An Analysis of the Hart Intercivic DAU eSlate

Elliot Proebstel* Sean Riddle* Francis Hsu* Justin Cummins*
Freddie Oakley† Tom Stanionis† Matt Bishop*

June 26, 2007

Abstract

This paper reports on an analysis of the Hart InterCivic DAU eSlate unit equipped for disabled access and the associated Judge's Booth Controller. The analysis examines whether the eSlate and JBC can be subverted to compromise the accuracy of vote totals, the secrecy of the ballot, and the availability of the system under the procedures in place for Yolo County. We describe several potential attacks, and show how election officials can block or mitigate them.

1 Introduction

The use of electronic voting systems reached Yolo County, California in 2006. In order to comply with the Help America Vote Act and California law, county officials provided systems to allow disabled voters to vote without assistance. The county chose Hart InterCivic's eSlate systems[1]. The county continued to use paper ballots for the majority of voters, but each polling station[2] one Disabled Access Unit (DAU) eSlate. Any voter, disabled or not, could use the eSlate system, but the primary voting mechanism was paper ballots that would be optically scanned at Election Central.

The Clerk-Recorder, who is the head election official for Yolo County, had two concerns. First, the poll workers might not have enough experience with computer equipment to feel comfortable setting up and running the eSlate. The vast majority of poll workers in Yolo County are retirees, most of whom are not skilled with computer systems. Second, as the county had never used eSlates (or, indeed, any kind of electronic voting terminal) before, the Clerk-Recorder had to develop policies and procedures to protect the systems from attack. From past collaboration with the Computer Security Laboratory (the "Seclab") at the University of California at Davis, located in Yolo County, the Clerk-Recorder asked if the members of the Seclab could help. We agreed.

To handle the first concern, roughly 30 students were gathered from across campus, most of whom were computer science majors or graduate students working with faculty on computer security projects[3]. Hart, the vendor, held a training session on campus teaching us how to set up, run, tear down, and troubleshoot the eSlates and JBCs. These technical expert volunteers, all with a fair degree of technical sophistication, met at the County seat on Election Day early in the morning. They retrieved the eSlates and delivered them to assigned polling stations. When there, the technical experts set up the eSlates and checked that they were working properly. After all the eSlates were set up, half of this group served as roving troubleshooters. If any polling station had a problem with the eSlate, they called Election headquarters, and a troubleshooter would go help them. The troubleshooters also drove around during the day, checking to be sure there were no problems with the eSlates.

To handle the second concern, the Clerk-Recorder loaned the University 6 eSlates, and asked that we examine them to determine what attacks might be feasible, and what policies and procedures were necessary to block the attack or decrease the chances of an attack succeeding. This paper reports on these efforts.

*Dept. of Computer Science, University of California at Davis, Davis, CA 95616-8562

†Yolo County Elections Office, 625 Court St., Room B05, Woodland, CA

[1] Version 6.1; the eSlate and JBC ran version 4.1.3, and the VBO ran 1.7.5.

[2] In Yolo County, each precinct has one polling station, and each polling station serves one precinct. We use the terms "polling station" and "precinct" interchangeably.

[3] A number of UC Davis staff members, and students from Sacramento City College, also joined.

1.1 Goals of an Election

For our purposes, an election has three goals:

1. *Accurate*: the results of the election should be correct, as defined by law.
2. *Secret*: one should not be able to associate a voter with a ballot, not even when the voter agrees that this information should be released.
3. *Available*: a registered voter should be able to vote when she is at the polling station.

From this, three classes of attacks emerge:

1. *Alter the outcome of an election.*
2. *Violate the confidentiality of a voter's ballot.* The voter may do this (to sell the vote), or a third party may do this (typically, to coerce the voter).
3. *Interfere with the voting.* Voting systems may be unusable, or so difficult to use that voters are likely to give up in frustration.

In what follows, a *race* is a contest in which one or more candidates are to be elected to a particular position, or a proposition or initiative is to be voted for or against. For example, a city council race may consist of 10 candidates running for 3 city council seats. A *ballot* is a collection of races upon which voters vote; we also use that term to refer to the paper (or its electronic analogue) on which voters express their choices.

1.2 The Ground Rules

Our task was to perform a vulnerability analysis on the systems that would be deployed to the polling stations. We wanted to discover any system issues that could potentially be exploited at any step in the election process and to propose procedural strategies to mitigate these threats. Most critical would be flaws that, if exploited, could alter the outcome of an election, but we wanted to note, and explore, lesser threats.

We had no access to either source code or detailed hardware manuals for the systems. Due to licensing requirements, we were unable to attempt any reverse engineering of the software. We also could not damage the equipment. So, our analysis was a "black box" analysis.

We did not examine the ballot generation system or scanning systems for vulnerabilities. Our study was limited only to those components at the polling stations. The other systems were in a secured area of County headquarters, and only clerks would be using them. Further, these mechanisms either had their output inspected beforehand (for example, ballots were checked before being printed and used) or were amenable to recounts (for example, the paper ballots being scanned could also be hand-counted). Hence the risk to these units was considered less serious than the risk to the field equipment.

2 Background

Electronic voting systems came into use in large part as a result of the confusion in obtaining the results from the Florida election in 2000. They promised to eliminate the ambiguity in determining whether a vote was cast for candidate A or candidate B. Supporters also pointed out that properly augmented electronic voting systems would enable handicapped people to vote without the need for a human assistant, eliminating that particular compromise of ballot secrecy.

Reviews of electronic voting systems have demonstrated that problems exist in all vendors' systems. For example, [11, 6, 15, 13, 10, 7, 8, 16] demonstrated problems with not only Diebold systems but many other vendors' systems. Other reports [14, 5, 2] focused on the requirements that election systems must meet, and problems with existing standards.

This report deals with the Hart InterCivic eSlate and JBC e-voting system. Bederson et al [3] and Herrnen et al [9] discuss the usability of various voting systems, including the Hart eSlate. Hart had @Stake[4], a security consulting firm, review security aspects of the eSlate and its development process; Hart made several changes as a result of their recommendations [1]. Similarly, a consultant's report for the California Secretary of State [12] found that system 6.1 could be used in elections.

3 How the DAU eSlate Works

Beginning in the November 2006 election, every polling station in Yolo County was equipped with one eSlate with a Disabled Access Unit (eSlate DAU). The DAU eSlate has a Verifiable Ballot Option

[4] Later merged with Symantec Consulting Services.

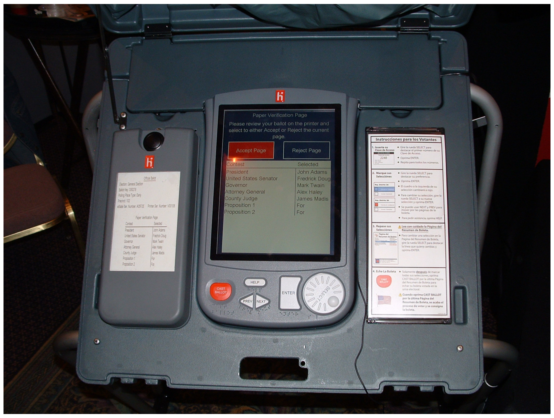

Figure 1: eSlate. (cc-by/3.0) 2005, Joseph Lorenzo Hall

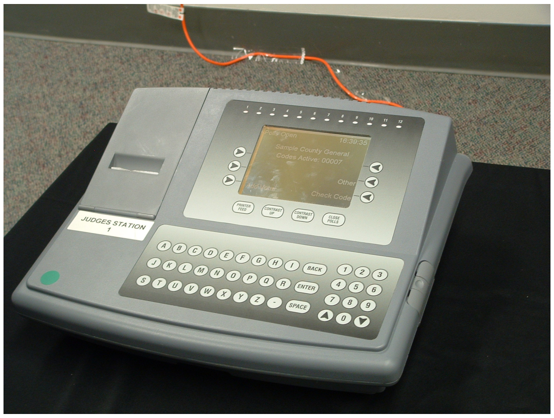

Figure 2: Judge's Booth Controller. (cc-by/3.0) 2005, Joseph Lorenzo Hall

(VBO), essentially a thermal printer sealed under plexiglass. A cable connects the DAU eSlate to the Judge's Booth Controller (JBC). This section first describes the physical machines, and then the procedure by which a voter votes on the system.

3.1 Physical description of the DAU eSlate and JBC

Figure 1 shows an eSlate system. The center component is the eSlate proper; it consists of a screen, and below it a wheel and 5 buttons. The voter highlights choices by turning the wheel until the proper area of the screen is marked. The wheel may be rotated to highlight individual contests or options. The SELECT button is used to select or de-select the voter's choices. The PREV and NEXT arrow buttons move the voter backward and forward through available pages, respectively. The HELP button provides on-screen assistance or summons a poll worker to help the voter. The CAST BALLOT button advances the voter to/through the vote review and acceptance steps and finalizes the voter's selection data to cast the voter's ballot.

To the left is the VBO. The printout is under plexiglass, and cannot be touched. To the right are directions for using the eSlate. Above the printer and eSlate is a compartment that runs the width of the voting booth. Note that the eSlate is *not* a touch screen voting system; the voter uses the wheel and buttons only.

Up to 12 eSlates can be daisy-chained together. In the top compartment is a cable that runs from the eSlate to the next eSlate in the daisy chain. Otherwise (or if this eSlate is the last one in the chain) the cable can be stored in the compartment.

Above the compartment, on the lid of the voting booth, is a Nylon fabric *privacy screen*. When set up for use, the privacy screen is unfolded to obstruct the view of the voter voting, giving the voter privacy.

Both the VBO and the eSlate can be removed from the voting booth. Removing the VBO requires releasing the large black retainer near the top of the VBO and may involve breaking/removing a wire seal, if such a seal is installed in the brass security retainer at the very top of the VBO case. Complete removal of the VBO also requires disconnecting power and data cables secured in the bottom of the VBO underside.

Removing the eSlate requires opening the storage compartment door and sliding the unit toward the top of the booth. This action unlocks the eSlate from the retaining pins in the booth compartment and disengages the electrical connection maintained between the eSlate and the VBO through slider switch contacts in the bottom of the booth and on the back of the eSlate. Complete removal of the eSlate can then be accomplished by disconnecting the power and data cable that provides connectivity with the JBC and lifting the eSlate out of its molded compartment.

The DAU is built into the eSlate. It consists of features designed to allow disabled voters to vote without help. The two main features are an audio mechanism that reads the ballots and repeats the voter's selections, for the visually impaired; and a set of "jelly switches" for the tactilely impaired. An audio recording of a human reading of the ballot is stored on the DAU audio card as part of the ballot creation process; the system does not use a speech synthesizer.

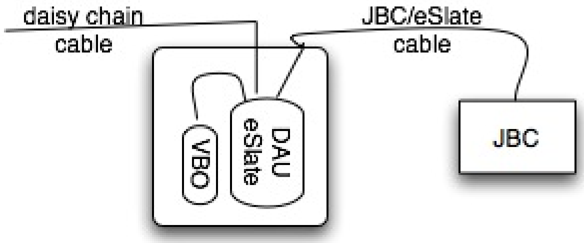

Figure 3: How the JBC, eSlate, and VBO are connected

The JBC shown in Figure 2 connects to the eSlate by a cable. The ten buttons around the screen are used to drive the JBC, and the row of lights above the screen indicate the status of each connected eSlate. For Yolo County, only the first light would be relevant because each JBC had only one eSlate connected. In the back of the JBC are a battery key that screws into place, a modem port, a printer port, and a connector for the JBC cable.

Each JBC has a card called a Mobile Ballot Box (MBB). When a voter casts her ballot, the eSlate transmits the voter's selection data (called a Cast Vote Record, or CVR) to the JBC, which stores it on the MBB. The MBB then contains an electronic record of votes cast on the eSlates associated with that JBC. The MBB also stores audit records.

The voting system uses triple redundancy to record votes electronically. Each CVR is recorded on the MBB, and in both the eSlate's internal memory and the JBC's internal memory. In addition, the VBO prints a record of the voter's selections, so if a recount is needed, the paper record may be used.

Figure 3 shows how the VBO, eSlate, and JBC are connected. Note the VBO and eSlate are in a single physical unit.

3.2 How a Voter Votes

When a voter enters the polling place, she registers as usual with a poll worker and signs her name into the poll book. If she wants to use the eSlate, a poll worker selects "Add Voter" from the JBC's main menu. The JBC produces a 4-digit access code, and the poll worker prints this access code for the voter on a small printout (looking like a traditional register receipt) with the date, time, location, precinct, and access code.

The voter then goes to the eSlate, and ducks under a privacy screen that shields her actions from others' views. The eSlate greets her with a welcome screen providing some basic instructions on how to operate the device. At this point, she has the option to navigate the eSlate using the wheel and buttons on the face of the device or to use an alternate input device. The eSlate is pre-equipped with two large buttons, called *jelly switches*, as an accessibility aid to those whose tactile skills do not lend easily to operating the eSlate with the embedded buttons. The jack into which these tactile inputs are plugged is a standard 3.5mm jack, allowing those who prefer to provide their own input device (such as a sip/puff device) to do so. Also available to the voter are a pair of standard headphones, or the option to plug in her own headphones, through which all operations on the eSlate will be narrated. This allows a voter with vision impairments to navigate the eSlate without assistance from a third party. The narration is given even if headphones are not used, but in that case the voter cannot hear the narration.

Once the voter has selected the input and feedback options best suited for her use of the eSlate, she is prompted to enter the access code she received from the poll worker. The eSlate verifies that the code is *authorized* by communicating with the attached JBC. After her access code has been verified, eSlate displays the first page of the ballot. The voter can navigate through the ballot at her own speed by manipulating the wheel and buttons, or an assistive device.

Once the voter has filled out the ballot to her satisfaction, she advances to the first ballot verification screen. If she makes a selection for every option on the ballot, she will be automatically advanced to this screen; she can, however, hit the "Cast Ballot" button to manually advance herself to cast a ballot with fewer selections.

The eSlate then displays the first ballot verification screen, called the *Ballot Summary Page*. A two-column table presents every ballot option and the voter's selection for that option, including a listing of "No Selection" where applicable, in the order in which the options appeared on the ballot. If the voter is using the headphones, the eSlate will read the ballot to the voter. She can choose to make changes to selected options, in which case the eSlate returns her to the ballot to change her selections. Or, she can choose to accept the ballot as is. In this case, she advances to a second verification screen. At this point, the contents of the ballot selections are printed on the

VBO printer, which is situated directly next to the eSlate screen. The voter is encouraged to verify her selections both on the screen and on the paper ballot. A visually impaired voter will be unable to verify the printout, but the eSlate will again read the ballot selections over the audio channel for her verification. If she wants to change something, she can reject the ballot at this point. In this case, the eSlate has the VBO print "BALLOT REJECTED" on the paper ballot, and a barcode indicating that the voter rejected the set of ballot selections immediately preceding. The eSlate then returns the voter to the original ballot to change her selections.

The voter may reject two printed ballots. After that, by law, the voter *must* accept the third printed ballot.

When the voter accepts the ballot, the VBO prints "BALLOT ACCEPTED" and a barcode directly below the human-readable printout of the voter's selections. This barcode contains a machine-readable encoding of the ballot selections. The VBO then immediately spools the printed ballot out of sight so that the next voter cannot see it.

Ballot acceptance also triggers a communication from the eSlate to the JBC to store the ballot contents. The vote is stored electronically on internal eSlate memory, internal JBC memory, and on a memory card known as the MBB (Mobile Ballot Box). The MBB is the primary record of the votes cast on an eSlate, and the data on the MBB is used to generate the results tabulated at the end of an election.

At this point, the eSlate shows a blue screen that thanks the voter for voting, and displays a waving American flag. The voter instructions state that a voter knows her vote has been cast when she sees this flag. If she has been using the auditory feedback, she will hear a similar message through the headphones and will know that her voting process is complete.

4 The Study and Its Results

We began by studying the devices as units and then, after removing the eSlates and VBOs, as components. This research phase suggested some possible avenues for attack: for example, understanding that the VBO is a thermal printer inspired us to test the resistance of the printed ballots to deliberate exposure to extreme heat — a test whose results were favorable to the eSlate design, as the VBO casing effectively prevented us from applying enough heat to maliciously alter the thermal printing.

Our direct testing involved arranging eSlates and JBCs in the typical Yolo county arrangement (a single eSlate connected to a JBC) and in configurations that might appear in other municipalities (multiple eSlates daisy-chained to a JBC). We brainstormed methods for entering malicious input, interrupting official communication channels such as between the eSlate and the JBC, ways to extract information from output, and means for generating malicious output.

Many of the team members also volunteered on the fall 2006 election day in Yolo County to serve as technical experts. This allowed us to provide a civic service, get access to more training about the eSlates from a Hart representative, and—most relevant to this exercise—observe the eSlates in use during an election. Our observations gave us a more solid background for assessing what types of attacks could reasonably be expected to go undetected and what types of actions would be likely to draw attention. These factors are inherently variable and depend largely on the confidence and expertise of the election officials present at a given precinct at the time of an attack. We observed that precinct volunteers were generally intimidated by the presence of the eSlates and would likely not notice subtle attack movements that took place within the space below the privacy screen.

We are not aware of any attacks that occurred during the election, nor were we authorized to attempt attacks to test the security procedures. The precinct workers' insecurity with the election technology suggests that attacks whose effects lead to error states would be attributed to technology instability rather than to malicious activity. This broadened the class of attacks we considered to be feasible without detection.

4.1 Results

The majority of our findings centered on the goal of altering the outcome of an election. Some of our attacks appeared to be trivial at first but later proved to be crucial steps to the completion of a larger attack scheme. We present these attacks first and then discuss attacks with broader significance or a greater scope of impact.

4.1.1 MBB and DAU Audio Cards

The MBB and DAU audio cards are standard, commercially available PCMCIA cards. This suggested that their contents could be copied or altered on a typical computer. To test this theory, we copied the contents of an MBB onto a computer, then used the MBB in a JBC while we cast several ballots on a connected eSlate. We removed the MBB (which caused the JBC to crash; it had to be rebooted with the card intact) and compared the new contents of the card to the file we previously copied. Noting that the contents had changed, we overwrote the new card contents with the previous card image and re-inserted it into the JBC. The JBC booted normally and did not appear to notice that the contents of the MBB had changed.

We have not yet had the opportunity to check if the tally system, which uses the Hart tallying software, is able to detect the tampering. If not, the MBB's records could be subject to falsification unless proper election protocols are observed to physically protect the MBBs.

☞ ***Policy recommendation*: Enforce strong physical security and chain-of-custody policies, as well as the audit measures built into standard election data processing procedures.** Yolo County secures the MBB cards with two layers of tamper-evident tape, the serial numbers of which are recorded by the precinct lead in the full polling station report. MBBs themselves are also strictly regulated in number and are tracked by unique serial number. Standard operating procedures for processing election data at Election Central call for the comparison of ballots read by Tally from an MBB with the JBC Public Count and Total Ballots Cast from the JBC close polls tape.

4.1.2 Battery Drain

The eSlates do not normally operate using battery power. Instead, they draw their power from the cable connecting them to the JBC. We tested the impact of shorting out the cable by examining the unused cable intended for systems being daisy-chained together. We found that connecting a DSub-15 null terminator (available at an electronics store for less than a dollar) to the daisy-chain cable effectively shorted the power and forced the eSlate to operate using battery power. If the battery pack on the eSlate does not provide power for the duration of the election (which depends on how long since the battery had been changed and how often the eSlate had since been forced to use the battery), an attacker could compel the eSlate to drain its own battery and then lose power entirely.

By placing the null terminator attached to the end of the cable tucked under the top panel[5], this attack could be carried out covertly, and resolving the problem could prove untenable for any but the most attentive election official. Its effect would be to disenfranchise those who were unable to cast paper ballots, forcing them to either enlist the assistance of another person or causing them to be unable to cast their ballot entirely.

☞ ***Policy recommendation*: Remove the daisy-chain cable from any eSlate that will not use this cable during an election.** Hart gave permission for Yolo County to remove the cable from the eSlates. We have verified that this does not affect the operation of the eSlates.

4.1.3 JBC Date/Time Attack

Another battery-based attack centers on Hart's election software using time for certain functions. Elections are defined to occur during specific time periods, and attempts to initialize elections with the *open polls* command before the predefined poll opening time will cause an error. Similarly, attempts to *close polls* before the predefined poll closing time will also cause an error. The JBC must maintain constant power from its CMOS battery to track time. Removing the CMOS battery for 30 seconds or so resets the JBC to a date in 1996, which is outside the range of time for any current election. Thus, temporarily removing the CMOS battery causes a JBC to require a time reset, which can only take place at election headquarters.

A JBC that loses track of time could be exchanged for one that maintains an accurate view of time, but identifying the problem would require an adept election official. Additionally, exchanging the JBC would require a significant amount of down time and might disenfranchise voters who would be unable to cast their ballots before the JBC was replaced.

☞ ***Policy recommendation*: Test and replace CMOS batteries regularly, and ensure that no untrusted person can disconnect the battery before the JBC has been delivered to the precinct.** This attack requires disassembling the JBC, so multiple observers mitigate this attack. Yolo County, for example, assigned volunteer observers to ride along with the technical expert volunteers who deliver and help assemble the eSlates. These observers are randomly assigned the morning of the

[5] Given the use of the privacy screen and the compartment at the top of the voting booth housing the unused cable, observing the null terminator would be highly unlikely, in our experience.

election, a measure that helps prevent advance collaboration or conspiring.

4.1.4 JBC Soft Buttons

It is possible to crash the JBC using the soft buttons surrounding the LCD screen on its face. At the *open polls* menu, three of the soft buttons do not correspond to any listed actions. Pressing them separately does nothing. Pressing and holding all three together causes the JBC to pass rapidly through various menu states, print pages of nonsensical characters, and within about 10 seconds enter an error state. The JBC's power must be manually reset to clear this error. While this does not seem to have a permanent effect on the JBC, the ability to reboot the JBC is useful in some of the more elaborate attacks.

☞ ***Policy recommendation*: Only trusted election officials should have access to the JBC.** In our experience, the JBCs are very stable and do not enter error states without being given suspect input. Any deviation from their ordinary operations should be viewed as highly indicative of malicious behavior.

4.1.5 Waving American Flag

All instructional materials available to voters, including the pictorial guides next to the eSlate devices at polling stations, specifically remind voters to watch for a waving American flag, which indicates that their vote has been recorded properly. The instructions do not indicate any particular written (displayed or printed) feedback that indicates the completion of the process. We asked if we could produce the image of the flag *before* the vote has actually been recorded.

After an eSlate has successfully authenticated a voter's access code with the JBC, communication between the two devices can be interrupted without any indication on the eSlate. When the voter completes the voting process and attempts to cast her ballot, she is presented with the image of a waving American flag, even if the connection between the eSlate and the JBC has not been restored. The displayed message accompanying the flag image states: "*Reconnect to voting system to record ballot.*"[6]

Since the waving American flag is present, the voter is likely to believe that this message is part of normal operation. Moreover, if the voter were asked if anything had gone wrong while she was voting, she would likely remember having seen the flag image and believe all went well.

☞ ***Policy recommendation*: Instruct voters to watch for the message, "Your vote has been recorded," rather than only the waving flag image.** The ballots are presented in written format, so expecting the voter to read the final screen rather than to trust pictorial feedback[7] is reasonable.

The ability to produce the flag image before a ballot has been successfully recorded is of little import, because the ballot results are immediately transmitted as soon as the connection is restored. Causing a voter to believe her vote has been recorded at a specific time and then not recording it until a later time is not an attack with the potential to alter the outcome of an election. However, it presents the opportunity to violate the voter's privacy, because the VBO retains the most recent ballot results on display until the vote is transmitted to the JBC. So the next voter entering the booth will see the previous voter's vote on the VBO. We also found other uses for this disruption of communication (see Section 4.1.7).

4.1.6 Rebooting the JBC

The JBC has two sources of power: AC power and an internal battery pack. The battery is only available as a power source when a key (provided with every JBC) is connected in the back. The key screws in, and precinct worker manuals instruct those assembling the eSlates to ensure that the key is connected before polls are opened. If this key is not connected—or if the battery pack is dead—the JBC can be rebooted from within the eSlate privacy screen.

The cable from the JBC uses a typical 15-pin VGA female connector to connect to the eSlate. Attaching a commercially available 15-pin VGA male connector shorts the power circuits. If the battery key is properly connected and the battery has power, shorting the power circuit forces the JBC to draw power from the battery. Otherwise, the JBC immediately reboots.

☞ ***Policy recommendation*: Test and replace JBC batteries regularly, and require that the battery key be connected before opening polls. Also, check relevant cable and battery key connections periodically throughout the day.** The workers can be given a short list of connections

[6] The eSlate is designed to operate this way to accomodate voters who cannot exit their vehicles and thus make use of Hart's *curbside voting* feature.

[7] The audio feedback verbally instructs the voter: "*Reconnect to voting system to record ballot.*" Since a voter using the audio narration will not be watching for a picture, she will be less easily fooled.

to check. The lists could use pictures to ensure that technologically-inexperienced poll workers knew what the connections should look like and so could visually detect deviations.

4.1.7 Causing Record Inconsistencies

When the eSlates are operating properly, CVRs are stored electronically on the MBB, on JBC internal memory, and on eSlate internal memory. The VBO also prints a copy of every accepted ballot followed by a message stating "Ballot Accepted" and giving a machine-encoded version of the ballot contents in a 2-dimensional barcode. In Yolo County, the MBB is the primary record of votes cast on an eSlate. That record is consulted first and, unless there are discrepancies or a mandated recount, is the *only* record ever consulted.

We found several variations on one attack. Each intends to cause the various records to become inconsistent with one another. The effect of having inconsistent records is determined by local law and election policies and procedures. For example, if a county does not verify that the number of ballots recorded on an MBB matches the number expected, then the records on the MBB will not be compared to the records on the eSlate internal memory or printed paper trail. If a county does discover such discrepancies, the law dictates which record or combination of records is considered the official result. Creating a significant number of inconsistencies could accomplish attack goals such as undermining public trust in the legitimacy of an election.

The following are outlines of the variations. The headers indicate which records correctly reflect the ballot the voter would have cast had she not been interrupted by any malicious activity, including (but not limited to) her own. We call this ballot the *voter intent*. The first section, for example, will discuss an attack that causes the JBC and MBB to incorrectly reflect *voter intent*, while the eSlate internal memory and the VBO printed record will be correct; thus, the section is labeled *Correct: eSlate, VBO. Incorrect: JBC, MBB.* Some attacks will cause ambiguous records, so the three categories for any record are *Correct*, *Incorrect*, and *Ambiguous*.

Because the countermeasures for these attack variants are similar, we save discussion of procedural suggestions for the end.

Correct: eSlate, VBO. Incorrect: JBC, MBB For this attack, the voter enters her access code into the eSlate and begins to vote. At any point after the eSlate has verified the access code with the JBC, but before the ballot has been completed and transmitted to the JBC, the communication between the eSlate and JBC is cut (perhaps by the cable being loose, or by some nefarious means).

When the voter completes her ballot, the eSlate advances to the waving American flag and display a message indicating that the ballot will be completed when communication is restored. If the power to the VBO is cycled (for example, by turning off and then on the power bar to which the plug is connected), the VBO reboots and prints the "Ballot Accepted" message and barcode. At this point, the ballot has been recorded on the eSlate internal memory and the VBO printed record, but has not yet been transmitted to the JBC. If either the eSlate or the JBC is rebooted before the connection between the eSlate and the JBC is restored, the ballot will never be transmitted to the JBC. The JBC will record the access code for this voter as "aborted"—the technological equivalent of a spoiled ballot.

Rebooting the JBC requires executing one of the attacks listed above (see Sections 4.1.4 and 4.1.6). If the battery key was improperly connected, or not connected at all, a malicious voter could execute the JBC reboot. Based on our observations, in Yolo County a voter would be unlikely to notice such a reboot. But rebooting a JBC would likely be visible to other poll workers, even though it would probably be reported as a problem with the technology.

Rebooting the eSlate requires removing the unit from its casing and cutting the connection to battery power. The limited space below the privacy screen, and the bulkiness of the eSlate, makes this very difficult to do without being noticed. Based on our observations, in Yolo County it is unlikely that a voter could remove the eSlate from its casing without drawing attention.

Correct: eSlate. Ambiguous: VBO. Incorrect: JBC, MBB This attack differs from the last only in that the power to the VBO is never cycled. As a result, when the systems are rebooted, the ballot will have been properly recorded on the eSlate internal memory but never transmitted to the JBC or stored on the MBB. The VBO will have printed the ballot contents , but neither a "Ballot Accepted" message and barcode nor a "Ballot Rejected" message and barcode. So, if election officials use a barcode scanner to read the paper trail, this ballot will be missed. If the paper trail is read by a human, the ballot will appear inconsistent, and the *voter's intent* will be ambiguous at best. Double-checking with JBC printed records will reflect the associated access code as *aborted*, so whether this ballot would be counted depends on local policies.

Correct: eSlate. Incorrect: VBO, JBC, MBB This attack builds upon the previous attack in which the VBO record was left ambiguous by the previous voter. It requires the use of two access codes, one immediately following the other. The first ballot is "cast" according the attack described above. The second access code is entered, and the voter proceeds to select her options. She advances to the Ballot Summary Page. Her selections are presented on the eSlate screen but the VBO has not yet printed them.

At this point, communication between the eSlate and the VBO is cut, and the voter presses the red *Cast Ballot* button on the eSlate face. When communication is restored, the VBO will first print a "Ballot Rejected" message and barcode and *then* print the ballot options most recently selected. Because the previous ballot had neither an "Accepted" nor a "Rejected" message associated with it, the "Ballot Rejected" message generated by this attack will be associated with the previous ballot. So the paper trail for the "ambiguous" ballot will show as "Rejected" (*Incorrect*). The voter can then proceed to cast her own ballot (i.e., the second ballot) as usual.

Countermeasures for Inconsistent Records Countermeasures that secure power sources for the JBC, eSlate, and VBO hinder these attacks. If voters wait for the *written* message indicating that their vote has been recorded, these attacks are unlikely to work either. These measures do not prevent all variants of these attacks—in particular the ones where a voter disconnects the battery power from the eSlate—but they do force an attacker to take actions that are easier to see. Conversely, the vendor could implement a technical countermeasure by employing a more robust distributed protocol for communication among the various components.

4.1.8 Printing Extra Barcodes

Disrupting communication between the eSlate and the VBO could cause the VBO to print unauthorized data. Specifically, communication is disrupted (for example, by the eSlate being rocked slightly in its casing) immediately after the VBO has printed a "Ballot Accepted" message and accompanying barcode, but before the VBO has begun to scroll this page out of sight, the VBO will print a second "Ballot Accepted" message and barcode. Disrupting the communication again repeats the printing. The result is a paper trail with a ballot followed by several "Ballot Accepted" messages and barcodes.

If election officials read the human-readable ballots from the VBO records, this string of barcodes will be baffling (and, perhaps, suggest either machine failure or malicious activity) but will not likely affect the tally. However, in counties which use barcode-scanners to read the VBO records, these repeated barcodes (if undetected) effectively allow a voter to cast an indeterminate number of identical ballots—the electronic equivalent of ballot box stuffing.

☞ ***Policy recommendation*: Visually inspect the paper trail before using a barcode scanner to count the votes recorded on that paper trail, or have election officials count those votes by inspecting the printout of the ballot contents.**

4.1.9 Predicting Access Codes

According to the vendor, the JBC produces access codes randomly—in practice, this means pseudorandomly. A cryptographically strong pseudorandom number generator produces a sequence of numbers such that, given a sequence of past numbers, the next number cannot be predicted ([4], p. 169). The sequence produced by the JBC *is* predictable. After observing a small subsequence (200 sequential numbers) we were able to design an algorithm which when input an access code will generate, in order, the codes that follow and preceed it. The period of the sequence is 10,000 access codes, and the sequence is the same for all JBCs.

Knowing this access code sequence enables one to predict the *next* access code after any given access code. In a busy polling station with many eSlates, that voter could approach the eSlate, observe that others waiting in line already had their access codes, and choose to cast ballots using the access codes issued after hers and before those legitimate voters have a chance to use them. By casting their ballots first and then her own, a voter could cast several ballots and exit the polling station before anybody has an opportunity to observe that anything was askew. Again, the problems would be most likely ascribed to technological instability, or result in provisional voting.

☞ ***Policy recommendation*: Polling stations should only have one eSlate connected to any particular JBC, and only one access code should be assigned at a time.** Before a voter is issued an access code, the eSlate should be available for her to use. If another voter is currently using that eSlate, the poll worker should wait until the eSlate is open to issue the next access code. This will prevent voters from using more than one access code, as codes only become authorized when they are issued by the JBC.[8]

4.1.10 Automated Input Through the Tactile Input Jack

The tactile input jack (for plugging in devices such as jelly switches) is a standard 3.5mm jack. The functionality of such devices can be mimicked through the generation of specific audio signals. For the jelly switches, the signalling protocol is simply a high signal on the left channel for a click of the red button, and a high signal on the right channel for a click of the green button. Connecting the port to a signal generator generating a 1 Hz monophonic square wave is sufficient to emulate the jelly switches.

We created several Python scripts that issue signals over a typical 3.5mm audio cable to navigate the eSlate menus. One script takes as input the access code and a predefined set of ballot options, and automatically generates the specific signal patterns to enter the access code, select the ballot options, and cast the ballot. Given the timing in generating displays, it is possible to cast an entire ballot including the entry of the access code in about 20 seconds. Entering a write-in candidate significantly increases this time requirement because the alpha-numeric keyboard can only be traversed in one direction, so an entry could require several iterations of the keyboard. We have successfully run this automated entry script on a laptop and believe it could easily be done on smaller devices, such as pocket PCs with audio capabilities.

A voter who casts her ballot using automated input is simply entering the same data through different means. However, if proper protocols for the access codes are not enforced, many ballots could be cast quickly, without detection, whereas manually entering the same information using the the slow, moderately clumsy buttons on the face of the eSlate would lead to detection. Thus, the pertinent countermeasure effective at mitigating the threat of automated entry is the same as the protocol for prohibiting the exploitation of the predictability of access codes.

4.1.11 Recording Audio Vote Records

As a voter navigates a DAU eSlate, the audio card continuously generates an audio narration of her activities, regardless of whether she is using the headphones. This narration could be intercepted and recorded. Because the audio record also includes a narration of the access code entry, this would directly link a ballot to the only receipt a voter is given to prove that she has voted—nullifying the confidentiality intended by the “random” access code.

Connecting an audio splitter (available for less than a dollar at many electronic stores) to the audio jack would ensure that the headphones still work as expected, and send the audio output to a recording device tucked under the top panel of the eSlate casing. This would record all subsequent voting activity on the eSlate and link audio narrations of ballots to particular access codes.

Given access to voters’ access codes (for example, by a business requiring its employees to submit their access codes to receive pay for the time spent voting), an attacker could match those codes to audio records from eSlate narrations and thus determine how individuals voted. Alternately, an attacker could visually observe who used the eSlate. Because the narration would provide a record of ballots *in order*, the attacker could easily pair observed voters to their ballots.

☞ ***Policy recommendation*: Train poll workers on what comprises suspicious activity at an eSlate.** A voter trying to manipulate the eSlate in its casing should cause a poll worker to check for suspicious behavior. Also, the check for correct cable connections (see Section 4.1.6) should include verifying that the audio jack was connected only to headphones and no other devices.

5 Conclusion

Our task was to discover any system issues that could potentially be exploited, and to propose mitigations. We found that Yolo County had anticipated our suggestions. Of the 11 attacks we discovered, only the battery drain attack would work. When we identified the attack involving the unused cable, the Clerk-

[8] Ideally, a cryptographically strong pseudorandom number generator with a randomly chosen seed would generate access codes, but this is a function of the eSlate, and not under Yolo County’s control.

Recorder immediately obtained permission from the vendor to remove it, eliminating the attack. However, were the procedures in Yolo County not observed, *any* of the attacks could be successful.

Our solutions may not be appropriate in other counties. Some counties simply must daisy-chain their eSlates. For such counties, the remediation proposed for the access code guessing attack will not work. The best remediation (for everyone) is to fix the access code generator mechanism to generate a cryptographically strong pseudorandom number sequence.

Many avenues remain unexplored. We did not try to analyze the MBB card to see if it contained code, or only ballot and vote information, and how its contents are protected. Similarly, we did not analyze the signals going between the eSlate and the JBC to determine if attacks based on intercepting and manipulating that data would be successful. Also, we did not determine if a voter's selections could be obtained by measuring and analyzing changes in the electromagnetic field of the eSlate and the JBC (i.e. via a Tempest attack).

Our results allow us to make some general observations about using electronic voting systems in polling stations, and of the importance of policies and procedures in running elections.

It is often implied that electronic voting systems cannot be made completely secure and that therefore they should not be used. In our view, this implication is dangerous because *nothing* can be made completely secure. Frauds, rigged elections, and general electoral chicanery have existed as long as people have voted—long before the first electronic device was even conceived of. Requiring perfection of one voting mechanism implies either that perfect mechanisms exist or that as voting is imperfect, it should be abolished. We disagree with both statements.

A better question is whether introducing electronic voting systems also introduces new vulnerabilities in the voting process. If not, then the question of whether to use electronic voting systems depends on factors unrelated to security. But if so, then new policies and procedures must be created to mitigate those new vulnerabilities, and those must be weighed against vulnerabilities in the existing system.

In many cases, as in Yolo County, the deciding factor is the law. Given certification requirements and laws requiring county officials to provide disabled people with mechanisms for voting that did not require assistance, the use of an electronic voting system is unavoidable.

One must analyze the security of an electronic voting system (and indeed of any part of a voting system) in light of the policies and procedures in place when the system is to be used. This highlights the importance of analyses such as the one we conducted. This type of testing reveals problems that at first blush appear insignificant, but can affect the accuracy of election results; similarly, attacks that seem devastating may be mitigated completely by policies and procedures, *assuming they are followed*. The procedures that limit the damage from the attack, or block the attack entirely, are for the most part merely good practice: control the chain of custody of critical elements, have multiple observers of election procedures and events, and train poll workers and election officials to note unusual occurrences. The best security is an alert electorate, and alert election officials.

This type of analysis also disproves the claim that, without disclosed source code, electronic voting systems are safe. In fact, their safety depends on informed procedures being devised *and followed*. The human element is critical here. People, even election officials, make mistakes. People can be compromised, often unknowingly. Procedures—for elections involving electronic voting systems, and not involving electronic voting systems—must take human imperfections into account.

Acknowledgements This work was supported in part by a Sandia National Laboratories/University of California at Davis Excellence in Engineering Fellowship, as well as by Department of Education GAANN. Kind thanks to Sandia and the DOE for their support.

Thanks also to Jason Pope, Michael Cheng, and Asa "Joshua" Coats for helpful ideas and contributions, to Dan Wallach and Mark Gondree for insightful comments, and to Joseph Lorenzo Hall for permission to use the photographs in Figures 1 and 2.

References

[1] Brad Arkin. Securing the eSlate electronic voting system: Application security implementation. White paper, Symantec, 20330 Stevens Creek Blvd., Jan 2005.

[2] Earl Barr, Matt Bishop, and Mark Gondree. Fixing federal e-voting standards. *Communications of the ACM*, 50(3):19–24, Mar 2007.

[3] B.B. Bederson, B. Lee, R.M. Sherman, P.S. Herrnson, and R.G. Niemi. Electronic voting system usability issues. *ACM Conference on Human Factors in Computing Systems, CHI Letters*, 5:145–52, 2003.

[4] Henry Beker and Fred Piper. *Cipher Systems: the Protection of Communications*. Northwood Books, London, 1982.

[5] Brennan Center Task Force on Voting System Security. The machinery of democracy: Protecting elections in an electronic world. Technical report, Brennan Center, 161 Avenue of the Americas, 12th Floor, New York, NY 10013, August 2006.

[6] Compuware Corporation. Direct recording electronic (DRE) technical security assessment report, November 2003.

[7] Ariel Feldman, J. Alex Halderman, and Edward Felten. Security analysis of the Diebold AccuVote-TS voting machine. Technical report, Princeton University, September 2006.

[8] Rop Gonggrijp, Willem-Jan Hengeveld, Andreas Bogk, Dirk Engling, Hannes Mehnert, Frank Rieger, Pascal Scheffers, and Barry Wels. Nedap/Groenendaal ES3B voting computer: A security analysis. Technical report, Stichting "Wij vertrouwen stemcomputers niet", 2006.

[9] P.S. Herrnson, R.G. Niemi, M.J. Hanmer, B.B. Bederson, F.G. Conrad, and M. Traugott. The importance of usability testing of voting systems. In *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop*, Aug 2006.

[10] Harri Hursti. Diebold TSx evaluation and security alert, May 2006.

[11] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach. Analysis of an electronic voting system. In *Proceedings of the 2004 IEEE Symposium on Security and Privacy*, pages 27–40, May 2004.

[12] Paul Kraft. California secretary of state consultant's report on Hart Intercivic System 6.1. Technical report, 2006.

[13] RABA Innovative Solution Cell. Trusted agent report: Diebold AccuVote-TS voting system, January 2004.

[14] Roy G. Saltman. Accuracy, integrity, and security in computerized vote-tallying. NBS Special Publication 500-158, Institute for Computer Sciences and Technology, National Bureau of Standards (now NIST), Gaithersburg, MD, August 1988.

[15] Science Applications International Corporation. Risk assessment report: Diebold AccuVote-TS voting system and processes, September 2003.

[16] Alec Yasinsac, David Wagner, Matt Bishop, Ted Baker, Breno de Medeiros, Gary Tyson, Michael Shamos, and Michael Burmester. Software review and security analysis of the ES&S iVotronic 8.0.1.2 voting machine firmware. Technical report, Security and Assurance in Information Technology Laboratory, Florida State University, Tallahassee, FL, Feb 2007.