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 Diebold Election Systems Incorporated voting system (Diebold GEMS 1.18.24/AccuVote), 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 Diebold 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 14 and concluded on July 19, during which time the team was testing both the Diebold Election Systems Incorporated voting system and the Hart InterCivic 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 Diebold GEMS 1.18.24/AccuVote system, 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 Diebold Election Systems Incorporated voting system (Diebold GEMS 1.18.24/AccuVote) in order to discover exploits that have the potential of violating 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 Hart system are presented in a separate report.

We present our findings here. In Section 2, we present an overview of the Diebold voting system and how the system components interact. 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 to previous studies throughout this report. 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.

II. Device Descriptions

The following is a full list of Diebold GEMS 1.18.24/AccuVote devices evaluated during the Top to Bottom Review. This section will give a brief description of each device in the Diebold 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. **GEMS Server** - Diebold election management system software is called GEMS (Global Election Management Systems). It is run on a server that is manually configured by Diebold technicians. We use the phrase "GEMS server" to reference the entire physical server in its delivered configuration, including the operating system (Windows 2000 Server), all software – including but not limited to GEMS software, and the physical configuration of the server.

   The GEMS server is used to set up the ballot definition, create security and administrative smart cards, program TSx and AV-OS memory cards, and print paper ballots. During the election, the GEMS server is responsible for performing image processing on the ballots scanned by the Central Count AV-OS. After the election, the GEMS server tallies the election results and is used for generating election result reports and databases.

2. **AV-TSx** – The AV-TSx (AccuVote-TSx – also referenced throughout this document simply as TSx) is the DRE (Direct-Recording Electronic) voting terminal on which voters cast ballots. Diebold technicians informed us that a TSx is used at Election Central to program PCMCIA cards for the election; cards programmed in a TSx unit may be used in the unit in which they were programmed or in other TSx units. The TSx can perform initial setup (card programming) and final reporting to the GEMS server by memory card transfer, Ethernet connection, or modem line. Though other means exist for writing to and reading from the memory cards, the Red Team tested the configuration described by Diebold technicians.

3. **AV-OS** - The AV-OS (AccuVote Optical Scan) is an optical ballot scanner. The AV-OS uses an Espon 40-Pin memory card (or compatible card – though Epson discontinued production of these cards in 1998) to store configurations and election definitions. Diebold technicians informed us that cards may be programmed in the AV-OS in which they will be used during the election, or in another AV-OS unit. The AV-OS can perform initial setup (card programming) and final reporting to the GEMS server by memory card transfer, Ethernet connection, or modem line. Though other means exist for writing to and reading from the memory cards, the Red Team tested the configured described by Diebold technicians.

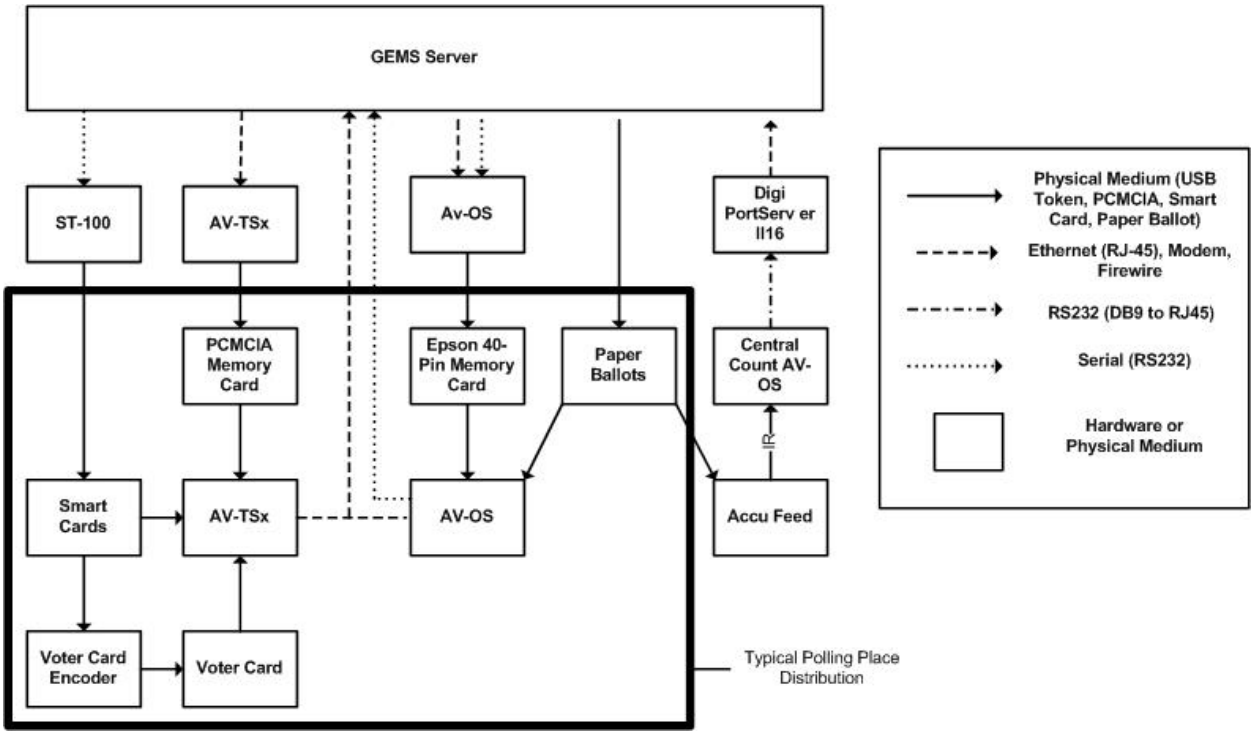
4. **Central Count AV-OS** – This AV-OS is connected to the AccuFeed to read paper ballots in bulk at a central count facility. It communicates to the GEMS server via the DigiPort Server II16, and the GEMS server performs all image processing of the paper ballots.

5. **AccuFeed** – The AccuFeed is used in a central count facility to feed paper ballots (cast at the polling places or by absentee voters) into the Central Count AV-OS. The AccuFeed communicates with the Central Count AV-OS via infrared.

6. **Smart Cards** – Smart cards are used to control the security and administration of an election. There are four distinct types of smart cards: Security Key Cards, Central Administrator Cards, Supervisor Cards, and Voter Access Cards. The first two are intended to be used only by Central Count officials, while Supervisor Cards are distributed to poll workers for their use during and after the election; the Central Administrator and Supervisor Cards grant access to the respective administrative menus. Voter Access Cards are used by voters as tokens which authorize each voter to cast a single ballot at a TSx unit. Smart cards are written either by the ST-100 card reader/writer connected to the GEMS server or (only in the case of Voter Access Cards) the Voter Card Encoder at the polling place.

7. **ST-100** – The ST-100 smart card reader/writer is connected to the GEMS server via a serial cable. It is used to encode the various smart cards used throughout the election process.

8. **DigiPort Server II16** – The DigiPort Server II16 is an intelligent network hub. It translates serial communication into Ethernet (and vice versa) in order to facilitate communication between the Central Count AV-OS units and the GEMS server.



Interactions Between Components

The GEMS server is used to create and define all aspects of an election, create security and administrative smart cards, and upload the election definitions to other components used during the election. The GEMS server encodes smart cards to be used by central count and polling place personnel using the ST-100.

The GEMS server is connected to both the TSx and AV-OS and the election definition will be downloaded to the removable memory cards for both systems: a PCMCIA for the TSx and an

Epson 40-Pin memory for the AV-OS. The GEMS server can also be used to create paper ballots for use in the election.

The TSx and AV-OS units used to create the original memory cards can be deployed to the polling place, or the cards can be deployed in other TSx and AV-OS units.

The smart cards programmed by the GEMS server through the ST-100 are used to program the Voter Card Encoder, to access administrative functions on the TSx units, to start and end the election on the TSx units, and (if applicable) to accumulate results from the PCMCIA cards used in other TSx units.

Each voter is given a Voter Card created by the Voter Card Encoder. The voter inserts her Voter Card into the TSx, and this authorizes her to cast a ballot on the TSx. Alternatively, the voter may receive a paper ballot that will either be read by the AV-OS at the voting site or accumulated and read by a Central Count AV-OS. If paper ballots are read at the central count site, they are fed into the Accu Feed device, controlled by an AV-OS and processed by the GEMS server.

At the end of the election day, the TSx and AV-OS units can transmit results to the GEMS server by a number of methods, including Ethernet or modem. The PCMCIA and Espon 40-Pin memory cards (from the TSx units and the AV-OS units, respectively) can be returned to central count where they are loaded into designated TSx and AV-OS units, which are connected, respectively, via Ethernet and serial connections. Alternately, the TSx and AV-OS units used in the polling stations can upload results via direct Ethernet and serial connections or via modem transmission[2]. The GEMS server tallies election results and prepares end of election databases and reports.

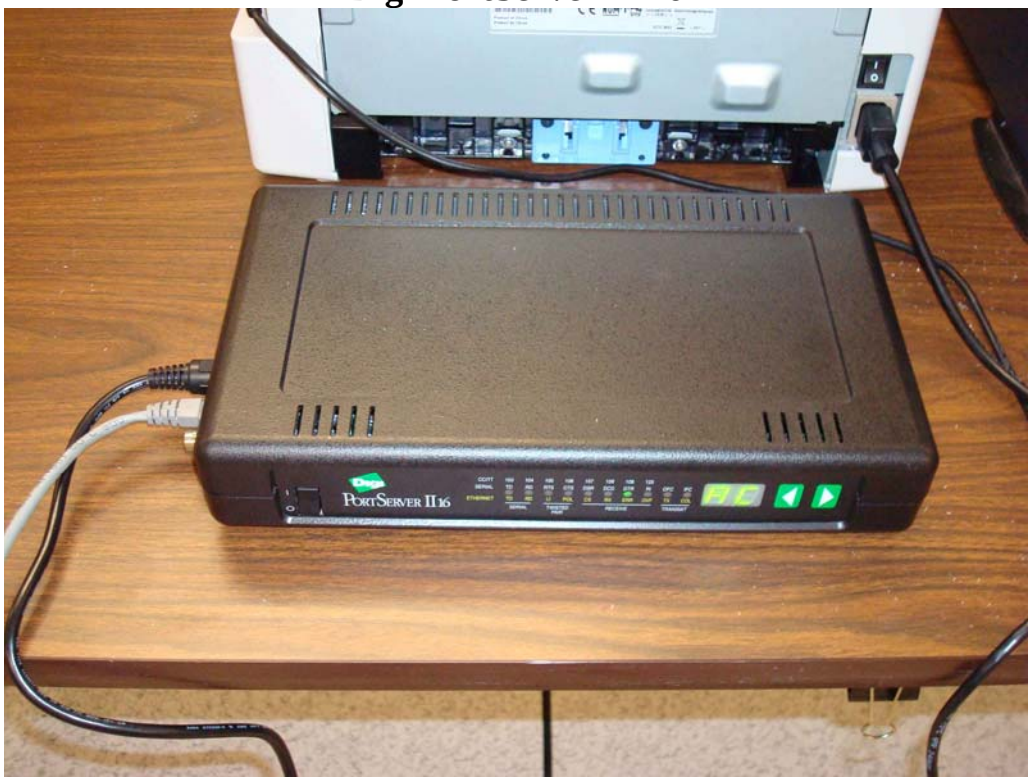
[2] Again, there exist other means for reading from the memory cards, but this is what Diebold technicians described to the Red Team as standard practice.

GEMS Server

Accuvote TSx

AccuVote OS (Optical Scan)

Digi PortServer II 16



SecureTech ST-100 PCMCIA Card Reader

Spyrus Voter Card Encoder and Smart Cards

AVOS and AVTSx Memory Media

III. Relevant Findings

In this section, we present a high-level description of the vulnerabilities we found in the Diebold 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:

Diebold GEMS 1.18.24/AccuVote

1. GEMS software, version 1.18.24
2. AccuVote-TSX with AccuView Printer Module and Ballot Station firmware version 4.6.4
3. AccuVote-OS (Model D) with firmware version 1.96.6
4. AccuVote-OS Central Count with firmware version 2.0.12
5. AccuFeed
6. Vote Card Encoder, version 1.3.2
7. Key Card Tool software, version 4.6.1
8. VC Programmer software, version 4.6.1

1. GEMS Server Vulnerabilities

There were stark discrepancies between the GEMS server as Diebold technicians delivered it and the GEMS server configuration as described in the Diebold documentation. The Diebold technicians assured us that the configuration we were given at the outset of the study was identical to the configuration Diebold technicians would supply to their customers (i.e. county officials). Thus, our findings are based on a system configured by Diebold technicians exactly as they informed us they would prepare a system for delivery.

The GEMS server is on a local area network (LAN) with other Diebold components, and this LAN is supposed to be isolated. However, even Diebold documentation reports that this requirement is not always met. Therefore, attacks via Ethernet against the GEMS server could reasonably be executed by personnel with physical access to the networking components (hubs/switches) in the isolated LAN or— if the Diebold LAN were intentionally or unintentionally connected to a public internet connection—by remote attackers

a. Windows Vulnerabilities

The Red Team performed vulnerability scans against the GEMS server. The results identified multiple vulnerabilities; primarily, these vulnerabilities existed because the Windows 2000 server (configured by the Diebold technicians) was not properly patched.[3] After noting these vulnerabilities, the Red Team was able to download an exploit from a

[3] Even if the Red Team had been expected to make other system configuration changes in order to make the GEMS server consistent with Diebold configuration documents, it would have been highly unreasonable for Diebold to expect the Red Team to patch Windows 2000 Server.

free public repository of well-known and documented exploits. This exploit gave the Red Team access of a Windows Administrator on the GEMS server.

Additionally, the Red Team noted that most standard Windows logging capabilities were either disabled or enabled in very limited states in the configuration provided by Diebold. This means that most malicious actions taken by attackers would not be traceable. More detail on the auditing configuration of this system is available in the report prepared by the 2007 TTBR Diebold Documentation Review Team.

Finally, the Red Team uncovered evidence that Diebold technicians created a remotely-accessible Windows account that, by default configuration (according to the Diebold documentation), can be accessed without the need to supply a password. There is evidence to suggest that this account is intended to be used by TSx units for dial-in access at the close of polls on Election Day, but the documentation for election officials never mentions this particular account by name. An attentive system administrator would notice the account. However, the responsibility should not be on election officials to discover remotely-accessible Windows accounts and act appropriately to ensure those accounts are not inappropriately accessed. Devices, as delivered to customers, should only have accounts that are well-documented and remote access that is necessary for the needs of the particular county. Undocumented remotely-accessible logins are contrary to generally-accepted security practices.

b. GEMS Databases
The Red Team used Windows Administrator access on the GEMS server to manipulate and corrupt GEMS databases. These actions could result in manipulated vote totals or in the inability to read previously-generated ballot definitions if no valid database backups were available (whether because the backups were not made or because the backups had also been corrupted). On election night, the inability to read results from the deployed TSx and AV-OS devices could render an election impossible to complete electronically. In this case, a hand count of paper ballots and VVPAT records would be the only option for deducing the intent of the voters who turned out on Election Day.

c. GEMS Audit Logs
The Red Team found methods for executing actions from within the GEMS server that could not be tracked by the GEMS audit logs, allowing malicious GEMS users to conceal actions they had taken while logged in. Additionally, the Red Team noted that one of the standard functions offered by GEMS is the ability for a GEMS administrative user to change the username of her account. This is a non-standard computing practice, and it could potentially be used by a rogue administrator to implicate another GEMS user (i.e. other elections personnel).

d. GEMS Election Configurations
The Red Team identified format string vulnerabilities that, when exploited, caused an election to run smoothly on a TSx unit until a voter from a particular precinct attempted to cast a ballot. When a voter from the affected precinct tried to cast a ballot on a TSx, the printer would generate an error, and the voter's ballot would be canceled. The voter

is notified about the error via a series of error messages that would be incomprehensible to the average voter, followed by this notification: "Your ballot has been canceled."

2. GEMS Server Networking Components

Using information gained from access obtained as the Windows Administrator user, the Red Team was able to guess the authentication credentials for the networking hardware supplied by Diebold, and gain root access on these devices. These root accesses would provide sufficient access for an attacker to manipulate every setting on the networking devices and on the server. Additionally, the Red Team was able to use this access on the GEMS server to install the drivers for a USB wireless dongle. This small device was then planted on the back of the server, ensuring remote access to the GEMS server even if it were disconnected from the Ethernet connection previously used to exploit the server.

3. Precinct Count AV-OS

The Red Team was able to verify the findings of some previous studies on the AV-OS unit; the impact of these was to alter vote totals in order to change the vote results on that machine.

The Red Team was also able to craft low-tech attacks that could cause an AV-OS unit to stop reading ballots, rendering it unusable for the remainder of the Election Day. This would not preclude voters from casting ballots or ultimately prevent ballots from being tallied. However, it could preclude ballots from being scanned at the precinct to help a voter determine if they "over-voted" their ballot.

4. TSx

a. TSx: Physical Security

The Red Team was able to violate the physical security of every aspect of the TSx unit, using only tools that could be found in a typical office. This guaranteed the access necessary to execute physical and electronic attacks. The team was also able to jam the locks, which would not only provide evidence of election tampering (the effects of which are unclear and would depend on county procedures) but which could also potentially render devices inoperable for future elections, let alone for the retrieval of election data already loaded on the device at the time of attack.

b. TSx: Malware

The team verified previous findings regarding multiple avenues for overwriting system firmware and software as well as for the introduction of malware that would affect the current software. These avenues, when exploited, are a platform for altering vote totals to potentially change the outcome of an election. They could also be leveraged to violate voter privacy[4] or enact a denial of service on affected devices.

Of potentially greater concern, the introduction of malware into a TSx unit could spread virally into the GEMS server via format string errors in the GEMS software as identified

[4] Cast ballots are stored – with timestamps – on the TSx in the order in which they were cast. For more details on this, please see the 2007 TTBR Diebold Source Code Team report.

by the team. TSx units use PCMCIA cards to store and transport election definitions and vote totals. When those vote totals are communicated back to the GEMS server (either by physical transfer of the PCMCIA card into a TSx unit connected directly to the server's LAN or over a dial-in connection), an exploited TSx could virally infect the GEMS server. Future TSx and AV-OS units connected to the GEMS server could likewise be infected as ballot definition files are transferred via serial or Ethernet connection.

c. TSx: Escalation of Privileges
The Red Team identified attacks that can escalate the privileges of a voter to those of a poll worker or those of a central count administrator. These attacks use tools that can be found in a typical office and could be executed by a very low-skilled attacker.

The privilege escalations can allow a voter to reset an election (deleting all electronic records of ballots cast so far on the system, including backup records), issue unauthorized Voter Access Cards (the single-use tokens used by voters to allow authorized voters to each cast only a single ballot at a TSx station), program a TSx unit to remotely call an attacker's modem, gather sufficient login information to gain unauthorized remote access to the GEMS PC, or close polls and view all ballots already cast on the particular TSx unit—all without any insider knowledge of election-specific data such as the security keys in use.

d. TSx: Default Static Key
The Red Team verified that a previously-identified default static key is still in use on the systems. Diebold documentation urges election officials to not use this static key and to generate their own election-specific keys. If election officials opt to use the static keys (or forget to change them), the TSx units display a particular icon on the screen to warn that the keys in use are insecure. A knowledgeable attacker could observe this icon and use the information being leaked by the TSx unit to craft more specific attacks for the system.

e. TSx: Malicious Voter Input
Multiple voter-accessible input fields on the TSx are susceptible to malicious input. The Red Team tested these input fields and observed erratic TSx behavior in response to proof of concept code. The team did not have time to study these vulnerabilities sufficiently to craft working exploits but notes that the lack of input validation allowed us to generate unusual printed output and/or crash the units when we provided malicious input to these fields.[5]

f. TSx: VVPAT
The Red Team found a simple attack that can put the Voter Verifiable Paper Audit Trail (VVPAT) printer out of service until the TSx unit is rebooted. This attack requires only tools that can be found in a typical office. Voters who were not aware that they should expect a printed version of their ballot for review would not observe anything unusual,

[5] Similar vulnerabilities exist in input fields accessible through administrative menus.

because one result of this attack is to cause the TSx to stop issuing reminders to voters that they should verify the printed record of their selections.

The team also found that the design of the TSx printer enabled us to devise attacks on the printed records that could covertly destroy VVPAT records using a common household substance.[6] This is particularly notable because the attack meets the following conditions:

1. It affects records printed before the attack is executed.
2. It affects records printed after the attack is executed.
3. It does not affect the way records are displayed to voters as they are produced – so as to avoid raising voter suspicion before the close of polls.
4. It does not affect the printer mechanisms or jam the printer – again, to avoid raising suspicion.

The impact of these attacks is to make many of the VVPAT-printed ballots completely unreadable and most of them barely or only partially readable. A successful attack could not only destroy records already printed by the VVPAT at the time of the attack but could also potentially destroy all records produced throughout the rest of the day by that particular VVPAT. The impact (once discovered) is highly visible, but when combined with an electronic attack that destroyed ballots, it could serve to effectively nullify most – if not all – of the ballots cast on a particular TSx unit. This attack is particularly viable on the TSx because the design of the VVPAT printer and the security casing for printed records allows the attack substance to linger undetected inside the machine until the end of election day; neither subsequent voters nor poll workers would know the attack had taken place until the printed records were removed at the end of Election Day.

g. TSx: PCMCIA card

The Red Team verified the results of other studies, which found that modifications to the contents of the PCMCIA card could affect the accuracy of vote totals. Additionally, the Red Team discovered that an attacker could extract GEMS server login credentials from the PCMCIA card in a TSx which had been programmed to dial in to GEMS at the close of polls.

[6] The Red Team has confirmed that the design of the printers on the Hart and Sequoia systems tested for the 2007 TTBR would not inherently enable attacks of the same magnitude. That is, no known attacks for the Hart or Sequoia printers could meet all four conditions listed above.

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, an attacker approaches a TSx unit during an election. The attacker may be a registered voter who first checks in with poll workers at the front desk and is issued a Voter Access Card, or she may simply walk into a busy polling station and slip unnoticed into the crowds and approach a TSx. She brings with her a few small tools for executing the attack; these tools, which can be concealed in the palm of her hand, are standard office equipment and would not be cause for suspicion even if they were seen by others in the polling station.

   In the span of time it takes for many voters to cast a typical ballot on a TSx unit, the attacker brings the system into an administrative mode, deletes the ballots cast thus far on the TSx (both the primary and backup records), and restarts the election on this particular unit. This effectively erases all electronic records of ballots already cast on this unit.

   Finally, the attacker executes a covert chemical attack that destroys or critically damages most, if not all, of the already established VVPAT records on this unit. The chemical attack also damages or destroys future records printed on this VVPAT, and it is highly unlikely that the attack will be observed until the close of election. This renders the paper trail almost completely unrecoverable, making it unlikely that the electronic attack would be detected, allowing the attacker to successfully nullify all ballots cast before the attack was launched.

2. Attack Scenario 2

   This scenario is a variation on the first, but in this scenario the attacker uses the "View Cast Ballots" option in the Polls Closed menu to view and print extra VVPAT records of ballots the attacker considers favorable. After printing an arbitrary number of favorable ballots, the attacker resets the election and leaves the TSx unit in Election Mode with zero recorded electronic ballots. At the close of polls, neither the VVPAT records nor the electronic records will be accurate.

3. Attack Scenario 3

   In this scenario, the attacker brings a stack of smart cards that she has formatted in such a way that a TSx unit will recognize them as generic Voter Access Cards. They do not contain election-specific credentials and thus require no insider information to prepare.

   He launches an attack that escalates his privileges to access a Poll Worker Menu and then uses the TSx to manually authorize the smart cards he brought. He can either use these himself to cast an arbitrary number of ballots or distribute them to collaborators who can each cast an arbitrary number of ballots. This effectively constitutes an electronic ballot box stuffing attack. While such an attack would likely be detected during the standard vote reconciliation process, it is not clear what would happen in the event more votes were recorded than there were voters who had signed in at the polling place.

4. Attack Scenario 4

In this scenario, the attacker launches a low-tech attack that can be discreetly executed at a Precinct Count AV-OS under the watch of a moderately attentive poll worker. The tools for completing the attack are small and easily concealed, and they can be obtained in a typical office. After the attack is completed, the AV-OS will no longer accept ballots for counting. While this won't preclude voters from casting ballots or ultimately having them counted, this attack does remove the AV-OS from service for the remainder of Election Day.

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, the attacker uses the TSx as a platform for gaining login credentials necessary to gain unauthorized remote access to the GEMS server. She executes an attack using tools found in a typical office to bring the TSx unit into a menu from which she can recover the phone number for the GEMS server's modem, as well as the username and length of password for a valid Windows account on the GEMS server.

She returns home with these credentials and remotely logs in to the GEMS server. With this Windows access, she is able to modify GEMS databases, altering vote totals. She can also simply delete GEMS databases, possibly making it impossible for election officials to read the electronic results from the TSx and AV-OS units at the end of Election Day.

2. Potential Attack Scenario 2

In this scenario, the attacker prepares a PCMCIA card with malicious software and brings it with him to the polling station. He bypasses the physical security protecting the PCMCIA card slots and inserts his card into the TSx unit. The malware on the card is loaded onto the TSx and overwrites the software on the system. He replaces the official election PCMCIA card, which is infected by the compromised TSx. When the card is later uploaded to the GEMS server, the malware is transferred to the GEMS server, which is used as a locus for spreading the infection to all other TSx units and future AV-OS memory cards. The attacker is able to use this viral infection to alter vote totals for the election at hand and to control future elections, as well.

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 Diebold GEMS 1.18.24/AccuVote system, we were able to discover attacks for the Diebold 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.