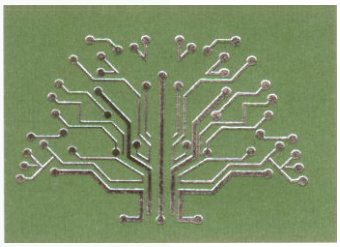

FREEMAN, CRAFT, MCGREGOR GROUP

PUBLIC REPORT

Red Team Testing of the ES&S Unity 3.0.1.1 Voting System

Freeman Craft McGregor Group (FCMG) Red Team

Prepared for the California Secretary of State by:

Jacob D. Stauffer, FCMG Red Team Project Manager

February 15, 2008

Executive Summary

The California Secretary of State tasked Freeman Craft McGregor Group (FCMG) to perform "red team" analysis (penetration testing) of the ES&S Unity 3.0.1.1 Voting System ("ES&S Voting System"). The Red Team's goal was to compromise the security of the voting system. The team demonstrated that several components of the voting system are vulnerable to attack. This report provides a description of the ES&S Voting System followed by the Red Team's findings.

1. Introduction

The Red Team attempted to compromise the physical security and logical security of the ES&S Voting System. The strategy involved the identification of vulnerabilities and the development and execution of attacks (exploits) that impact voting system confidentiality, integrity and availability. Components of the voting system that were evaluated included the election management software, audit system, reporting system, voter assist terminals, tabulators, and storage media.

The Red Team focused on identifying and exploiting vulnerabilities. After an exploit was shown to be feasible, it was further analyzed to identify the enabling factors. This included determining the potential actors, their familiarity with the target, their likely skill set, potential window of opportunity and the equipment required to execute the exploit.

The next section, Section 2, provides a detailed description of the ES&S Voting System. Section 3 describes some of the vulnerabilities identified and the exploits developed during penetration testing. Section 4 lists the exploits that were unsuccessful. Section 5 provides concluding remarks.

2. ES&S Voting System

The ES&S Voting System provides the functionality to set up, administer, tabulate and report elections. The configuration that was tested by the Red Team is shown in Figure 1. Note, however, that the system may be configured in a variety of ways to conform to specific state election regulations. The major components of the ES&S Voting System are:

Unity Election Management System: Used for election configuration and reporting.
M100 Tabulator: Used for scanning ballots at the precinct level.
M650 Tabulator: Used for high-speed scanning of mailed ballots and absentee ballots.
Voter Assist Terminal: Used to provide ballot-marking assistance for voters with disabilities.
AIMS System: Used for Voter Assist Terminal configuration.

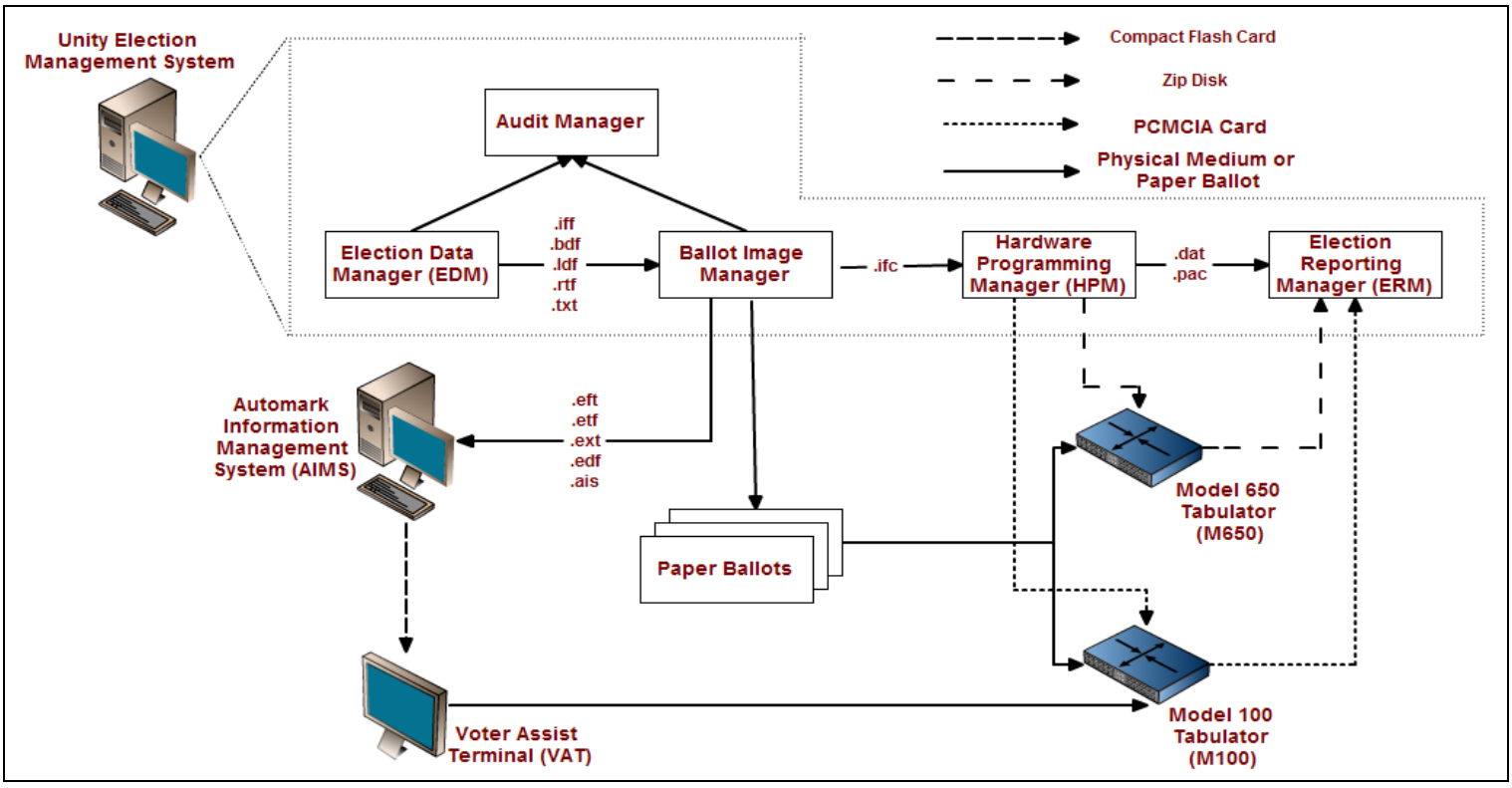

Figure 1: ES&S Voting System.

The following sections describe the major components and sub-components of the ES&S Voting System.

Unity Election Management System

The Unity Election Management System generates election definitions and audits their creation, administers system access controls, programs election hardware, helps design ballots and generates election reports. The Unity Election Management System consists of the Election Data Manager, Audit Manager, Ballot Image Manager, Hardware Programming Manager and Election Reporting Manager.

Election Data Manager

Election officials or ES&S election definition developers use the Election Data Manager (EDM) to configure all contest, candidate and polling place information used in an election. The EDM stores the election configuration information (precinct, office, race and candidate data) in a database. The database is used by the Ballot Image Manager (described below) for configuring the ballot layout. The EDM is accessed using a login name and password; authentication is performed by the Audit Manager (described below).

Ballot Image Manager

The Ballot Image Manager is used by layout artists to design paper ballots for the Model 100 Tabulator and the Model 650 Tabulator (described below). The artists create optical scan ballots using candidate and jurisdiction data from the EDM. After the ballots are designed, the Ballot Image Manager generates an interface file (`.ifc`) for use by the Hardware Programming Manager (described below) to program ballot scanning equipment.

Audit Manager

The Audit Manager provides various features including user activity tracking for the EDM and Ballot Image Manager. The Audit Manager runs in the background and provides a real-time audit log of user inputs and system outputs. Election officials use the Audit Manager to set passwords for the Unity Election Management System and to track user activity.

Hardware Programming Manager

The Hardware Programming Manager (HPM) is used by election officials to generate configuration data for the ballot scanning hardware based on the interface file produced by the Ballot Image Manager. The interface file contains ballot positions for all the candidates in an election. The HPM formats election data for the specific type of election equipment used in

a jurisdiction. In the case of the ES&S Voting System in this evaluation, the HPM is used to export election configuration information to PCMCIA memory cards for Model 100 Tabulators and to Zip Disks™ for Model 650 Tabulators.

Election Reporting Manager

The Election Reporting Manager (ERM) is used to generate election reports. Election data used to create the reports is imported from PCMCIA cards and Zip Disks™ used in the M100 and M650 Tabulators, respectively. The ERM may also be used to send election reports to state officials and the news media.

AutoMARK Information Management System

The AutoMARK Information Management System (AIMS) is used to set up configuration information required by Voter Assist Terminals (described below). AIMS imports raw election data from the Unity Election Management System and after some refinement by election officials, the configuration data is verified and AIMS writes the data to a Compact Flash memory card for use by a Voter Assist Terminal.

Voter Assist Terminal

The Voter Assist Terminal (VAT) is used by voters with disabilities to mark their ballots during an election. The VAT is a stand-alone machine that runs the Windows CE operating system and includes various sub-systems including a touch screen monitor and an integral ballot marker. A voter inserts a pre-printed unvoted ballot with bar codes (containing information about the ballot) into the input tray of the VAT. The device scans the bar codes and presents a series of menu-driven voting choices on a color touch screen. The VAT accumulates the voter's choices in its internal memory and, when the selection process is completed, provides a summary of the choices for review. After the voter confirms the selections, the VAT marks the ballot using its built-in printer and returns the ballot to the voter. The voter may then confirm that the ballot is marked as intended and insert it into a standard tabulator (described below).

Model 100 Tabulator

The Model 100 (M100) Tabulator is an optical scanner used to scan voted ballots at the precinct level. The election configuration is loaded from a PCMCIA card before an election. The same card used to load the definition, or a different PCMCIA card, can be used by the tabulator to store votes. After the polls are opened, ballots are marked by voters and fed into the M100. The M100 can be configured to detect ballot marking errors such as over votes and unmarked ballots. As ballots are scanned, vote counts are updated on the PCMCIA card.

After being scanned, ballots are dropped into one of two bins, one for standard ballots and the other for ballots containing write-in votes. After the polls close, the PCMCIA card containing the votes, as well as the paper ballots, are transported to a central location for processing by the Unity Election Management System.

Model 650 Tabulator

The Model 650 (M650) Tabulator is a high-speed optical scanner used for scanning mailed and absentee ballots at a central location. After the election configuration is loaded on a M650 using a 100 MB Zip Disk™, stacks of ballots are fed into the scanner using an automatic feeder. The M650 prints a continuous audit log to a dedicated printer; election results and reports are printed using another printer. At the conclusion of ballot scanning, the results are saved to a Zip disk and are subsequently processed by the Unity Election Management System.

3. Vulnerabilities and Exploits

This section is a high-level overview of all vulnerabilities discovered during the red team evaluation. Note that the evaluated system is very complex and is certain to have additional (undiscovered) vulnerabilities.

3.1 Ballot Box Stuffing (M100 Tabulator)

PCMCIA cards used by M100 Tabulators may be exchanged at the precinct during an election to implement ballot box stuffing attacks in favor of particular candidates. This exploit is difficult to detect without examining the audit logs.

3.2 PCMCIA Card Modification (M100 Tabulator)

All data on the PCMCIA card is unencrypted and can be viewed using commonly available programs. This enables a potential attacker to analyze the data on the card and develop strategies to defeat the embedded security mechanisms.

3.3 Ballot Box Stuffing (Election Reporting Manager)

Election results may be modified by a attacker with unauthorized access to the Election Reporting Manager (ERM). The Red Team identified an exploit that enables the unauthorized access. Upon gaining access to the ERM, attacker can manually add or remove votes from the official vote totals. Note that the ability to manually edit vote totals is necessary to correct errors, but only authorized individuals should have access to this feature. The attack would take a few seconds and, if executed properly, could only be detected by analyzing audit logs.

3.4 Election Result Modification (M650 Tabulator)

The Zip disk containing the Model 650 tabulation results may be modified while it is transported to the Election Reporting Manager, which would process the modified vote totals without questioning their validity.

3.5 Database Access (Audit Manager)

An attacker with unauthorized access can gain complete access to the Audit Manager database by cracking the password. Once access to the database is gained, the attacker can change records, create or remove login credentials for the Audit Manager, EDM, or ESSIM and delete audit log entries to cover his/her tracks.

3.6 Login Name and Password Enumeration (Audit Manager, Election Data Manager and Ballot Image Manager)

Login names and passwords for the Audit Manager, Election Data Manager and Ballot Image Manager, may be obtained by executing the exploit described in Section 3.5 (Database Access (Audit Manager)).

3.7 Malicious Database Modification (AutoMARK Information Manage-ment System)

An attacker with unauthorized access could modify stored procedures in the Microsoft SQL Server database used by the AutoMARK Information Management System (AIMS). The exploit gives the attacker the ability to write modified ballot definition files data to the Compact Flash cards used by the Voter Assist Terminals. This attack would mainly be used to modify the audio/visual information of the ballot so that candidates are misrepresented when a voter is using the audio ballot so that a vote for one candidate actually goes to another candidate. This exploit would be most effective if the attacker had ample knowledge of how a district would vote and if the marked ballots were not evaluated for discrepancies.

3.8 Audio/Visual Ballot Layout Tampering (Voter Assist Terminal)

An attacker with unauthorized access could configure a Voter Assist Terminal (VAT) so that the audio information is inconsistent with the visual information. For example, a voter might hear *Candidate A* while the screen reads *Candidate B*, resulting in a vote for the wrong candidate (*Candidate A*). The exploit will not be detected unless the voter verifies his/her printed ballot.

3.9 Access Control System Tampering I (Hardware Programming Manager and Election Reporting Manager)

An attacker with unauthorized access working with a computer systems expert could disable the access control system for the Hardware Programming Manager (HPM) and the Election Reporting Manager (ERM) in a few minutes. Unauthorized access to the HPM and/or ERM constitutes a serious breach of voting system security.

3.10 Access Control System Tampering II (Hardware Programming Manager and Election Reporting Manager)

An attacker with unauthorized access could tamper with the access control system for the Hardware Programming Manager (HPM) and the Election Reporting Manager (ERM). In

particular, the attacker could selectively grant (or deny) any individual the right to access the HPM and ERM.

3.11 Access Control System Password Compromise (Hardware Programming Manager and Election Reporting Manager)

An attacker with physical access to the system and the appropriate expertise could obtain the password for accessing the Hardware Programming Manager (HPM) and Election Reporting Manager (ERM) in a few minutes.

3.12 User ID Enumeration (Hardware Programming Manager and Election Reporting Manager)

An attacker with assistance from a computer systems expert could compile a list of user ids for the access control system used by the Hardware Programming Manager (HPM) and Election Reporting Manager (ERM). While this attack would not produce significant results in the Hardware Programming Manager, other then the ability to remove candidates from a ballot, it can significantly affect an election outcome using the Election Reporting Manager. One of the administrative controls in the Election Reporting Manager is the ability to modify election results (e.g. add or remove votes from a candidate). An attacker with an administrator user ID can log into the Election Reporting Manager, change vote tallies for specific candidates, and logout of the system unchecked. Access to a working system prior to the election is a prerequisite for this exploit.

3.13 Lock Picking (Voter Assist Terminal, M100 Tabulator and M650)

An individual with sufficient expertise can pick the locks located in the front of the Voter Assist Terminal (VAT), the M100 Tabulator and the M650. The time taken by the Red Team to pick the VAT, the M100 and the M650 locks ranged from five seconds to one minute. With this method an attacker can shutdown, turn on, or put the VAT into "Test Mode" which would allow an attacker to access system information and system administration controls. This exploit can be used to turn off a VAT, serving as a denial of service attack. Recovery from the attack would require a poll worker to restart the system. Once the system is restarted, the VAT takes approximately 2-5 minutes to reinitialize prior to continuation of voting.

If an attacker was able to pick the lock of the ballot box holding the M100, an attacker can gain access to the front panel of the M100 that holds the PCMCIA cards only if seals are not correctly used. If the PCMCIA card is accessible a number of vulnerabilities can be exploited. For example an attacker can remove the card after it has recorded votes and place a blank

card with the same ballot definition and discard the previous PCMCIA card and the votes recorded on it. If the front panel of the M100 is not accessible an attacker can remove the system from the ballot box diverter disabling write-in ballot sorting (see section 3.13). Furthermore an attacker can use this method to gain access to the paper ballots stored in the ballot box.

An attacker can gain access to the controller boards and mechanics of the M650 using this method only if no paper seals are used or if the paper seals can be removed without evidence of tampering. Once inside, an attacker can misalign rollers used to feed ballots or misalign ballot scanners so that ballots are not read correctly, ultimately serving as a denial of service attack for mass ballot reading and tallying.

3.14 Wire Security Seal Compromise (M100 Tabulator)

The wire seal on the front panel of an M100 Tabulator can be bypassed. The wire security seals tested by the Red Team were provided by ES&S. If a seal is not tightened correctly, an attacker can bypass the seal on the front access panel of the M100 providing a vector of attack on the PCMCIA cards (see sections 3.1 and 3.2).

3.15 Paper Security Seal Compromise (Voter Assist Terminal and M650 Tabulator)

The Voter Assist Terminal (VAT) and M650 Tabulator incorporate several paper seals whose damage or removal would indicate tampering. The Red Team used commonly available products to remove the paper seals affixed to the machine cases. It was difficult to remove the paper seals, supplied by ES&S, without damaging them and triggering the paper seal voiding mechanism. However, it was possible to cleanly remove the paper seals on the VAT and M650 back panel.

4. Unsuccessful Exploits

4.1 Vote Count Tampering (M100 Tabulator)

The Red Team attempted several attacks intended to modify the election results recorded by the M100 Tabulator. The security mechanism on the digital media was resistant to attack -- every attempt at directly modifying the data failed.

4.2 Remote Access (AutoMARK Information Management System and Unity Election Management System)

The Red Team performed network scans on the AutoMARK Information Management and Unity Election Management Systems to discover open ports and exposed services. However, the Red Team established that the ports and the corresponding services posed no risk.

4.3 Access to Voter Assist Terminal Operating System

The Red Team attempted to gain access to the operating system on the AutoMARK Voter Assist Terminal (VAT) by crashing the user-interface used to facilitate ballot marking. This testing proved unsuccessful.

4.4 Media Compromise (AutoMARK Information Management System)

The Red Team made several attempts to compromise the Voter Assist Terminal (VAT) configuration data stored on digital media. However, all the attempts failed.

4.5 Password Compromise (AutoMARK Information Management System)

The Red Team had great difficulty determining the password for the AutoMARK Information Management System. The password is very well-hidden and would take potential attackers a considerable amount of time to locate, if ever.

5. Conclusions

The Red Team identified several vulnerabilities, devised fifteen exploits and performed these exploits which compromised voting system accuracy and integrity. Some of the more serious exploits include ballot box stuffing, election result modification and unauthorized access to vital voting system components.

The ES&S Voting System has complex hardware and software components. It is almost certain to have additional undiscovered vulnerabilities that would make it susceptible to other attacks. Many of the identified vulnerabilities can be partially mitigated by adopting various security policies and procedures. However, some of the vulnerabilities are due to system design and may, therefore, require hardware and/or software upgrades or re-design. Addressing the vulnerabilities described in this document will enable the voting system to better satisfy the important security goals of accuracy, integrity and confidentiality.