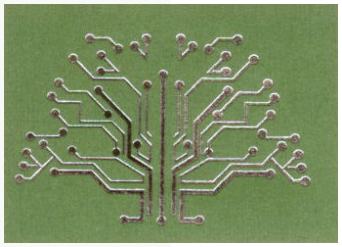


FREEMAN, CRAFT, MCGREGOR GROUP

Red Team Testing Report
Dominion Democracy Suite 4.14-A and Dominion Democracy Suite 4.14.A.1 w/ Adjudication 2.4

Author:
Jacob Stauffer, CISSP
Freeman, Craft, McGregor Group

Contributors:
Louis Losee
Steve Weingart, CISA
atsec information security

November 18, 2014

Table of Contents

Executive Summary

On February 10, 2014, three members contracted by the Freeman, Craft, and McGregor Group, Inc. (FCMG) executed a computer and network penetration test, commonly referred to as a "Red Team" evaluation, on the ***Dominion Democracy Suite version 4.14-A Voting System.*** Over the course of five days, the team evaluated the physical, computer, and communications security of each system within the Democracy Suite.

In response to the initial findings, the developers of the system made configuration changes to the system and built a new version of a system component. Supplemental evaluation was required to assess the effectiveness of changes and to test the new component.

On October 11, 2014, one member from the Freeman, Craft, and McGregor Group, Inc. executed a second computer and network penetration test on the new version of the system, ***Dominion Democracy Suite version 4.14.A.1 Voting System,*** including the new version of the component, ***Adjudication 2.4 (Democracy Suite version 4.14.A.1 with Adjudication version 2.4 Voting System).***

This report includes both rounds of testing. Methods used to complete this evaluation include but are not limited to:

- Attempts to compromise physical security controls
- Automated and manual computer and network vulnerability assessments
- Analysis of hardening procedures and scripts
- System memory (i.e. RAM) analysis
- Decompiling and reusing source code from installed Democracy Suite programs
- Logging in, viewing, and modifying centralized election database

During the testing in February, the physical security team evaluated all seals, stickers, and locks used to verify the integrity of the systems and ballot boxes. Furthermore, evaluators attempted to compromise hardware security controls on the ballot box in efforts to remove or add ballots to the system, creating a discrepancy between the physical and electronic records. At the end of the evaluation it was determined that most plastic "lock-type" seals could easily be compromised while the "tie-wrap" and "security stickers" provided adequate integrity validation if properly used. It was also determined that if an attacker had a key or lock-pick set, they could unlock the front of the ballot scanner box, lift up the top cover, and place false ballots into the box unbeknownst to a poll worker.

The scope of the computer and communications security evaluation was to find flaws in software-based controls (e.g. system hardening processes, weak credentials), enumerate vulnerabilities in the system, and provide proof of concept exploits for discovered vulnerabilities. At the end of the evaluation in February, team members reported security concerns with the Democracy Suite's Windows-based programs developed under the

Microsoft .NET framework. Testing led to the complete decompiling of Democracy Suite executables back into their original source code (with developer comments), extraction of vital information (e.g. encryption keys), and the reuse of Democracy Suite code to develop a custom user credential decryption tool. At this point, evaluators were able to login to the centralized election database, view the election definitions, and change the outcome of the election.

Using the findings from the February 2014 evaluation, the scope of the testing in October 2014 was to validate security hardening of the Democracy Suite binaries that could be easily decompiled into its original source code. Additional testing was conducted to verify the removal of all user credentials, passwords, keys, etc. from system memory that may be used by the Democracy Suite. Finally, an evaluation of the new Adjudication module version 2.4 was conducted.

Within the October testing period, the FCMG member validated that an obfuscation technique was used to harden function and variable names within the "EMS Application Server" application. While some source code structures were recovered during the de-compilation process, the content of the functions were not readable. Furthermore, an evaluation of the EMS workstation and server memory determined that plain-text encryption keys were protected, but plain-text user credentials (i.e. usernames and passwords) still resided in memory. This test was based off a precompiled wordlist of usernames, passwords, and hard-coded encryption keys found in the source code of the EMS Application Server.

The October testing found that while some vulnerabilities were addressed, multiple critical vulnerabilities were not addressed in the various systems and subsystems within the Democracy Suite. This included remote code execution and denial of service vulnerabilities as well as off-line ballot tampering.

The following report is a comprehensive list of all findings discovered by the Red Team during the evaluations conducted in Sacramento, California.

Introduction

The California Secretary of State's Office of Voting Systems Technology Assessment (OVSTA) contracted with the Freeman, Craft, and McGregor Group, Inc. (FCMG) to perform a computer/network penetration test, commonly referred to as a "Red Team evaluation," on the ***Dominion Voting Systems (DVS): Democracy Suite (DemSuite) version 4.14-A Voting System***. The scope of the evaluation was to gain access to the system in efforts to deceive, deny, degrade, disrupt, or destroy a target election. This evaluation was conducted in February 2014. Systems within the scope of this evaluation included:

- Election Management System (EMS) Server
- Election Management System (EMS) Workstation
- ImageCast Central (ICC) Workstation
- ImageCast Evolution (ICE) Ballot Scanner and Ballot Box

A second round of testing was ordered on a revision to the system, ***Dominion Voting Systems: Democracy Suite version 4.14.A.1 with Adjudication version 2.4 Voting System***. This revision included a new version of the Adjudication module and the use of an obfuscation technique to harden the system against attempts to decompile executables back into their original source code. This evaluation was conducted in October 2014. Systems within the scope of this evaluation included:

- Election Management System (EMS) Server
- Election Management System (EMS) Workstation 1 and 2
- ImageCast Central (ICC) Workstation

The following is a report of all findings discovered by the "Red Team" during the evaluations. Findings are divided into three categories: initial observations, physical security, and computer/communications security.

Systems Evaluated in February 2014

The following systems were subjects of the Red Team evaluation during the onsite review between February 10-14, 2014. Items that are different from those examined in October 2014 are marked with an asterisk "*". Items that have changed solely due to the newly obfuscated build are marked with two asterisks "**".

System Name:	EMS Server
Hardware Manufacturer:	Dell Inc. PowerEdge T620 (SN: **GG85FX1**)
System Specifications:	2.0 GHz Intel Xeon E5-2620 8 GB of RAM 2 x 500 GB Hard Drive in RAID 1 configuration (mirror)

Operating System:	Windows Server 2008 R2 Standard x64 Service Pack 1
Evaluated Software:	DVS Adjudication System Version 1.0.14.17601* EMSApplicationServerManager Version 4.14.23.0 ** EMSAuditModule Version 1.0.0.0
Additional Software:	avast! Antivirus Version 8.0.1603.399 Cepstral, LLC CepstralLicSrv Version 4, 2, 0, 0 Cepstral - SwiftTalker Version 4, 2, 0, 0 Microsoft Internet Explorer Version 8.00.7600.16385 Microsoft SQL Server Version 10.0.2531.0 Microsoft SQL Server Version 10.50.4000.0 Microsoft Visual Studio 2008 Version 9.0.30729.4462 Java Platform SE 6 U29 Version 6.0.290.11

System Name:	**EMS Server Backup**
Hardware Manufacturer:	Rocstor Guardian 4RM (SN: **SB10080060**)
System Specifications:	1U Rack mounted Server 4 x 500 GB Hard Drives eSATA connection to EMS Server USB dongle containing encryption key
Operating System:	Unknown

System Name:	**EMS Workstation**
Hardware Manufacturer:	Dell Inc. Latitude E6530 01 (SN: **8QD9CW1**) *
System Specifications:	2.50 GHz Intel Core i5-3210M 4 GB of RAM * 500 GB Hard Drive
Operating System:	Windows 7 Professional x64 Service Pack 1
Evaluated Software:	DVS Adjudication System Version 1.0.14.17603* DVS.DemocracySuite.ElectionEventDesigner Version 4.14.23.0 ** DVS.DemocracySuite.ResultTally Version 4.14.23.0 ** EMSAudioStudio2010 Version 4.14.23.0 ** FileSystemService Version 4.14.23.0 ** ImportAdapter Version 4.14.23.0 **
Additional Software:	avast! Antivirus Version 9.0.2013.292 * Kofax - VCDEMO32 Application Version 4.50.032 * Kofax Image Products - Scanner Configuration Utility Version 4.50.32.0 *

System Name:	ICC Workstation
Hardware Manufacturer:	Dell Inc. OptiPlex 9010 AIO 01 (SN: **7X1WDX1**)
System Specifications:	3.30 GHz Intel Core i3-3220 4 GB of RAM 500 GB Hard Drive
Operating System:	Windows 7 Professional x64 Service Pack 1
Evaluated Software:	ImageCast Central Version 4.14.4
Additional Software:	Adobe Systems - Reader Version 10.1.1.33 * avast! Antivirus Version 9.0.2013.292 * IDT - PC Audio Version 1.0.6388.0 * Maxim Integrated Products - Default 1-Wire Version 1.0.0.1 * Maxim Integrated Products - OneWireViewer_x64 Version 0.3.15.50 * Microsoft - Internet Explorer Version 8.00.7600.16385 SafeNet - Sentinel Keys Version 1, 0, 3, 0 SafeNet - SPI Version 7, 4, 0, 0

System Name:	ICE Scanner and Ballot Box
Hardware Manufacturer:	ICE Scanner (SN: **AAFEBDW0062**) * DVS Ballot Box (SN: **AAUCBDY0013**) *
System Specifications:	8 GB Compact Flash Card as CF0 (Operating System) * 8 GB Compact Flash Card as CF1 (Ballot Definition and Count) * 8 GB Compact Flash Card as CF2 (Backup for CF1) *
Operating System:	Unknown Linux Operating System *

Systems Evaluated in October 2014

The following systems were subjects of the Red Team evaluation during the onsite review on October 11 and 12, 2014. Items that are different from those examined in October 2014 are marked with an asterisk "*". Items that have changed solely due to the newly obfuscated build are marked with two asterisks "**". EMS Workstation2 is marked with the superscripted pound sign"#" because it was a new computer that was added specifically for the new version of Adjudication and was not part of the February testing.

System Name:	EMS Server
Hardware Manufacturer:	Dell Inc. PowerEdge T620 (SN: **GG85FX1**)
System Specifications:	2.0 GHz Intel Xeon E5-2620 8 GB of RAM 2 x 500 GB Hard Drive in RAID 1 configuration (mirror)
Operating System:	Windows Server 2008 R2 Standard x64 Service Pack 1
Server Roles:	Application Server Web Server (IIS) File Services DHCP Server DNS Server
Evaluated Software:	DVS Adjudication System Version 4.14.37* DVS Adjudication Services Reports 2.4.1.3201* DVS Adjudication Client 2.4.1.3201* EMSApplicationServerManager Version 4.14.2301.0 ** EMSAuditModule Version 1.0.0.0
Additional Software:	avast! Antivirus Version 8.0.1603.399 Cepstral, LLC CepstralLicSrv Version 4, 2, 0, 0 Cepstral - SwiftTalker Version 4, 2, 0, 0 Microsoft Internet Explorer Version 8.00.7600.16385 Microsoft SQL Server Version 10.0.2531.0 Microsoft SQL Server Version 10.50.4000.0 Microsoft Visual Studio 2008 Version 9.0.30729.4462 Java Platform SE 6 U29 Version 6.0.290.11

System Name:	EMS Server Backup
Hardware Manufacturer:	Rocstor Guardian 4RM (SN: **SB10080060**)
System Specifications:	1U Rack mounted Server 4 x 500 GB Hard Drives eSATA connection to EMS Server USB dongle containing encryption key
Operating System:	Unknown

System Name:	EMS Workstation1 *
Hardware Manufacturer:	Dell Inc. Latitude E6530 01 (SN: **CX69CW1**) *
System Specifications:	2.50 GHz Intel Core i5-3210M 8 GB of RAM * 500 GB Hard Drive

Operating System:	Windows 7 Professional x64 Service Pack 1
Evaluated Software:	DVS Adjudication System Version 4.14.37* DVS.DemocracySuite.ElectionEventDesigner Version 4.14.2301.0 ** DVS.DemocracySuite.ResultTally Version 4.14.2301.0 ** DVS Adjudication Client 2.4.1.3201 * EMSAudioStudio2010 Version 4.14.2301.0 ** FileSystemService Version 4.14.2301.0 ** ImportAdapter Version 4.14.2301.0 **
Additional Software:	avast! Antivirus Version 9.0.2021.515 *

System Name:	**EMS Workstation2 #**
Hardware Manufacturer:	Dell Inc. Latitude E6420 01 (SN: **FH32HV1**) *
System Specifications:	2.50 GHz Intel Core i5-2520M * 8 GB of RAM * 1 TB Hard Drive *
Operating System:	Windows 7 Professional x64 Service Pack 1
Evaluated Software:	DVS Adjudication System Version 4.14.37* DVS.DemocracySuite.ElectionEventDesigner Version 4.14.2301.0 ** DVS.DemocracySuite.ResultTally Version 4.14.2301.0 ** DVS Adjudication Client 2.4.1.3201 * EMSAudioStudio2010 Version 4.14.2301.0 ** FileSystemService Version 4.14.2301.0 ** ImportAdapter Version 4.14.2301.0 **
Additional Software:	avast! Antivirus Version 9.0.2021.515 *

System Name:	**ICC Workstation**
Hardware Manufacturer:	Dell Inc. OptiPlex 9010 AIO 01 (SN: **7X1WDX1**)
System Specifications:	3.30 GHz Intel Core i3-3220 4 GB of RAM 500 GB Hard Drive
Operating System:	Windows 7 Professional x64 Service Pack 1
Evaluated Software:	ImageCast Central Version 4.14.4
Additional Software:	avast! Antivirus Version 9.0.2021.515 * Microsoft - Internet Explorer Version 8.00.7600.16385 SafeNet - Sentinel Keys Version 1, 0, 3, 0 SafeNet - SPI Version 7, 4, 0, 0

Considerations and Assumptions

Upon entering into the evaluation, the Red Team assumed that the systems would be configured as it would be at a central count or voting facility. This configuration would include: all computer and networking hardware in proper working order, all proper software installed, updated, security hardened to Dominion's documented specifications, systems properly connected to a secured network, and all proper security controls in place.

February 2014 Initial Observations

Red Team members spent the first two days of the evaluation with Dominion and OVSTA personnel to become familiarized with the Democracy Suite Voting System. This time was spent reviewing system specifications, configurations, and running a simulated election through the system. The following are initial observations of the system:

Hardware Failure (EMS Server)

Two sets of system components designated "Functional Test" and "Red Team" were acquired and configured, according to Dominion specifications, for the complete OVSTA evaluation. The "Red Team" components, understood to be exact copies of the "Functional Test" components, were specifically designated for all computer and network penetration testing operations while the team was on site.

On the first day of the evaluation, the EMS Server experienced a hardware failure with the storage array, more specifically the Dell RAID[1] hardware. This system was configured in a RAID 1 specification that writes all data to a primary hard drive and a copy to a secondary drive (of equal size) for redundancy. Upon initial startup, team members noted the system was not booting into the operating system and was extremely slow in response. Hard drives from the "Red Team" system were removed and installed into the "Functional Test" hardware with the same hardware specifications. System booted directly into the operating system with no issues.

On the fourth and final day of the evaluation the EMS workstation experienced a catastrophic hardware failure in the onboard network interface. From the factory, the Dell PowerEdge T620 has two onboard network interface ports to facilitate inter-network connectivity. During the evaluation of the DVS Adjudication Software version 1.0, team members began receiving multiple errors not seen earlier in the week. It was later determined that both network interfaces had failed on the system which led to the errors. This failure resulted in ceasing all future evaluation of the EMS Server since network connectivity was a vital part of its functionality.

[1] RAID - Redundant Array of Inexpensive Disks

Administrator Credentials (EMS Server)

By default, the user that logs into the EMS Server to oversee election operations is a system administrator. System administrators and election operation officials should have separation of privileges.

No Display Timeout and Lock Configuration (All Systems)

DVS system developers implemented multiple Windows Group Policies throughout each system in efforts to harden server and workstation security. One configuration that was not present was the timing out of an inactive user session (enabling the screen saver) and locking the system, forcing the user to re-enter their credential to resume their session.

No Centralized GPO Configuration Management

While Windows Group Policy Objects (GPO) were deployed throughout the entire Democracy Suite Voting System, no centralized management was found during the evaluation. This would imply that system hardening through GPO's is a manual process that must be repeated on each component within the Democracy Suite system. A manual process allows the opportunity for missed steps, GPO's, configurations, etc. Most enterprise networks deploying Windows servers and workstations utilize a "domain" architecture with a centralized set of GPO's. All systems joined to the domain install the initial set of GPO's and receive periodic policy updates when applicable. While a "domain" architecture may not be suitable for one or two systems within a network, it would be significantly beneficial in networks containing multiple servers and 10-1000 workstations.

Furthermore a "domain" architecture would allow centralized user management, granular role separation, and proper auditing depending on the security requirements that govern the system.

Missing Windows Updates

As stated in the Considerations and Assumptions section of this report, on arrival the evaluation team considered all systems as properly configured and updated. The following systems had a number of missing Windows and application updates. Note that the ICE system is an embedded Linux system and could not be audited with the software available to the Red Team.

System	Missing Updates[2] February 2014	Missing Updates October 2014
EMS Server	Critical: **27** Important: **49** Moderate: **8** Low: **3**	Critical: **22** Important: **59** Moderate: **9** Low: **4**
EMS Workstation	Critical: **39** Important: **50** Moderate: **3** Low: **1**	N/A
EMS Workstation 1	N/A	Critical: **20** Important: **42** Moderate: **1** Low: **1**
EMS Workstation 2	N/A	Critical: **20** Important: **42** Moderate: **1** Low: **1**
ICC Workstation	Critical: **34** Important: **41** Moderate: **2** Low: **1**	Critical: **16** Important: **31** Moderate: **0** Low: **1**

Anti-virus in "Evaluation Mode"

While all systems within the Democracy Suite had avast! anti-virus software[3] installed, each system's anti-virus software was in "evaluation mode." This implies that after an evaluation period, set by the anti-virus vendor, the system would no longer be protected to include up-to-date signatures.

Election Data Translator Application is Quarantined by Anti-Virus

In the October 2014 testing, during the execution of the DVS Election Data Translation (EDT) application on the EMS Workstation, avast! anti-virus quarantines the "DVS.Bridging.ImportAdapter.exe" file located in *%ProgramFiles%\Dominion Voting Systems\Election Data Translator* directory. Avast! classifies the threat as "Win32:Evo-gen."

[2] Microsoft Security Bulletin Severity Rating System - http://technet.microsoft.com/en-us/security/gg309177.aspx

[3] Avast Anti-virus – http://www.avast.com

Findings (Physical Security)

The following constitutes all findings regarding the physical security of all devices within the scope of the evaluation. Integrity devices such as physical seals and stickers where also included within the scope.

Stickers and Seals

There were four types of security seals used by the Dominion Voting system and evaluated by the Red Team. These included: a tamper evident adhesive sticker marked "SECURITY SEAL," a lock type plastic seal, hinged-lock type plastic seal, and the tie wrap type seal.

Tamper Evident Adhesive Sticker

This sticker seal is placed over sections of the ICE ballot box, ICC Workstation, and EMS Workstation to ensure the integrity of the ballot box contents and visibly show signs of tampering if attempts are made to compromise the system or ballots within the ballot box.

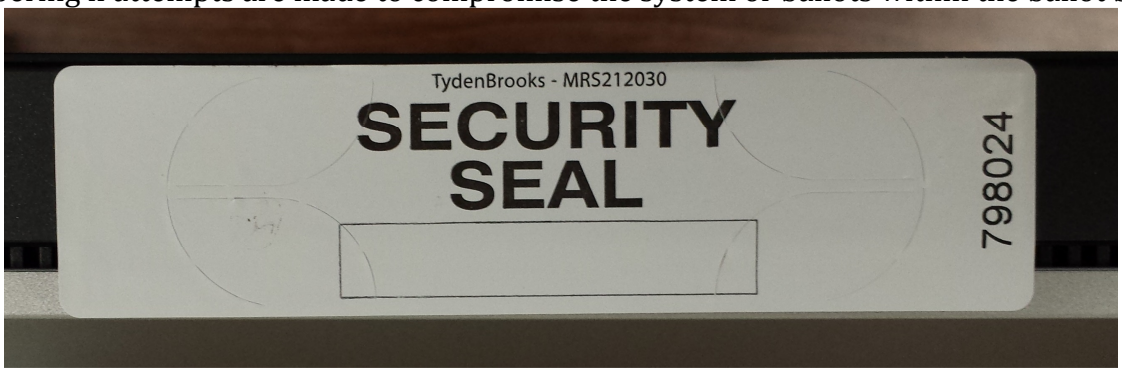


Figure 1 - Tamper Evident Adhesive Sticker Sample

This sticker seal has a very aggressive adhesive and is scored to promote tearing if removal is attempted. It is also serialized to assist protection via replacement. Please see Figure 1.

The security sticker was tested using the most effective current technique known to the tester. In Figure 2, the damage to the printing can be seen as well as that the right edge has been lifted.

There was no fault found with this seal. However it is noted that the ICC workstation only had one seal at the top edge of the case and could be hinged open without displacing or damaging the seal.

Figure 2 - Damaged Sticker

Lock Type Plastic Seals.

These plastic seals were used to seal doors and hinges that would allow access to vital parts of the ICE ballot scanner like the Compact Flash compartment that contains ballot definitions and tally results. They are to be installed once, and should break if removed.

These seals were found vulnerable to tampering without leaving evidence.

Figure 3 - Lock Type Seal Sample

Hinged-Lock Type Plastic Seals.

As observed by the Red Team, these plastic seals were used to verify the integrity of the ICE ballot scanner with the system cover installed. This is to ensure system integrity during storage. These seals are similar to the lock seals above, but use a slightly different mechanism. They also use a one-way 'click' insertion, but these use round pins rather than flat pins.

Figure 4 - Hinged-Lock Type Seal Sample

The end of the seal is plugged with a hard resin type substance to prevent pushing the plunger through the back of the lock type seal (See Figure 5). These seals were found vulnerable to tampering without leaving easily observable evidence.

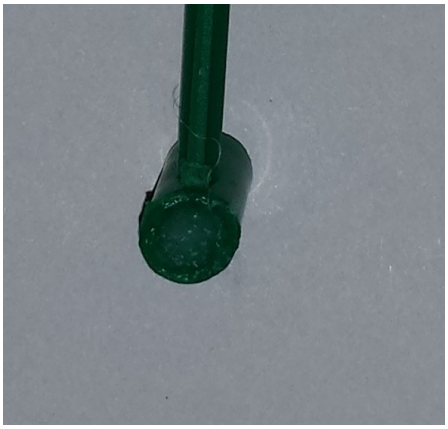


Figure 5 - Plugged End of Hinge-Lock Type Seal

Figure 6 - Broken Hinge-Lock Type Seal

Tie Wrap Type Seal

This seal works by inserting a round plastic strand through a hole in the base, which has metal teeth to prevent removal.

Figure 7 - Tie Wrap Type Seal Sample

This seal is safe and could not be defeated by the tester if it was pulled tight such that the back of the lock is pulled tightly against the sealed item.

Voting System Hardware

The following are findings regarding the physical security of the Democracy Suite system hardware.

EMS Server, EMS workstation and ICC Workstation

Each of the computers is based on common off-the-shelf computer systems as described in the "Systems Evaluated" section of this report.

Tamper evidence is provided by use of the "tamper evident adhesive sticker" seals described above. If a sufficient number of stickers are used to prevent "hinging" a cover away from the case, there is little possibility of opening the case undetected.

The EMS Server tested was not sealed at all, the EMS workstation was sufficiently sealed and the ICC workstation had only one seal so that the maintenance panel could be hinged out on the sticker without damaging it.

ICE Ballot Scanner

The ICE ballot scanner is a multi-purpose device that performs both ballot scanning and ballot marking for voters with disabilities. Please see Figures 8, 9 and 10 for pictures of the overall system.

Figure 8 - ICE Ballot Scanner - Package for Transport and Storage

Figure 9 - ICE Ballot Scanner - Transport / Storage Cover Removed

Figure 10 - ICE Ballot Scanner, Screen, and Privacy Shield in Place for Voting

The Ballot Scanner consists of three major assemblies:

1. The ballot box (see the lighter appearing grey seam just below the two light grey handles in Figure 10 at the top of the box)
2. The ballot box top (the approximately 3" thick slab on top of the ballot box in Figure 10)
3. The scanner/computer/display section, which sits on the ballot box top.

The ballot scanner is normally shipped with the top cover in place and sealed (see Figure 8). When put into service the cover is removed, the display is raised and a privacy shield is unfolded around the display screen (see Figure 10).

If the accessibility feature is to be used to assist voters with disabilities, then the accessible tactile interface is removed from its storage cradle and plugged into the computer for use. See Figure 10 at the upper right corner for the small box on the ballot box top with the red, yellow, and blue inputs.

The ballot box has a sliding door (the large light grey panel on the ballot box, see Figure 10) that has a lock and an electronic opening detection switch. Besides the serialized tamper-evident seals that are placed on the ballot box by the election officials, there are no specific detection mechanisms to detect if the ballot box top is in place or sealed.

The ballot scanner/computer has a number of opening doors and panels. Most of them have electronic opening detection switches and hasps for seals. See Figures 11 – 13.

Figure 4 - ICE Scanner Compact Flash Door Seals in Place

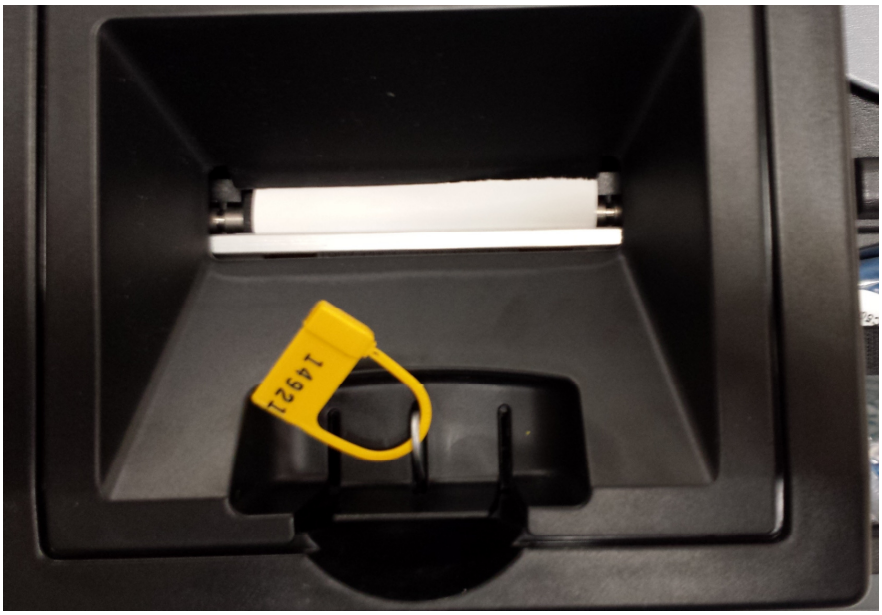


Figure 5 - ICE Scanner Thermal Printer Door Seal in Place

Figure 6 - ICE Scanner Ballot Marking Printer Door Seal in Place

The ballot box top is locked to the ballot box with a lock at each end of the box. The lock can be seen near the yellow dot on the ballot box in Figure 9.

The ICE ballot scanner was examined for vulnerabilities and the following items were determined:

- As stated previously, all of the lock and hinged lock type seals are vulnerable to tampering without leaving evidence, this means that the shipping cover can be easily removed and replaced without leaving evidence.

Once the cover is removed there are several attacks that can be mounted successfully.

- The Compact Flash Drive door covers can be opened once the seals have been removed and there is a potential attack on CF1 & CF2 (the voting definition and voting backup disks).

  There are recessed cover switches that audit the opening of the CF doors. Figure 11 shows the doors closed and sealed.

  The Red Team designed an attack which would allow the door covers to be opened without being audited. This attack was not performed to avoid damaging the ICE computer. This technique was discussed with Dominion Voting representatives and they agreed that the attack was feasible and would likely succeed.

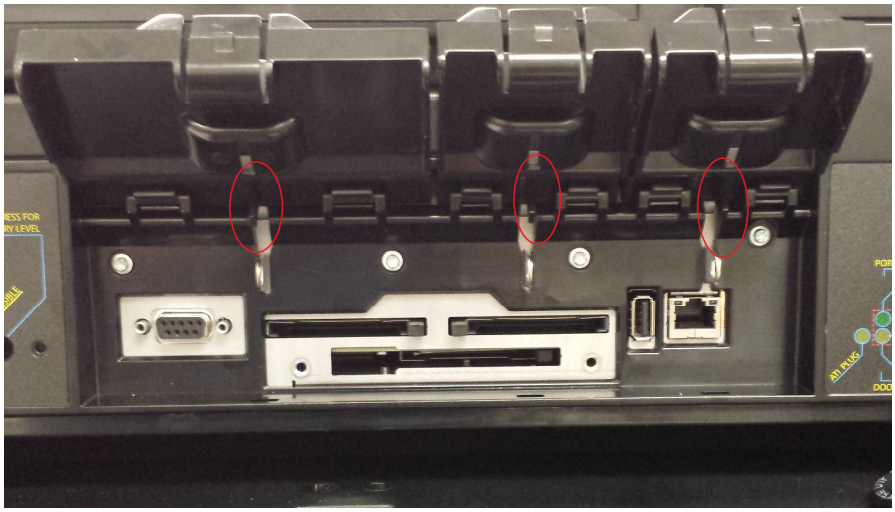


Figure 14 - Door Closure Tabs

- The ballot box may be opened during an election and ballots added or removed without detection.

  The ballot box is closed and attached to the ballot box top with only two locks. If someone with the key or lock pick opens the front lock, a large entry path can be opened. See Figure 15 for the front access.

Figure 15 - Ballot Box Open from the Front

A similar attack is feasible at the rear of the system. It takes an extra step, but also disables the switch that detects opening of the main ballot box sliding door.

The wire that connects the computer to the ballot box door switch runs through the auxiliary bin of the ballot box and is subject to tampering by individuals who have the key or can pick the lock on the auxiliary bin door. See Figure 16 for the view of the wire. The wire is traced in red in the picture.

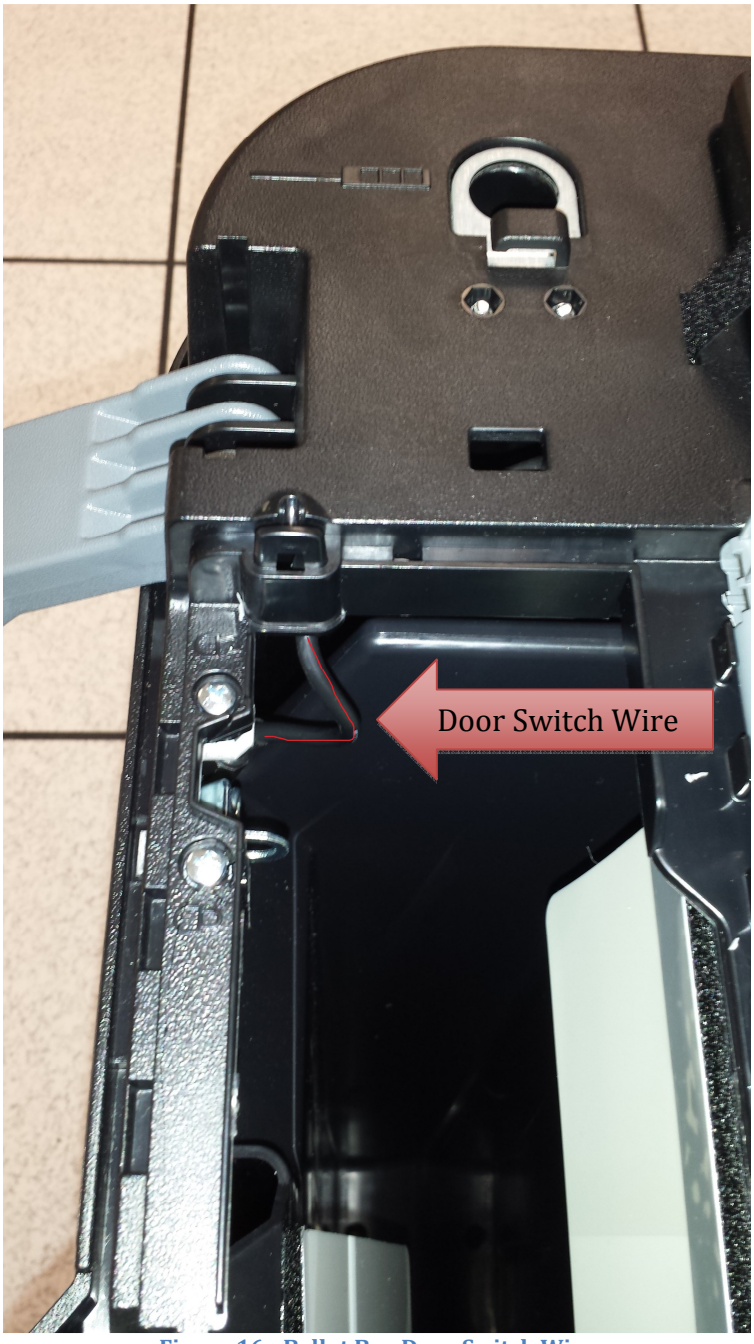


Figure 16 - Ballot Box Door Switch Wire

If the wire is tampered, it can be configured such that the switch that detects ballot box opening is rendered undetected. This will also allow the rear of the ballot box to

be lifted, or the main ballot box door can be opened if the key is available or the lock is picked.

NOTE: This attack was not performed to avoid damaging the ICE computer. This technique is simple and was discussed with Dominion Voting representatives and they agreed that the attack was feasible and would succeed.

- The main On/Off switch can be switched even when the door that covers it is closed and sealed. The main power switch is in the compartment with the thermal printer as shown in Figure 17. This will permit draining the battery if the unit is not plugged in and it is turned on. The machine can be taken out of service if the switch is turned off while it is running (the battery will not backup the system, this is the main switch).

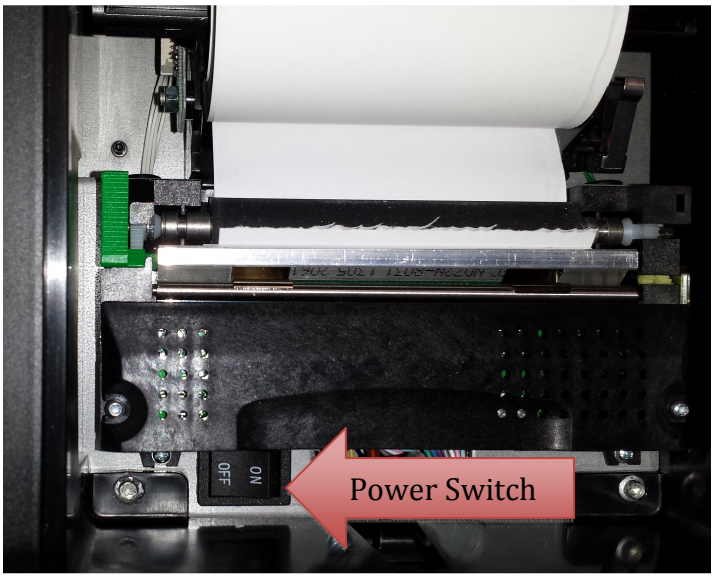


Figure 17 - Main Power Switch

Findings (Computer and Communications Security)

The following constitutes all findings regarding computer and communication security that could have a significant impact on information assurance.

Binaries Can Be Converted Into Original Source Code (All Windows Systems)

Upon examination of the DemSuite software installed on each of the Windows based systems, it was discovered that each binary (executable) was developed in Microsoft C# under the .NET[4] framework. This discovery allowed the Red Team to easily decompile all

[4] Pronounced "dot net"

target binaries into its original source code, to include most developer comments, and recover vital information like software configurations and hard coded encryption keys.

These decrypted credentials were later used from an evaluator's workstation to gain access to the EMS Server's SQL database. At that point the evaluator was able to view the database schema, which included current election definitions and tallied results, and modify fields within the database, to include fields (e.g. candidate information and vote tallies) within the test election.

UPDATE From October 2014 Testing: Obfuscation Technique Used on DemSuite Binaries

As described above, during the February 2014 evaluation, the Red Team was able to decompile the executable files and DLL's back into its original source code. In the 4.14.2301.0 version of the EMS Application Server Manager an obfuscation technique was used to rename variables and function calls to names with random hexadecimal characters. While some of the source code structure, like function call names, were recovered; the actual functionality (local variable instantiation, function calls, other algorithms) of the function call could not be recovered.

It should be noted that the original encryption keys found in the first evaluation continue to remain un-obfuscated.

Zero Trust Relationship Between EMS Server and Workstations

On examining the communications between the EMS Server and the Workstation, it was determined that no "trust relationship" exists between the systems. Trust relationships are predetermined parameters a system must meet prior to accessing resources on a network. In a Microsoft enterprise environment, this is usually established using domains.

This lack of a trust relationship allowed an evaluator to access the SQL database, located on the EMS Server, from an untrusted system resulting in the modification of the test election.

Encryption Keys Recovered From Memory (EMS Server and Workstation)

The evaluation team parsed through all human readable "strings" within the system memory of the EMS Server and Workstation. In the process of searching for possible encryption keys, the team noticed a 128-bit value that was consistent across both machines. After examining the memory spaces near this 128-bit value, keywords were discovered in plain-text. It was later determined that these keywords are used in the encryption process of both the Server and Workstation. These keywords were also found after decompiling the EMS Server's "Application Server Manager" binary and analyzing the cryptography library.

Now this does not prove that the implemented cipher is insecure, only the methods of which the user provided information; in this case the hard coded password is used to

derive the encryption key. No attempts to obfuscate or protect the password were taken by the programs cryptography library.

UPDATE From October 2014 Testing: No plain-text encryption keys found in memory

As described above, during the February 2014 evaluation, the plain-text strings were found in the EMS Server's system memory. While these strings were also recovered in the decompiling process outlined previously in this report, they were not present in memory of the EMS Server version 4.14.A.1. This presents the conclusion that either the keys are contained in a secure key-store within memory, or the keys have changed unbeknownst to the evaluation team.

User Credentials Recovered From Memory (EMS Server and Workstation)

During an investigation of human readable strings within system memory of the EMS Server, it was discovered that plain-text credentials used to login to the DemSuite software and into the SQL database were in the Unicode strings. If an attacker had physical or network access to the system and was able to dump the system's physical memory, they would be able to recover usernames and passwords to log into specific DemSuite software and the MS SQL database.

MS11-030 Vulnerability in DNS Resolution (EMS Server)

A vulnerability within the Windows DNS Server was discovered while auditing the network ports and protocols of the EMS Server. This vulnerability is known by Microsoft and referred to as "MS11-030[5]: Vulnerability in DNS Resolution Could Allow Remote Code Execution." Attempts by the evaluation team were made to crash the service and gain access to the system; however, all were unsuccessful.

UPDATE From October 2014 Testing: Vulnerability in DNS Resolution (EMS Server)

The MS11-030 vulnerability was not present in the 4.14.A.1 version during the October testing. However, a new vulnerability, the "*MS11-058[6]: Vulnerability in DNS Server Could Allow Remote Code Execution"* was discovered. Microsoft currently rates this vulnerability as "critical".

SafeNet Directory Transversal Vulnerability (ICC Workstation)

A vulnerability within the SafeNet Sentinel Keys License Monitor web console (version 1.0) was discovered while auditing the network ports and protocols of the ICC Workstation. This program resided on a port that is commonly used to manage licenses that reside in hardware. This vulnerability allowed a remote user to traverse system directories without authenticating to the system, and display contents of files directly to the browser.

---

[5] Microsoft Security Bulletin MS11-030 (Critical) - http://technet.microsoft.com/en-us/security/bulletin/ms11-030

[6] Microsoft Security Bulleting MS11-058 (Critical) - https://technet.microsoft.com/en-us/library/security/ms11-058.aspx

For this evaluation, a Red Team member connected to the ICC workstation on the port and using the directory traversal vulnerability was able to view the Windows Update Log.

Election Definition Modification (EMS Server and Workstation)

The EMS Workstation (amongst other functionality) is used to load election definitions by communicating with the EMS Server over an Ethernet network. The EMS Server then stores the election definitions into a MS SQL Server database.

Election definitions (definitions) were loaded via the EMS Workstation from a USB device containing the definitions. The definitions were contained in a single zip file (in this case "Red Team Trilingual Election-2014-01-29-15-20-34_package.zip") that contained two files; a high level directory and a file containing a SHA hash value.

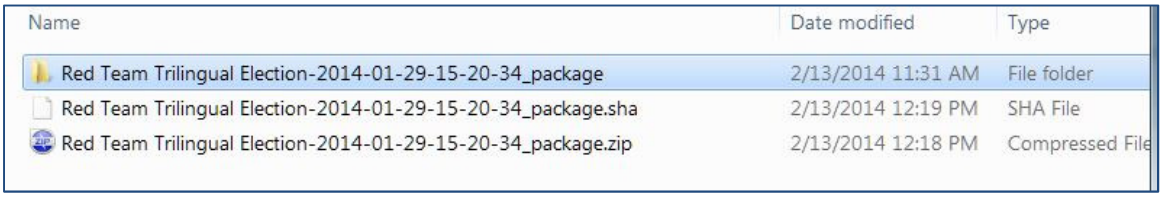


Figure 7 – Election package content listing

It was determined that the SHA value in the .sha file was a SHA-256 hash of the uncompressed contents of the "<ELECTION NAME>_package" folder.
The "DB\Backup\" folder contains a file, "PackageInfo.xml" which contains general information regarding the election definition.

Values in this file were altered using a standard editor. The file "PackageInfo.xml" was altered:

The SHA-256 hash value of the altered contents of the "package" folder was recomputed and inserted into the .sha file and then a .zip of the folder and the .sha file was created. This altered zip file was used to create a new election. The EMS Workstation was later used to retrieve and view the election definitions from the EMS Server with the altered values.

Hardening Script Found and Unprotected on System (All Windows Systems)

Dominion documentation, regarding system setup, neither specifies that the hardening scripts should be deleted after their execution, nor mentions requirements to protect them from being viewed by a typical user.

With no access control method in place on this file structure, any user is able to determine what steps were taken to harden the system.

With knowledge of how the system is secured, the attacker can now quickly develop tactics, techniques and procedures to work around these controls or possibly target a specific configuration and change it to a less secure setting, unbeknownst to the user, depending on access of the attacker (e.g. administrator access).

UPDATE From October 2104 Testing: No Hardening Scripts Found

As described above, during the February 2014 evaluation, system security hardening scripts were discovered on the EMS Server, EMS Workstation, and the ICC Workstation. These scripts were not present during the October 2014 evaluation.

DVS Adjudication 2.4 Network Traffic Evaluation

Network traffic was captured during the use of the DVS Adjudication 2.4 software to test the confidentiality and integrity of data (i.e. ballot images) moving across the following systems:

- EMS Workstation to EMS Server
- ICC Workstation to EMS Server

Traffic captured between the EMS Workstation to the EMS Server revealed combined IPv4 and IPv6 traffic as well the use of the SOAP[7] protocol to transfer data between systems. While industry network encryption standards like SSL or TLS were not apparent, no plain-text usernames or password or recoverable files were found. Furthermore, with the appearance of various public-key cryptography certificates, it is assumed that all data is encrypted and verified by the target DVS application prior to its transmission over the network. This would need to be verified by a source-code evaluation.

Traffic captured between the ICC Workstation to the EMS Server revealed the use of the Microsoft file-sharing protocol commonly referred to "*Server Message Block*" or "*SMB*[8]." Analysis of the SMB traffic revealed that a remote user could recover full images of voter ballots as well as the "Detail," "Raw", and "Totals" DVD files directly from the traffic. Furthermore, the remote user can recover usernames and directory paths of the target files within the traffic. In theory, a remote attacker could recover these files from the network, modify them, and replay the network session with the modified data. This theory was not tested or verified during the October 2014 evaluation. A sample of a recovered ballot is in Appendix A of this report.

[7] Simple Object Access Protocol (SOAP)- http://en.wikipedia.org/wiki/SOAP
[8] Server Message Block - http://en.wikipedia.org/wiki/Server_Message_Block

Severity Levels of Findings

The California Secretary of State has requested assignment of one of the following three Severity Levels to each finding.

- Low Severity – Implies either the impact to the product is low or already mitigated by the system, or the difficulty in exploitation would likely require indefinite access to the systems, expert knowledge of the system, or would require cost prohibitive resources.
- Medium Severity – Implies either the impact of exploitation to the product would be significant, or the difficulty in exploitation would likely require extended access to the systems, informed knowledge of the system, or would require significant resources.
- High Severity – Implies either the impact of exploitation to the product would result in complete compromise of security, or the difficulty in exploitation would likely require little to no access or knowledge of the systems or little to no resources.

Findings from the February 2014 testing which were found to have been mitigated by changes to the system during the October 2014 testing are assigned a severity level of MITIGATED.

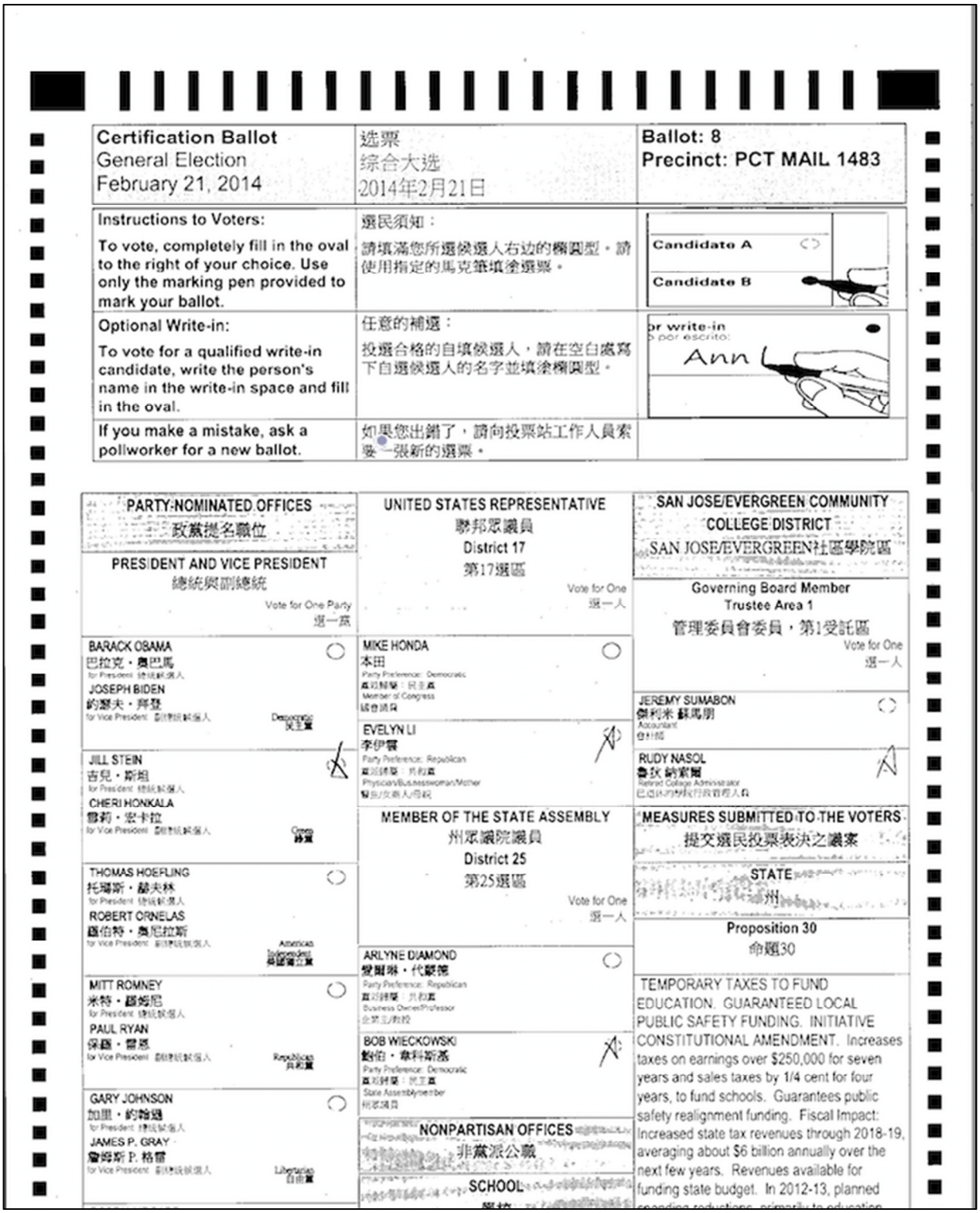
Page #	Finding	Severity Level
14	Lock type plastic seals can be unlocked without leaving any evidence.	Low
15	Hinged-lock type plastic seals are vulnerable to tampering without leaving easily observable evidence.	Low
16	Tie wrap type seals are safe only if pulled tight such that the back of the lock is pulled tightly against the sealed item.	Low
21	The ICE ballot scanned shipping cover can be easily removed and replaced without leaving evidence when the Lock or Hinged-lock type seals are used.	Medium
21	On the ICE ballot scanner the Compact Flash Drive doors can be opened after removal of seals and there is a potential attack on the voting definition and voting backup disks.	High+
22	On the ICE ballot scanner, the ballot box may be opened during an election and ballots added or removed without detection.	High+
24	On the ICE ballot scanner, the main power on/off switch and be switched even when the door that covers it is closed and sealed.	High+
24	Binaries can be converted into original source code allowing access to developer comments, software configurations and hard coded encryption keys.	MITIGATED
25	Zero Trust relationship between EMS Server and workstations allowed access to the SQL database and modification of the test election.	High
25	Encryption keys were recovered from system memory.	MITIGATED
26	User credentials were recovered from system memory.	Medium
26	MS11-030 Vulnerability in DNS Resolution was found on the EMS server but attempts to exploit it were unsuccessful.	MITIGATED
26	MS11-058 Vulnerability in DNS Server allows remote code execution on EMSServer	High
26	SafeNet Directory Transversal Vulnerability was discovered on the ICC Workstation.	Medium
27	Election definition modification on EMS Server and Workstation	High
27	Hardening script was found and was unprotected on system	MITIGATED
28	Recovery of ballot images and DVD files within the SMB traffic between the ICC Workstation and the EMS Server.	High

The items within the table that are marked with the addition sign "+" have been identified by OVSTA to have been mitigated procedurally, through the use of seals, or physically by a change in the ballot box design. These mitigations were not retested by the Red Team reviewers.

Conclusions

While the 4.14.A.1 build of the Democracy Voting System proved to mitigate four previously enumerated vulnerabilities, multiple medium and high vulnerabilities still exist within the suite of systems. A remote user could leverage most of the vulnerabilities across the network to obtain information about the system, voter ballots and results, or gain remote access to the system. If remote access is gained, recovery of user credentials through system memory (RAM) analysis could be executed and used to modify the backend database of the EMS Server.

Appendix A: Recovered Ballot from Adjudication Traffic



Certification Ballot
General Election
February 21, 2014

选票
综合大选
2014年2月21日

Ballot: 8
Precinct: PCT MAIL 1483

Instructions to Voters:
To vote, completely fill in the oval to the right of your choice. Use only the marking pen provided to mark your ballot.

選民須知：
請填滿您所選候選人右边的橢圓型。請使用指定的馬克筆填塗選票。

Candidate A
Candidate B

Optional Write-in:
To vote for a qualified write-in candidate, write the person's name in the write-in space and fill in the oval.

任意的補選：
投選合格的自填候選人，請在空白處寫下自選候選人的名字並填塗橢圓型。

or write-in
o por escrito:
Ann

If you make a mistake, ask a pollworker for a new ballot.

如果您出錯了，請向投票站工作人員索要一張新的選票。

PARTY-NOMINATED OFFICES
政黨提名職位

PRESIDENT AND VICE PRESIDENT
總統與副總統
Vote for One Party
選一黨

BARACK OBAMA
巴拉克・奧巴馬
for President
JOSEPH BIDEN
約瑟夫・拜登
for Vice President
Democratic
民主黨

JILL STEIN
吉兒・斯坦
for President
CHERI HONKALA
雪莉・宏卡拉
for Vice President
Green
綠黨

THOMAS HOEFLING
托瑪斯・赫夫林
for President
ROBERT ORNELAS
羅伯特・奧尼拉斯
for Vice President
American Independent
美國獨立黨

MITT ROMNEY
米特・羅姆尼
for President
PAUL RYAN
保羅・瑞恩
for Vice President
Republican
共和黨

GARY JOHNSON
加里・約翰遜
for President
JAMES P. GRAY
詹姆斯 P. 格雷
for Vice President
Libertarian
自由黨

UNITED STATES REPRESENTATIVE
聯邦眾議員
District 17
第17選區
Vote for One
選一人

MIKE HONDA
本田
Party Preference: Democratic
Member of Congress

EVELYN LI
李伊寧
Party Preference: Republican
Physician/Businesswoman/Mother

MEMBER OF THE STATE ASSEMBLY
州眾議院議員
District 25
第25選區
Vote for One
選一人

ARLYNE DIAMOND
愛麗琳・代蒙德
Party Preference: Republican
Business Owner/Professor

BOB WIECKOWSKI
鮑伯・韋科斯基
Party Preference: Democratic
State Assemblymember

NONPARTISAN OFFICES
非黨派公職

SCHOOL

SAN JOSE/EVERGREEN COMMUNITY COLLEGE DISTRICT
SAN JOSE/EVERGREEN社區學院區

Governing Board Member
Trustee Area 1
管理委員會委員，第1受託區
Vote for One
選一人

JEREMY SUMABON
傑利米 蘇馬朋
Accountant

RUDY NASOL
魯狄 納索爾
Retired College Administrator

MEASURES SUBMITTED TO THE VOTERS
提交選民投票表決之議案

STATE
州

Proposition 30
命題30

TEMPORARY TAXES TO FUND EDUCATION. GUARANTEED LOCAL PUBLIC SAFETY FUNDING. INITIATIVE CONSTITUTIONAL AMENDMENT. Increases taxes on earnings over $250,000 for seven years and sales taxes by 1/4 cent for four years, to fund schools. Guarantees public safety realignment funding. Fiscal Impact: Increased state tax revenues through 2018-19, averaging about $6 billion annually over the next few years. Revenues available for funding state budget. In 2012-13, planned

¶