 67.7 • Voting machines of all kinds can malfunction, or fail to turn on at all. In the case of a DRE, even with a ballot-printer, the voters cannot vote. With optical scan ballots, voters can still use a pencil to mark their ballots without any difficulty. If a precinct-count machine fails to operate, voters can simply deposit their ballots into the ballot box for counting later.
- 67.8 • Only one person can use a DRE at a time. If the ballot is very lengthy or complex, this can take several minutes, especially with the review of the DRE-printed paper ballot. In contrast, several voters using optical-scan ballots can fan out into several (cheap) voting booths and use several (cheap) pencils to fill out their ballots. When each voter has taken as long as she wants to fill out and review the ballot, she can emerge from the booth and deposit the ballot into the machine.
- 67.9 • Fewer optical-scan machines are needed (per precinct) than DRE voting machines. This is mainly for the reason described in the previous paragraph, but also for another reason. It is best to have two DRE machines in every precinct, even if there are not very many voters, just in case one fails—it takes two hours or more to dispatch a spare by truck if one machine fails.¹²⁶ In contrast, optical-scan ballots are still very usable by voters even if the scanner fails.
- 67.10 • With DRE-plus-printer, there is a difficult and ambiguous situation if the voter claims that the machine is printing choices that do not correspond to the voter's choices. Either the machine is cheating (or malfunctioning); or the

¹²⁶ Records of replacement machines delivered to precincts, Bates Number CAM 000297–000299

voter is lying (or mistaken). The pollworker cannot know which is the case without violating the privacy of the ballot—and in any case, resolving this kind of touchy situation is one that we should not have to ask of pollworkers. In contrast, there can be no doubt about the selections written on an optical-scan ballot, because the voter (and only the voter) wrote those selections with a pencil.

- 67.11
- The user-interface of optical-scan ballots is simple and intuitive. That is not to say it is perfect—like the Sequoia AVC Advantage DRE, optical-scan ballots have difficulty giving the voter feedback about undervotes (see Section 33). But the system is understandable by voters, and they have no difficulty knowing whether their ballot has been cast.

67.12

Precinct-count preferred to central-count. Of the two forms of optical-scan voting, it is the overwhelming consensus of experts (not just computer scientists but others as well) who have studied these technologies that **precinct-count optical-scan is preferable to central-count optical-scan**. This is for two main reasons:

1. Precinct-count optical-scanners can practically eliminate the rate of overvoted and otherwise voided ballots by giving immediate feedback to the voter. If the voter feeds an overvoted or otherwise invalid ballot into a precinct-count optical-scan machine, the machine spits it back out with a message informing the voter about the problem. The voter then has a chance to correct the problem, either win an eraser or by having his ballot destroyed and receiving a fresh ballot from election workers.¹²⁷
2. Precinct-count optical-scanners deliver a total immediately at the close of the polls, in the presence of witnesses, before there is any question of chain-of-custody. In contrast, when a ballot box that is to be centrally counted leaves the polling place, it is subject to manipulation, stuffing, and replacement before it reaches the central-count facility.

67.13

In conclusion, it is our own opinion—and that of the overwhelming consensus of election technology experts—that precinct-count optical scan is the most trustworthy, robust, and cost-effective method of voting that is now available. we recommend that New Jersey adopt precinct-count optical scan technology.

¹²⁷ Usually there is an override available: if the voter is in a hurry to leave, he can cast the ballot anyway; the overvoted *contest* will be void, but all the other contests she voted in will count.

68 SUMMARY OF CONCLUSIONS REACHED IN THIS REPORT

68.1 **Part I.** 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 this “hack” takes just 7 minutes to perform.

The fraudulent firmware can steal votes during an election, just as its criminal designer programs it to do. 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 manipulate them all simultaneously.

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

68.3 **Part III.** Design flaws in the user interface of the AVC Advantage disenfranchise voters, or violate voter privacy, by causing votes not to be counted, and by allowing pollworkers to commit fraud.

68.4 **Part IV.** 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.

68.5 **Part V.** Sequoia’s sloppy software practices can lead to error and insecurity. Wyle’s ITA reports are not rigorous, and are inadequate to detect security vulnerabilities. Programming errors that slip through these processes can miscount votes and permit fraud.

68.6 **Part VI.** Anomalies noticed by County Clerks in the New Jersey 2008 Presidential Primary were caused by two different programming errors on the part of Sequoia, and had the effect of disenfranchising voters.

68.7 **Part VII.** 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. New Jersey should

not use any version of the AVC Advantage that it has not actually examined with the assistance of skilled computer-security experts.

68.8

Part VIII. The AVC Advantage is too insecure to use in New Jersey. New Jersey should immediately implement the 2005 law passed by the Legislature, requiring an individual voter-verified record of each vote cast, by adopting precinct-count optical-scan voting equipment.

PART IX

APPENDICES

A Memory Devices

A.1 In evaluating the security of the AVC Advantage, We considered all of its memory devices in which executable software/firmware could, in principle, reside. These are the ones that are relevant to the installation of fraudulent vote-stealing firmware. Of these memories, we mark with a * those memories from which instructions are directly executable.

***Z80 Program ROM.** Three 128 KB EPROM chips located on the Z80 motherboard, mappable (in 16 KB segments) into the lower 32 KB of the Z80 address space.

***Z80 Program RAM.** One 32 KB SRAM chip (optional) located on the Z80 motherboard, mappable (in 16 KB segments) into the lower 32 KB of the Z80 address space. Was not installed in the 9.00H machines we examined from Union County, NJ. Was not installed in the 8.00D machine we purchased from Buncombe County, NC.

Configuration ROM. One 8 KB EPROM chip located on the Z80 motherboard. Accessible to the Z80 by I/O instructions.

Direct-mapped data memory. One 32 KB SRAM located on the Z80 motherboard. Mapped into the upper 32 KB of the Z80 address space, except that the highest 1 KB may of the Z80 address space may be mapped to other devices.

Audit trail memory. One or two 128 KB SRAMs located on the Z80 motherboard. Mappable (in 1 KB segments) into the highest 1 KB of the Z80 address space.

8 KB SRAM. One 8 KB SRAM located on the Z80 motherboard. Accessible to the Z80 by I/O instructions.

Real-time clock chip. A few tens of bytes of storage, accessible to the Z80 by I/O instructions.

Results cartridge. A removable cartridge containing 96 KB (or other amounts) of battery-backed SRAM, that plugs into the port on the motherboard marked "Results Cartridge". Accessible to the Z80 by I/O instructions.

Auxiliary cartridges. A removable cartridge that plugs into the port on the motherboard marked “Auxiliary cartridge”. These may be “results cartridge,” “simulation cartridge,” “technician cartridge,” or other. See section 44. On the 9.00H model (but not on the 5.00D model) this “auxiliary” port can also connect to other devices, including but not limited to the audio-kit daughterboard. All these devices are accessible to the Z80 by I/O instructions.

***Daughterboard RAM.** The daughter-daughterboard is a Compublab 486CORE printed circuit board, approximately 2x3 inches, containing an 80486-compatible processor, an 8 MB DRAM, and a 2 MB flash memory. We refer to the 8 MB DRAM as the “daughterboard RAM”. It is directly mapped into the address space of the 486-compatible computer.

Daughterboard flash memory. The 2 MB flash memory on the daughterboard (AVC Advantage versions 9 and 10) is formatted as a Microsoft standard (FAT) file system. This flash memory is not directly executable, but, the daughterboard operating system probably has a bootstrap loader that automatically copies from the onboard Flash memory and/or the Audio Ballot Cartridge to the DRAM on start-up.

Audio ballot cartridge. A PCMCIA cartridge, typically 64 MB, that plugs into a PCMCIA slot on the top of the audio kit (daughterboard). Formatted with a FAT file system. Most probably accessible to the 486CORE processor as a virtual disk drive.

DSP flash memory. On the Audio Voting Assembly there is a (probably) DSP processor with (probably) a flash memory containing executable program as well as data.

B Buffer overrun reading messages from daughterboard

[REDACTED]

3 pages redacted

[REDACTED]

C Technical details of the option-switch bug that disenfranchised some primary voters

[Redacted]

2 pages redacted

[Redacted]

D How the ballot images can be unshuffled, thereby violating voter privacy

[Redacted]

2 pages redacted

[Redacted]

E The Source Code violates the FEC's software-engineering guidelines for voting-machine firmware

[Redacted]

4.5 pages redacted

[Redacted]

F Installing fraudulent software into Z80 Program RAM

[Redacted]

2.5 pages redacted

[Redacted]

G The security measures in Technician Cartridges are easily defeated

[Redacted]

1.5 pages redacted

[Redacted]

H Printer inaccuracy can change vote totals in results report

- H.1 **Summary: The AVC Advantage printer does not have a mechanism to overcome transmission errors in the printer cable. This could in principle cause erroneous vote totals to be printed, but we do not believe it is a very significant source of inaccuracy.**
- H.2 The AVC Advantage has a printer mounted inside the cabinet, accessible by opening the rear door. This printer is used to print Results Reports after the close of the polls, listing the vote totals for each candidate. These reports are signed by the election-board workers.
- H.3 The AVC Advantage Z80 computer communicates with the printer using a standard parallel printer cable, of the kind that was used on personal computers in the 1980s and 1990s. There is no error-checking on this cable, neither parity checking nor checksums of any kind. If at any time a localized electrical failure, radio interference, or other transient signal causes a 0 signal to be transmitted as 1, or vice versa, the wrong character would be printed on the Results Report. Such intermittent failures could be also caused by a corroded contact on the connector plug, for example.
- H.4 We performed the following experiment to demonstrate the lack of error-checking on the printer cable. We simulated a bad connection by unplugging the Centronics-style parallel connector from the printer, and putting a tiny piece of paper over one of the connectors, corresponding to the low-order bit in the ASCII code. Then we plugged the connector back in with the paper in place. Therefore no electrical signal could flow through this pin of the 36-pin connector.
- H.5 The printer did not detect any error, and did not report any error to the AVC Advantage's Z80 computer. All characters were transmitted with low-order bit =1; that is, the letter "b" printed as "c", the number 6 printed as 7, and so on.
- H.6 Therefore it is possible that a bad connection could cause intermittent failures of this type. Such a connection could be caused by a corroded contact in the plug at either end of the printer cable, or by a bad solder joint. Depending on which wire of the cable had an intermittent failure, it is possible for the digit 1 to change to 9, or 0 to 8, or 3 to 7, or 2 to 3, and so on. In general, numbers could be misprinted as too large by any of the following amounts: 1, 2, 4, 8, 10, 20, 40, 80, 100, 200, 400, 800.

H.7 Thus, the printer can print erroneous numbers, and the AVC Advantage machine is incapable of detecting the error. However, at present we cannot say that this kind of error is likely to happen.

I Inadequate indications of undervotes

I.1 In section 33, we explain that the AVC Advantage has been found to have a high rate of undervotes. In this appendix we explain what mechanisms AVC Advantage permits election officials to use, to try to prevent undervotes, and why these are not very successful.

I.2 Computer scientists study user interface design, so that their computer programs can better “understand” and carry out the intent of the user. User-interface issues are also important in voting machines and ballot design.

I.3 The election official should design the printed ballot on the paper covering the voter panel so as to clearly lay out the contests. In this respect, at least in the elections we have observed in New Jersey, the election officials (as users of this software) lay out the ballots as clearly as this full-face technology permits. However, when there are many races, *especially* when there a mix of partisan contests and nonpartisan contests, the voter will inevitably be presented with a large amount of information at once: she must find all the contests on the ballot. (See Figure 2 on page 11) In general we would not fault the way that election officials in Union County and Mercer County lay out the ballots: *they are doing the best they can within the limitations of the technology of the voting machine.*

I.4 The Cast Vote button does not light, and remains inactive, until at least one contest has been voted. But this solves the problem only partially: it mostly prevents a 100 percent undervote by a voter, but does not help remind the voter to vote every contest.

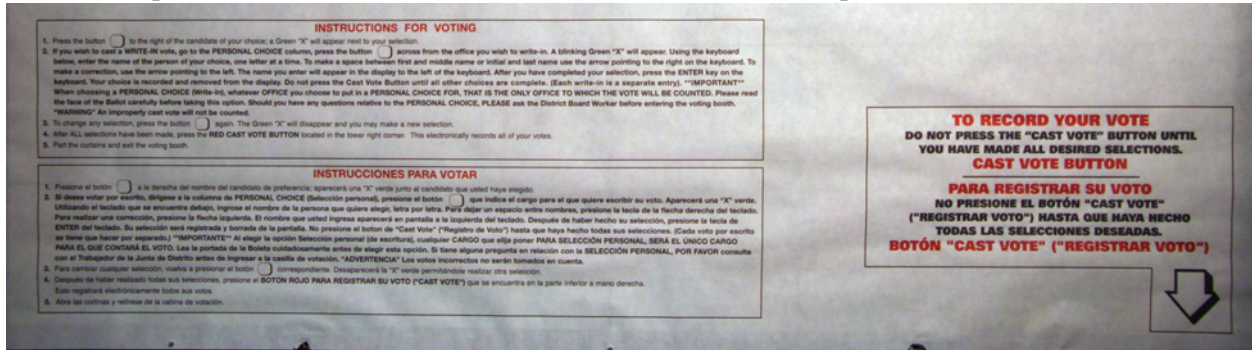
I.5 As another reminder, the bottom right portion of the printed ballot says



TO RECORD YOUR VOTE
DO NOT PRESS THE “CAST VOTE” BUTTON UNTIL
YOU HAVE MADE ALL DESIRED SELECTIONS.
CAST VOTE BUTTON

followed by the same message in Spanish. The entire display occupies a space of about 10 inches by 5 inches. There is a similar message, shorter and smaller, to the

left of the button itself, in English only. In fact, the large full-face ballot is densely printed with textual instructions, which in itself becomes a problem.



I.6 The green X lights up by each candidate selected. This is useful feedback, but may not help the voter who has overlooked one part of the large voter panel. For example, suppose the ballot is laid out such that all the *candidate* contests are in one large grid at the center-left of the voter panel, and all the *public questions* are at the right. It is easy for voters to overlook the public questions.

I.7 A green X can be made to light up in the “contest header” of each undervoted contest. We describe this below.

I.8 **Xs in contest headers.** Suppose there are three races on the ballot, for President, for Senator, and for Representative. The printed page looks like this:

	DEMOCRATIC	REPUBLICAN	GREEN
President	Smith <input type="checkbox"/>	Jones <input type="checkbox"/>	Johnson <input type="checkbox"/>
Senator	Bobkin <input type="checkbox"/>	Dobkin <input type="checkbox"/>	Froomkin <input type="checkbox"/>
Representative	Harman <input type="checkbox"/>	Fenwick <input type="checkbox"/>	Menn <input type="checkbox"/>

I.9 If the “Xs-in-contest-headers” feature is enabled in the ballot definition, then *when the machine is initially Activated* the ballot will be presented like this, with the X’s illuminated in green:

	DEMOCRATIC	REPUBLICAN	GREEN
President ×	Smith <input type="checkbox"/>	Jones <input type="checkbox"/>	Johnson <input type="checkbox"/>
Senator ×	Bobkin <input type="checkbox"/>	Dobkin <input type="checkbox"/>	Froomkin <input type="checkbox"/>
Representative ×	Harman <input type="checkbox"/>	Fenwick <input type="checkbox"/>	Menn <input type="checkbox"/>

I.10 If the voter presses the box next to “Smith”, then the X by “President” goes out, and the X by “Smith” illuminates:

	DEMOCRATIC	REPUBLICAN	GREEN
President	Smith × <input type="checkbox"/>	Jones <input type="checkbox"/>	Johnson <input type="checkbox"/>
Senator ×	Bobkin <input type="checkbox"/>	Dobkin <input type="checkbox"/>	Froomkin <input type="checkbox"/>
Representative ×	Harman <input type="checkbox"/>	Fenwick <input type="checkbox"/>	Menn <input type="checkbox"/>

I.11 The Xs by “Senator” and “Representative” are still lit, indicating that these contests are not yet voted. However, at this time the Cast Vote button illuminates, indicating that the voter is permitted to cast this ballot (and thereby undervote in the Senator and Representative races).

I.12 Although the purpose of this user-interface design (that is, illuminate the X in the contest header to indicate undervote) is supposed to help the voter avoid undervoting, in fact some voters find it confusing. We have informally interviewed voters, after elections, about their use of these machines. Many voters do not really understand what the user-interface is trying to tell them. This is especially true when this method is applied to Public Questions, the X in some cases appears right in the middle of the text of the public question, which some voters find mysterious.

I.13 **In general, the prompting of the voter (to avoid undervotes by those not expert in the operation of the machine) is barely adequate and not completely effective. This can lead to undervoting, and thus impairs the accuracy of the AVC Advantage in recording the voter’s intent.**

J Cumbersome procedure for dealing with fleeing voters

J.1 **Summary: In Section 37, we explained that the AVC Advantage’s procedures for handling fleeing voters leave opportunities for violating the privacy or integrity of the ballot. Here we describe those procedures.**

J.2 A voter who makes one or more selections, and then leaves the booth without pressing Cast Vote, is known as a “fleeing voter.”

J.3 As we explained in the previous section, the user interface of the AVC Advantage is not completely intuitive. In addition, on the AVC Advantage the Cast Vote button is far below, and to the right, of the voter’s line of sight and focus of

attention—the contests and candidates printed on the full-face ballot. Therefore some voters forget to press the Cast Vote button.

J.4 In the old days of mechanical lever machines, the “cast vote” lever caused the curtain to open behind the voter. Thus, the voter was (gently) physically restrained from leaving the booth by the curtain. The AVC Advantage does not have such an automatic curtain, and it would not be practical to add one.

J.5 If the voter leaves an AVC Advantage without pressing Cast Vote, the operator can tell from indications on the LCD display on the operator panel that the vote has not been cast (and also the barely audible chirp has not been heard). The operator is supposed to remind the voter to press Cast Vote.

J.6 If the voter has already left the polling place, then the operator must follow a certain procedure, as dictated by the regulations of the County or State (etc.), for fleeing voters. Usually the intent of this procedure is to record the voter’s selections (already made on the machine) as if she had pressed Cast Vote.

J.7 The procedure that pollworkers have to follow in order to “clean up” after a fleeing voter is very cumbersome.

J.8 **The procedure requires the pollworker to reach into the booth without looking, and to press the ENTER button followed by Cast Vote. But the ENTER button is set nearly flush in a panel with many other buttons, and is very difficult to press without looking. In practice, to accomplish this procedure the pollworker may find it necessary to enter the booth, where the voter’s selections are visible and changeable.**

J.9 The Sequoia AVC Advantage Operator’s Manual prescribes no procedure for fleeing voters.

J.10 From our examination of the machines, we have found that the following procedure works. Unlock the back door of the machine with the key; press the PRINT MORE button. This records the selections made by the voter (up to the point where she fled), as if CAST VOTE were pressed, and records a Fleeing Voter for subsequent printed reports. Actually, PRINT MORE is more powerful than CAST VOTE, for the following reasons:

- If the voter has made no selections at all, and if the ballot definition programmed into the Results Cartridge prohibits blank ballots, then CAST VOTE

will not do anything.¹²⁸

- If Audio Voting is in use (e.g., by a disabled voter), then the voter panel (including CAST VOTE) may be inactive.

J.11 Even so, the PRINT MORE button is not a completely effective way of handling fleeing voters. If a Personal Choice (write-in) has been selected, and the write-in name has not been completed by pressing the ENTER key below the voter panel, then the CAST VOTE button has no effect, and neither does PRINT MORE.

J.12 Consequently, a more complicated procedure is prescribed to pollworkers by Mercer County,¹²⁹ is as follows. First, ask the voter to return to the booth to press the CAST VOTE button. But “If the voter has left the polling place, perform the following steps:

“1. Reach underneath the curtain (without going into the voting unit) and press the ENTER button on the Write-In Keypad,¹³⁰ and then press the CAST VOTE button. If the four signals¹³¹ listed in Assuring the Voter Voted Properly occur, the voting unit is ready for the next voter.

“If these signals do not occur, it means the previous voter left the voting booth without making any selections (known as a fleeing voter).

“2. When the next voter arrives, allow them to vote at the booth.

“3. Make note of the voter fleeing in the official documents.”

J.13 A somewhat different set of instructions is also found in Mercer County’s manual for pollworkers for the Presidential Primary of February 5, 2008.¹³² That is,

¹²⁸Note that in this case, the Mercer County instructions below will lead to a different result. This may be deliberate on the part of Mercer County election officials, perhaps in order to comply with New Jersey election laws. Or it may be that Mercer County officials are unaware of the PRINT MORE feature for fleeing voters, since it is not described in the AVC Advantage operator manual.

¹²⁹Mercer County Board Worker Manual, Revised November 25, 2003, page 18. Bates number MERCER 004647 in *Gusciora et al. v. Corzine et al.*

¹³⁰[footnote mine] Pressing ENTER is difficult to do by feel alone.

¹³¹ [footnote mine, paraphrase summary] (1) chirping noise, (2) light on Operator Panel next to Activate button goes off, (3) display on Operator Panel LCD reads “VOTER INACTIVE,” (4) overhead booth light goes off

¹³² A document entitled, “What to do if..., Presidential Primary Election – February 5, 2008” [ellipsis in original], Bates Number Mercer 004641, page 13. Part of a package of information given as instructions to pollworkers.

Mercer County gives several different instructional documents to its election workers, and two of the documents disagree about procedures for fleeing voters.

- J.14 Mercer County's "What to do if..." document's instructions echo the process of reaching under the door to press the CAST VOTE button, though they do not mention pushing ENTER first. The next step is to wait two minutes and repeat. If the machine still does not cast the ballot, then two board workers, one from each party, are to look inside to see if any contests are voted, and if not the next voter can enter the machine and cast a ballot. The instructions do not specify what to do if the fleeing voter had voted some contests.

K Bug in WinEDS causes ballot programming to be extremely slow

- K.1 **Summary: A bug in WinEDS causes the software to be extremely slow in preparing AVC Advantage cartridges before each election. This limits the flexibility of election officials in dealing with last-minute ballot changes.**

- K.2 WinEDS fails to remove temporary files that are generated during the audio-ballot preparation process. The TEMP directory of Union County's WinEDS computer contained over 7000 useless files. This bug in WinEDS slows down the process of preparing ballot-definition Results Cartridges (with accompanying audio-ballot cartridges) enormously. We found, by examining the dates of these files, that Union County election workers were able to use this machine to prepare only an average of 8 audio-ballot cartridges per day in the weeks before an election! In a county that has hundreds of voting machines, this must be extremely frustrating and inefficient for election workers.

- K.3 In addition to costing the taxpayers money to pay employees or contractors for the extra time it takes to prepare the AVC Advantage voting machines for each new election, this WinEDS bug causes another problem. It means that these employees of the Board of Elections will need weeks more time than necessary to prepare ballot cartridges before an election. In the event that a County Clerk or a Court orders a change in the ballot just a few weeks before an election, the Board of Elections will not have enough time to install the new ballot into the AVC Advantage voting machines.

L The Court Order

In the fall of 2004, the Rutgers Law School Constitutional Litigation Clinic filed a lawsuit seeking to decommission of all of New Jersey's voting computers. Approximately 10,000 voting computers are used in New Jersey; all of them are direct recording electronic computers "DREs," and the vast majority of these DREs are Sequoia AVC Advantages. None of those DREs can be audited: they do not produce a voter verified paper ballot that permit each voter to create a durable paper record of her electoral choices before casting her ballot electronically on a DRE. The legal basis for the lawsuit is quite simple: because there is no way to know whether the DRE voting computer is actually counting votes as cast, there is no proof that the voting computers comply with the constitution or with statutory law that require that all votes be counted as cast.

A critical part of every lawsuit is 'discovery,' i.e., the exchange of information by adversaries in a lawsuit. Discovery is designed to give parties access to their adversaries' documents and other information that is relevant to a lawsuit. Discovery provides litigants with crucial information needed to prove their case, when that information is in the sole custody of their adversaries. In this case the Plaintiffs did not have access to information that would help them prove their case that DREs were unreliable and insecure. The Plaintiffs did not even have the ability to test the DREs they suspected were constitutionally infirm. The DRE voting computers belong to New Jersey's 21 counties. Those counties also have information about DRE malfunctions. Additionally, the Attorney General and Secretary of State ¹³³ also have information about DRE malfunctions, as well as information related to the application for certification of every DRE used in the State.

As part of the discovery process, the Court ordered the defendants (officials of the State of New Jersey) to provide to the plaintiffs: Sequoia AVC Advantage voting machines, the source code to those voting machines, as well as other information that would enable them to support their legal claims. The Sequoia Voting Systems company, which had not been a party to the lawsuit, objected to the examination of their source code by the plaintiffs' experts, on the grounds that the source code contained trade secrets. The Court recognized that concern, and crafted a Protective Order that permitted the plaintiffs' experts to examine the source code while protecting the trade secrets within it. However, the Court Order does permit the plaintiffs' experts to release this report to the public at a specified time.

We delivered our report to the Court and to the defendants on September 2,

¹³³Respectively, the former and current State chief election officer. Until April 2008, the chief election officer of New Jersey was the Attorney General. The legislature modified this, effective April 2008, to conform with the practice in many other states, where the chief election officer is the Secretary of State.

2008. 30 days after that date, on October 2, we were to have been permitted by the Court Order to release our report (but not the source code itself) into the public realm. However, in late September Sequioa filed a motion, alleging that this report revealed protected trade secrets. On October 17, 2008 the Court permitted release of the report as redacted here.

Later this year, the Court will rule on the substance of the trade secret issue, and we expect that she will permit release of the full unexpurgated report at that time.