Executive Summary

The California Secretary of State entered into a contract with the University of California to test the security of three electronic voting systems as part of her Top to Bottom Review. Each Red Team was to try to compromise the accuracy, security, and integrity of the voting systems without making assumptions about compensating controls or procedural mitigation measures that the vendor, the Secretary of State, or individual counties may have adopted. The Red Teams demonstrated that, under these conditions, the technology and security of all three systems could be compromised.

This report presents the findings of the Red Team testing on the Hart InterCivic voting system (System 6.2.1), as performed by the following team members: Robert P. Abbott (team leader), Mark Davis, Joseph Edmonds, Luke Florer, Elliot Proebstel, Brian Porter, Sujeet Shenoi, and Jacob Stauffer.

The Red Team tested the physical and technological security of the hardware and software included in the Hart voting system in order to identify vulnerabilities that could be exploited to violate the accuracy, secrecy, or availability of the systems and their auditing mechanisms. Red Team testing began on June 22 and concluded on July 19, during which time the team was testing both the Hart InterCivic voting system and the Diebold Election Systems Incorporated voting system[1]. This limited time frame did not allow the team to fully test the systems. Thus, results from this study should not be viewed as a complete report on all of the vulnerabilities that may exist in this system.

As tested, the Red Team found vulnerabilities in the Hart InterCivic System 6.2.1, which – in the absence of procedural mitigation strategies – could be exploited to compromise the accuracy, secrecy, and availability of the voting systems and their auditing mechanisms.

I. Introduction

The Red Team undertook the task of attempting to violate the physical and technological security measures of the Hart InterCivic voting system (System 6.2.1) in order to discover exploits that would violate the accuracy, secrecy, or availability of voting systems and their respective auditing mechanisms. This analysis was performed by the following team members: Robert P. Abbott (team leader), Mark Davis, Joseph Edmonds, Luke Florer, Elliot Proebstel, Brian Porter, Sujeet Shenoi, and Jacob Stauffer.

In developing our attacks, we made no assumptions about constraints on the attackers. "Security through obscurity" – or the practice of assuming a veneer of security by relying on attackers not having access to protocol specifications or of using tools that are perceived to be difficult to acquire – is not an acceptable option for any system that can't afford to have its security compromised Our study examined what a dedicated attacker could accomplish with all possible kinds of access.

[1]The findings from the Diebold system are presented in a separate report.

We present our findings here. In Section 2, we present an overview of the Hart voting system and how the system components interact. Section 3 offers visual representations of the classes of attacks we achieved or consider highly feasible and the roles that of those with sufficient access to execute such attacks. Sections 3 and 4 offer a more detailed overview of the vulnerabilities we exploited and what we believe, based on our research, are some viable attack scenarios, although not all of these scenarios were tested. Finally, Section 5 presents some concluding remarks.

We also note here that there are a great number of details that are not present in this public report. In particular, we have taken great care to ensure that we are offering the maximum amount of detail without violating our non-disclosure agreements with the vendors and without providing a "road map" to would-be attackers. Though state and county procedures may mitigate the impact of potential attacks, we believe it is in the public's best interest that this report not provide too much detail. To this end, we note that there are occasional references throughout this report to our verification of findings from previous studies. In order to perform due diligence, we attempted to verify previous security-related findings, where applicable, on all of the devices we were testing. Because citing those reports specifically in this report would provide the road maps we are seeking to avoid disclosing, all reference citations have been redacted to the confidential report[2].

[2] A single exception was made in the case of a previously-reported flaw that we found to have been addressed by Hart in System 6.2.1.

II. Device Descriptions

The following is a full list of Hart System 6.2.1 devices evaluated during the Top to Bottom Review. This section will give a brief description of each device in the Hart InterCivic e-voting system outlining their functionality. Also included in this section is a full connectivity diagram, outlining all physical connections between devices, and full pictures of each device.

Components

1. **BallotNow** – BallotNow derives information for printing paper ballots for an election from an MBB (see below) that was created with the Hart Voting System's Ballot Origination Software System (BOSS) application. These ballots can either be scanned at the voting locations with an eScan unit or shipped back to a central location to be scanned by BallotNow using a central count optical scanner.

2. **BOSS** – Ballot Origination Software System software application (BOSS) is used to create a BOSS Election database for an election that uses the Hart InterCivic, Election Solutions Group's eSlate System voting units, eScan System paper ballot scanners, and/or Ballot Now absentee paper ballots. BOSS also creates MBBs and defines ballot templates. BOSS is used for programming all software and hardware components of the system.

3. **eCM Manager** – Hart InterCivic's eCM Manager is a software application that reads and writes a Key ID, Key GUID, and a signing key to an eCM (eSlate Cryptographic Module). A PIN (password) is required to write the eCM. The eCM is a physical USB[3] security key provided by Hart InterCivic that is required for access to secure functions in the BOSS, Tally, Rally, Ballot Now, and SERVO applications. In order for an election to process from start to finish, the eCM cryptographic key must be provided to all applications, which will not run unless the USB security keys are inserted.

4. **eScan** – A precinct based optical ballot scanner. The eScan scans and tabulates ballots, storing results to an MBB.

5. **eSlate** – A DRE voting unit connected to a JBC. This is the end terminal that voters use to cast their ballots electronically. The eSlate is a dumb terminal that serves as a slave to the JBC.

6. **JBC** – The Judge's Booth Controller (JBC) is the console for controlling up to 12 eSlate/DAU voting devices. This device generates voter access codes, distributes appropriate ballot configurations to eSlates, records Cast Vote Records (CVRs), stores all the ballots cast on the eSlates to internal memory and to an MBB, and accumulates and reports vote results at the end of Election Day.

7. **MBB** – The Mobile Ballot Box (MBB) is a PCMCIA storage card used to store information about the election, including ballot definitions and cast ballots. MBBs are the means by which election definitions are transferred from the election management system to the JBCs

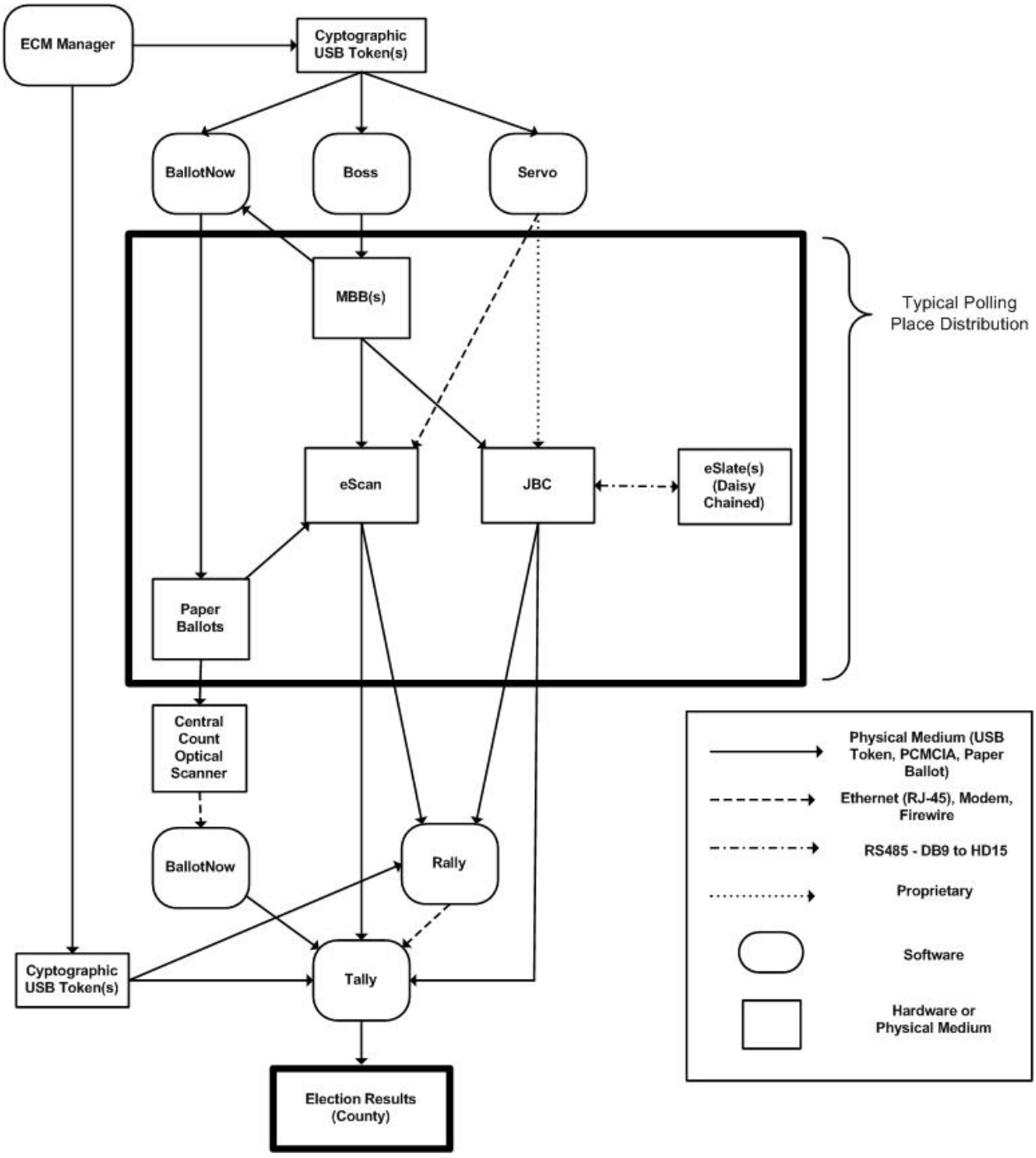
[3] Universal Serial Bus

and eSlates. MBBs are needed for many components of the Hart Intercivic system to run an election, including, JBC/eSlate, eScan, and BallotNow.

8. **Rally** – Used in the voting locations to total the ballots from the MBB and communicates remotely to Tally. NOTE: It was originally stated to the Red team that Rally was not used in the state of California due to regulations concerning the transmission of official ballots results over unsecured mediums (phone lines, internet, etc). The team was later informed that Rally may be used at remote collection sites, but security considerations of Rally in this report were minimal. Other entities using data from this report may want to examine the Rally system in more detail.

9. **SERVO** – System for Election Records and Verification of Operations (SERVO) is an election-records and recount-management system for the JBC, eSlate, or eScan voting devices from the Hart Voting System. SERVO is used to perform backups of JBC, eSlate, and eScan memory (including both Cast Vote Records and audit logs) as well as to reset the memory contents of these devices. It is also used to track Hart-branded assets.

10. **Tally** – The Tally application directly reads Mobile Ballot Boxes (MBBs) that were produced by BOSS and populated with voting data from Hart Voting System equipment and indirectly reads MBB data transmitted by the Rally application installed at remote locations for tabulation. Tally tabulates and reports the entire election results.



Interactions between Components

This section will describe the Red Team's perception of how all of the Hart components interact during a typical election. There may be some discrepancies depending on individual polling jurisdictions' policies and/or procedures. An effort has been made to not include any considerations of polices or procedures in this section.

First, the eCM manager is employed to create a cryptographic key, which will be used by various Hart InterCivic components throughout the course of an election. The keys are loaded onto Spyrus USB cryptographic tokens ("cryptographic modules"), any number of which may be created by anybody with access to the eCM manager and the PIN (which is really a password/pass phrase).

The cryptographic key is used by the BOSS application to create an election database. This database contains all of the details needed to run an election, including precinct and race definitions, ballot definitions, and numerous other options. The BOSS application "burns" MBBs (i.e. writes to PCMCIA cards) to be used in the election. The number of MBBs burned is dependent on the size of the county and the number of Hart JBCs and eScans it uses. An audio card (also a PCMCIA card) containing audio information for the eSlate voting units can also be burned at this time. At least one of the MBBs will be dedicated to BallotNow in order to print paper ballots. An MBB used by BallotNow may not be reused in any other Hart component during the election; attempts to reuse the MBB without formatting and re-burning it will be met with error messages that the card has already been opened and may not be re-used. The number of MBBs burned is tracked by BOSS, and the burning of MBBs must be completed before the election is considered "finalized" (a setting within BOSS). No results from the election may be tallied until the election is "finalized," but no further MBBs can be burned (nor election configurations altered) after the election is "finalized".

SERVO is used in conjunction with the cryptographic key module to reset and encode the cryptographic key into the eScan and JBC/eSlate units. MBBs encoded to the election will be inserted into the eScan and JBC units, making eScans, JBCs, and eSlates ready for a polling location.

At the end of the election, the entire unit, each MBB from each JBC and eScan can be physically transported to central headquarters for tallying. Alternately, regional processing centers may use computers running Rally (with a cryptographic module) to accumulate results from MBBs and then transmit electronic votes to the Tally server at election headquarters via modem connection. Paper ballots may also be transported to a central facility where they are read by a central count optical scanner, which does image processing via BallotNow. The votes are tabulated by Tally, which will use the original cryptographic key value to ensure that votes are not tampered with. Finally, Tally produces various election result databases and reports.

For auditing and reconciliation purposes, SERVO is also used after the election to backup the CVRs and audit logs from JBC, eSlate, and eScan units. After these records are backed up, SERVO is also used to reset all units, which clears their memory contents.

eSlate


Certification Testing
CAST BALLOT
HELP
PREV
NEXT
ENTER
SELECT

Judge's Booth Controller (JBC)

eScan

Mobile Ballot Box and Spyrus eCM Module

III. Relevant Findings

In this section, we present a high-level description of the vulnerabilities we found in the Hart System 6.2.1 voting systems. Our study was constrained by the short time allowed. ***The vulnerabilities identified in this report should be regarded as a minimal set of vulnerabilities***. We have pursued the attack vectors that seemed most likely to be successful. Other attack vectors not described here may also be successful and worth pursuing. This work should be seen as a first step in the ongoing examination of the systems. All members of the team strongly believe that more remains to be done in this field—and, more specifically, on these systems.

The systems and software versions we tested were:

Hart Intercivic System 6.2.1

1. Ballot Now software, version 3.3.11
2. BOSS software, version 4.3.13
3. Rally software, version 2.3.7
4. Tally software, version 4.3.10
5. SERVO, version 4.2.10
6. JBC, version 4.3.1
7. eSlate/DAU, version 4.2.13
8. eScan, version 1.3.14
9. VBO, version 1.8.3
10. eCM Manager, version 1.1.7

1. Hart Election Management System Servers

Hart InterCivic provided two laptops running Election Management System (EMS), specifically the applications numbered 1-5 above. The laptops were running Windows 2000, but Hart emphasized that they would install their EMS applications on any (presumably Windows-based) computers provided or purchased by their customers. Although Hart would provide security recommendations for those systems, Hart does not configure the operating system or provide a default configuration. Thus, the Red Team did not pursue any Windows vulnerabilities or investigate any potential vulnerabilities introduced by configuration of the system. This is not to say that the Windows system on which Hart software is installed is always secure; rather, the team was unable to test a representative Windows operating system configuration because it was not provided.

The fact that Hart does not specify how the underlying operating system should be configured means that county configurations are unpredictable and are likely to vary. ***The team does not assume that customers will harden their systems appropriately, nor that Hart EMS servers will be free of vulnerabilities – even well-known or easily exploited vulnerabilities***. The Red Team is only able to confirm that the particular Windows configuration delivered for testing was not examined for vulnerabilities simply because the team did not consider it a wise use of their very limited time to examine an operating system configuration they'd been explicitly told was not representative.

The Hart EMS software does configure a few aspects of the Windows operating system configuration, namely ODBC handling and the desktop environment. The Red Team was able to locate an undisclosed user name and password for the Hart ODBC databases. This is an attack vector that could provide unauthorized access to Hart EMS databases if an attacker were to penetrate the system on which the Hart software was running. The Red Team was also able to manually bypass the Hart software security settings that automatically define a Hart-defined environment. This allowed the team to run the Hart software in a standard Windows desktop environment. The Red Team did not have time to craft an exploit that would leverage this unauthorized runtime environment, but it may prove to be a vector for future attacks.

The Red Team, working in close conjunction with the 2007 TTBR Hart Source Code Team, discovered that the Hart EMS software implicitly trusts all communication coming from devices appearing to be Hart-branded and neither authenticates the devices nor performs adequate input validation on data transmitted to it by the devices. This allows for the possibility that a compromised device, such as an eScan that had been tampered with at a polling station, could infect the EMS systems. In particular, the Source Code Team discovered a weakness in the code that would allow an eScan to perform a buffer overflow attack and execute arbitrary code on the computer running SERVO.

2. eScan

The Red Team located a vector for overwriting the eScan executable. Although the team did not have enough time to craft an exploit for altering vote totals, given more time, the team is confident that eScan vote tallying could be modified maliciously.

The team was also able to access device-level menus that should be locked with passwords but were not. This access could allow an attacker a vector for altering configuration settings and/or executing a denial of service on the eScan.

Some of the findings from previous studies on precinct count optical scanners were replicated on the eScan, and they allowed the Red Team to maliciously alter vote totals with the potential to affect the outcome of an election. These attacks were low-tech and required tools that could be found in a typical office.

The Red Team implemented an attack devised by the 2007 TTBR Hart Source Code Team that was able to extract election-sensitive information from the eScan and issue administrative commands to the eScan. The leaked information would allow an attacker the ability to execute further attacks, while administrative commands issued to the eScan could erase electronic vote totals and audit records from an eScan while putting it out of service for the remainder of the Election Day. For more details on these attacks, please see the 2007 TTBR Hart Source Code Team report.

3. JBC

The Red Team verified previous findings on the JBC regarding access code generation and also discovered that a surreptitious device could issue commands that caused the JBC to authorize access codes. If the JBC is in early voting mode, it will not print receipts for the

access codes issued. If the JBC is in regular election mode, it prints a receipt each time an access code is issued. When in early voting mode, an attacker could attach the surreptitious device to the JBC. (Note: the surreptitious device is easily concealable in one hand.) After waiting for about a minute, while all possible access codes are issued, the attacker could then proceed to cast multiple ballots using any access codes.

Additionally, the team expanded on previous findings that the MBB in the JBC is vulnerable to tampering during an election. Extracting the MBB from within the JBC during an election and tampering with it without detection would probably require poll worker access, but the team was able to prove that this access would be sufficient to alter vote totals – and in such a manner that it would not be detected in the course of normal operation, though a very thorough audit might reveal it. Furthermore, the team found that post-election MBB tampering safeguards (by which we mean only the technological safeguards, not procedural safeguards such as the use of tamper-evident seals) are insufficient to guarantee that such tampering would be detected. Thus, the team is confident that post-election MBB tampering would succeed in many, if not all, instances.

Finally, the Red Team collaborated with the 2007 TTBR Hart Source Code Team to decode the protocol used for communication between the JBC and eSlates. This protocol does not authenticate the devices on the bus (the communication line), so all communication is considered trusted. The teams were able to intercept the communication, but they were unable to get an exploit working to interrupt or manipulate the communication; this, again, was due to time constraints. Full details of this work can be found in the 2007 TTBR Hart Source Code Team report. The teams are confident that, given more time, they could craft a device that could maliciously alter vote totals and violate voter privacy.

4. eSlate

The eSlate provides a continual audio narration of all on-screen events, including the entering of the access code and voter selections, and this audio is directed into attached headphones. The Red Team found that it was possible to remotely capture this narration – which includes an audio replication of each vote cast– without any physical access to the eSlate. This could be done covertly and would violate a voter's fundamental right to privacy . Polling stations that utilize a single eSlate (as opposed to multiple eSlates) might be more vulnerable to attacks of this nature than polling stations that utilize multiple eSlates, as the team suspects that the narration from multiple eSlates running simultaneously would be nearly impossible to separate. The team did not have an opportunity to test this suspicion, but we can confirm that the remote capture of narration is possible when a single eSlate is configured with an audio card.

The Red Team was able to reproduce previously reported attacks on the eSlate that enable a voter to generate multiple "BALLOT ACCEPTED" barcodes on the VVPAT-printed records. If a county is using barcode scanners to read VVPAT records, this might result in a single ballot being counted multiple times. If the county does not use barcode scanners, the presence of multiple barcodes in a row on the VVPAT records might trigger suspicion that the device had malfunctioned. The effects of this would depend on county procedures.

The team was able to validate Hart's claim that no information with the potential to violate a voter's privacy is leaked in the 2D barcode printed by the VVPAT below every cast ballot. The barcodes are machine-encoded versions of what is printed in human-readable format above, and none of this information includes voter-identifiable information when the devices are configured properly. For example, in California, the "ballot key" option is turned off, preventing unique serial numbers from being printed on the VVPAT records—and when this option is turned off, the barcodes do not contain ballot keys.

The team was also able to verify that Hart had resolved the issues identified as "Inconsistent Records" in the report "An Analysis of the Hart InterCivic DAU eSlate," forthcoming in the 2007 USENIX/ACCURATE Electronic Voting Technologies Workshop. Inconsistent records can no longer be produced through the methodologies described in that report; instead, the JBC has an added "Access Code Recovered" function that ensures ballots are consistently recorded between devices in the event of communication interruption and/or temporary device failures.

IV. Successful Attack Scenarios

The following attack scenarios were successfully carried out in the laboratory environment of the Secretary of State's testing facility.

1. Attack Scenario 1

   In this scenario, a malicious voter prepares a surreptitious device and brings it with her to the polling station during early voting. She registers as usual and is issued an access code. Before she leaves the registration table, however, she quickly connects her device to the JBC and converses with the poll workers for a brief time—thirty to forty seconds should suffice. She proceeds to an eSlate and casts a ballot normally. She then enters arbitrary access codes and casts ballots at will, continuing to do this for as long as she suspects she will be unchallenged in the voting booth, casting an arbitrary number of ballots. This results in an electronic ballot box stuffing attack.

   In an early voting situation, when the JBC doesn't print out a ballot access receipt each time an access code is issued, the Polls Suspended Report (automatically printed by the JBC) will indicate an unusually large number of access codes issued and more ballots cast than voters who checked in at the registration desk when polling concludes. In regular election mode, this problem would likely be detected much sooner, since the JBC is designed to print a ballot access receipt each time an access code is issued by the machine.

2. Attack Scenario 2

   In this scenario, a malicious poll worker finds an opportunity after the close of polls to alter the contents of the MBB using his personal laptop. The attacker identifies ballots containing votes for a candidate he doesn't want to win the election and overwrites those ballots with records containing votes for a candidate he does want to be successful. After tampering with the MBB, the attacker replaces it in the expected chain of custody. The technological safeguards for detecting this tampering are insufficient and can, by default, go unobserved. This results in altered vote totals that can only be detected in the event of a manual recount of eSlate VVPAT records.

3. Attack Scenario 3

   In this scenario, a malicious observer uses a remote device to capture the audio narration – including the narration associated with a voter's actual voted ballot – from an eSlate with audio capabilities. She is able to observe voters walking up to the eSlate and match them to the audio narration she is capturing, allowing her to violate a voter's right to privacy by linking voters to their vote selections.

V. Potential Attack Scenarios

The team believes, based on our research, that the following scenarios would be successful; however, we didn't have the time necessary to successfully complete them.

1. Potential Attack Scenario 1

   In this scenario, a malicious voter again prepares a surreptitious device to bring to the polling station. However, this time the voter plants his device inside the voting booth itself, where it is able to intercept communication between the JBC and eSlates. The device can issue signals to the JBC mimicking the casting of an arbitrary number of ballots (even without being issued access codes), effectively performing an electronic ballot box stuffing attack.

2. Potential Attack Scenario 2

   In this scenario, a malicious voter uses a surreptitious device to extract the image of the eScan. Using a prepared parser, the voter identifies the secret key from this image. She uses this insider information to prepare a handful of forged MBB cards, which she manages to work into the chain of custody either by replacing valid MBB cards or by tossing forged MBB cards into poll worker materials at the close of polls, undetected by poll workers who unwittingly return both the valid and the forged MBB cards to central count. These MBB cards alter vote totals and can impact the outcome of an election.

   Note: The Red Team was able to extract the eScan image and, from the image, identify the secret key. The team did not have time to successfully forge an MBB.

3. Potential Attack Scenario 3

   This scenario is a variation on Potential Attack Scenario 2. In this case, instead of extracting an image from the eScan, the attacker reflashes (i.e. reinstalls) the eScan's software. The new software mimics valid software, but when the eScan is connected to SERVO at the post-election processing, the eScan maliciously exploits a buffer overflow in SERVO's input handling procedures. Using this leverage, the eScan implants malicious software into SERVO, and SERVO infects all future devices (eScans, JBCs, eSlates, and MBBs) to which it is connected. The next election is controlled by the attackers, who have covert management of the devices.

   Note: The Red Team, in conjunction with the 2007 TTBR Hart Source Code Team, was able to overwrite eScan software and also to exploit an existing buffer overflow vulnerability on SERVO. The teams did not have time to combine the attacks nor to craft the rest of the attack scenario provided here.

VI. Conclusions

Although the Red Team did not have time to finish exploits for all of the vulnerabilities we discovered, nor to provide a complete evaluation of the Hart voting system (System 6.2.1), we were able to discover attacks for the Hart system that could compromise the accuracy, secrecy, and availability of the voting systems and their auditing mechanisms. That is, the Red Team has developed exploits that – absent procedural mitigation strategies – can alter vote totals, violate the privacy of individual voters, make systems unavailable, and delete audit trails.