



REGISTRAR OF VOTERS

ALAMEDA COUNTY • CALIFORNIA

DAVE MACDONALD
ACTING REGISTRAR

CHARLES CORUM
ACTING ASSISTANT REGISTRAR

AGENDA 14 Date: October 10, 2006

October 4, 2006

The Honorable Board of Supervisors
Administration Building
Oakland, California 94612

Dear Board Members:

SUBJECT: VULNERABILITY ASSESSMENT OF SEQUOIA VOTING SYSTEMS FOR REGISTRAR OF VOTERS

RECOMMENDATION:

That the Vulnerability Assessment conducted on Sequoia Voting Systems be received by the Board of Supervisors.

DISCUSSION/SUMMARY:

The State of California has put the Sequoia Voting System through an extensive testing and certification process. Although not required by the State or Federal government, the Board of Supervisors recognized the need to conduct an additional assessment of the Sequoia Voting System in the context of the Alameda County implementation. On June 8, 2006 the Board of Supervisors requested that the Registrar of Voters hire a security specialist to conduct a vulnerability assessment of the complete electronic voting system provided by Sequoia. The purpose of this assessment was to review the end-to-end security of the Sequoia Voting System as it has been implemented in Alameda County and identify any election system vulnerabilities that should be mitigated.

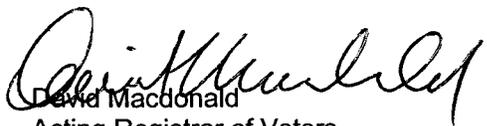
This unprecedented vulnerability assessment was conducted by Pacific Design Engineering. No other County has conducted a voting system assessment of this magnitude. The assessment revealed that the majority of vulnerabilities were already being mitigated by procedures implemented by the Registrar of Voter. Any remaining vulnerabilities were low risk and readily remedied by network security and human process countermeasures.

Alameda County has enhanced its voting system security beyond that of any other county in the State of California. The vulnerability assessment that the Board of Supervisors directed the Registrar of Voters to conduct will help improve the security of the November 2006 election and enhance confidence in the security of Alameda County's voting system and process. This is a step forward for election security.

FINANCING

No additional appropriations are required, and there will be no impact to the net County cost.

Respectfully submitted,


Dave Macdonald
Acting Registrar of Voters

cc: Susan Muranishi, County Administrator
Patrick O'Connell, Auditor-Controller
Richard E. Winnie, County Counsel

Sequoia Voting Systems
Vulnerability Assessment and
Practical Countermeasure
Development
for
Alameda County

October 4, 2006

By

Pacific Design Engineering

Craig Humphreys, craig@pacengr.com

Craig Merchant, CISSP, craigm@pacengr.com

<i>Executive Summary</i>	<i>ii</i>
Scope	ii
Result	ii
Comparison	ii
Key Findings	ii
Summary Findings	iv
<i>Threat Categories</i>	<i>iv</i>
<i>Potential Threats</i>	<i>iv</i>
<i>Countermeasures</i>	<i>iv</i>
Conclusion	v
<i>Scope</i>	<i>1</i>
<i>Methodology</i>	<i>1</i>
Definition of Terms	2
Electronic Voting System Architecture	3
Vote Count Room Security	3
Electronic Voting System Process	4
<i>Electronic Voting System Architecture</i>	<i>5</i>
AVC Edge Touch Screen with VeriVote Printer	5
Optech Insight	6
Optech 400C	7
WinEDS	8
<i>Central Facility Security Assessment</i>	<i>9</i>
Vote Count Room Security	9
Unauthorized Physical Access to Vote Count Room	9
Unauthorized Physical Access to Vote Count Room Computers	9
Unauthorized Physical Access to Vote Count Room Optical Scanners	10
Network Cable Infrastructure	10
Phone Cable Infrastructure	11
Host-Based Security Vulnerabilities	11
Network-Based Security Vulnerabilities	13
Communication Security	13
<i>Voting Process Assessment</i>	<i>15</i>
Electronic Voting System Process	15
Inventory	15
Machine Assignments to WinEDS	15
Generation of Precinct Cards	15
Programming of Equipment for Precincts	16

Assignment of Equipment to Precincts.....	16
Pre-Logic & Accuracy Testing.....	17
Seal and Check-Out.....	18
Poll Operation.....	18
Poll Closing.....	19
Check-In Assets.....	20
Vote Counting.....	20

<i>Diebold and Sequoia Vulnerability Table Details</i>	21
---	-----------

Executive Summary

Scope

At the request of Alameda County, PDE has analyzed public and proprietary information regarding the Sequoia AVC Edge, Optech Insight, 400C, and WinEDS election management and electronic voting components in order to determine possible overall election system security vulnerabilities that can be closed with appropriate and practical countermeasures prior to, or as part of the upcoming November, 2006 elections.

The intent of this engagement was to view the proposed voting process at Alameda County *in aggregate*, and determine practical counter measures for vulnerabilities that may exist in the system components, the information being handled by election workers, and the operation of the various Sequoia Voting System products to be deployed by Alameda County. Thus, the scope of the report is limited to Alameda County and its election processes, systems, and tools. The report is therefore neither a discussion of, nor compilation of theoretical vulnerabilities and exploits against Direct Recording Electronic voting systems (DRE's) or Precinct Count Optical Scan (PCOS) systems. Nor does this report assess non-technical processes and security such as warehouse physical security, guard training, poll-worker training, and so forth.

Result

No practical, realizable vulnerabilities were uncovered that could not be eliminated through appropriate countermeasures involving additional software and data validation or improved physical process countermeasures. The countermeasures recommended to close all discovered vulnerabilities are documented in this report.

From a technology perspective, the Sequoia Electronic Voting System acquired by Alameda County, along with the processes and countermeasures planned by Alameda County for Election Day, can be considered secure.

Comparison

In order to place the findings of this report in context, PDE developed a risk matrix comparing the current/production models of Diebold Electronic Voting System products with the Sequoia Electronic Voting System products in use at Alameda County. The sources of information for this analysis were publicly available well-conducted reports and security audits performed by third parties, and widely disseminated publicly available information on the Diebold system. In performing this comparison PDE endeavored to ensure that information was applicable to **current** products from both vendors (as opposed to the recent Princeton Internet video, which exploits a Diebold system no longer in production).

Vulnerability Comparison for Precinct-Located Electronic Voting Systems		
Vulnerability/Attack	Sequoia	Diebold
Boot Loader Attack	No	Yes
Paper Trail Attack	No	Yes
Microsoft Windows Attacks (various)	No	Yes
Malicious Code Insertion (trojan/virus)	No	Yes
Memory Card Tampering	No	Yes
Known Software Bugs	No	Yes (latest info)
VVPAT or Printout Attacks	No	Yes
Cryptographic Key Attacks	Yes	Yes (keys public)
Window Manager Attacks	No	Yes
Miscalibration Attacks	No	No
I/O Port Attacks	No	No
Network Communication Attacks	No	Yes
Vulnerability Comparison for Centrally-Located Electronic Voting Systems		
Vulnerability/Attack	Sequoia	Diebold
Network Communication Attacks	No*	Yes
Microsoft Windows Attacks (various)	Yes	Yes
Malicious Code Insertion (trojan/virus)	No*	Yes
Election Software Tampering	No*	Yes
Cryptographic Key Attacks	No	No
* = Requires IPSEC communication & election software polynomial checksum validation		

Key Findings

The key findings in our study and the recommended actions are:

1. Plain text password network communication exists between WinEDS and election PC's. The passwords can be discovered by anyone with access to the isolated and physically secured Vote Count Room network.

EXECUTIVE SUMMARY

- a. **Recommend:** The communications between the WinEDS server and the WinEDS client PC's be encrypted with IPSEC.
2. Constant hash and DES encryption keys for the AVC Edge device means the keys may eventually be discovered by someone who gains physical access to a machine, or discovers the key through association with Sequoia Voting
 - a. **Recommend:** We should presume the keys are known to attackers and rely on the existing County strong Chain of Custody physical processes to prevent alteration or corruption of Memory Cards. Also, the state mandated 1% manual vote count provides additional protections against any exploitation of this nature.
3. AVC Edge memory card results are not bound together cryptographically. This means an attacker could theoretically conduct two types of attacks: 1) copy the results from one memory card over another, removing a precinct's results from the final tally, and 2) just copy the results file and SHA1 hash value over the results file of another memory card. WinEDS will recognize a duplicate memory card (theoretical attack #1) and will notify election operators. However, for theoretical attack #2, WinEDS system would simply not record the results from the overwritten memory card.
 - a. **Recommend:** As in (2a), ensure that strong Chain of Custody processes are in place. We further recommend upgrading to newer versions of Edge and WinEDS software that already eliminate this vulnerability, when these new versions are certified by the State of California.
4. The WinEDS system, which is located in a physically secured and isolated network in the Vote Count Room, is based on a vulnerable operating system, Microsoft Windows, that is known to be susceptible to viruses, worms, and other forms of hacking, and for which many hacking tools are readily available on the Internet (e.g. WAREZ IRC chat rooms and websites)
 - a. **Recommend:** The key program files can be checksummed (using a checksum application external to Windows itself) before, during, and after an election and the results compared to the WinEDS "Gold Standard" image. If the results check out, we know that the WinEDS software stayed intact throughout the election process.

Conclusion

The Sequoia Electronic Voting System selected by Alameda County to conduct election operations is inherently secure. The relatively low risk vulnerabilities that do exist in the Sequoia Electronic Voting System components are readily remedied by network security and human process countermeasures, which have been adopted by Alameda County. This positive analysis is based on the fact that Sequoia precinct equipment, although microprocessor-based, does not have an underlying operating system that can be obtained in the public domain, inspected, analyzed, and vulnerability-exploiting tools created, as is true with Windows, Linux, and most every standard operating system.

Sequoia Voting Systems, of Oakland, California, has taken a very different strategy than other manufacturers in implementing their Electronic Voting Systems. Their products are straightforward, purpose-built electronics systems, which do not use publicly available technologies for precinct equipment, and, therefore do not suffer from vulnerabilities common in Microsoft Windows based precinct equipment.

Further, Alameda County has elected to implement strong security processes to further tighten security around setup and operation of the Electronic Voting System components, with special attention to memory cards and voting results tabulation. The County has designed a voting system that is inherently paper-based, and is thus intrinsically verifiable.

Scope

Alameda County engaged Pacific Design Engineering (PDE), a network, IT services, and system security consultancy, to perform a vulnerability assessment and practical countermeasure development effort for its Electronic Voting Systems and associated processes. The scope of the engagement encompassed the technologies and processes that were unique to the Electronic Voting System as implemented at Alameda County. Threats against voting systems in general, such as vote buying schemes or invalid registration of voters, were not considered part of this scope. Further, post-election vote count analytics and validation decision-making processes were not considered part of this engagement.

A number of areas with the potential to create vulnerabilities of the Electronic Voting System were included in the vulnerability assessment and practical countermeasure development effort:

- Computer Security Practices of Electronic Voting System Vendor
- System Architecture of Direct Recording Electronic voting machines with Voter Verified Paper Trail (DRE with VVPAT)
- System Architecture of Precinct Count Optical Scan (PCOS) Machines
- System Architecture of Vote Count Software
- Configuration of DRE with VVPAT Machines
- Configuration of PCOS Machines
- Configuration of Vote Count Room Computers
- Configuration of Tally Servers
- Physical Security of Vote Count Room
- Security of Vote Count Room Networks
- Electronic Voting System Election Processes

Methodology

The vulnerability assessment started with the development of a catalog of potential attacks against electronic voting systems. This catalog was developed from attacks outlined in the Brennan Center report, *The Machinery of Democracy: Protecting Elections in an Electronic World*, attacks outlined on several Internet sites devoted to electronic voting, and a variety of common attacks against computing systems in general.

After the attack catalog was assembled, PDE performed an in-depth analysis of the Alameda County voting system in three major areas: Electronic Voting System Architecture, Vote Count Room Security, and Electronic Voting System Processes.

Definition of Terms

Vulnerability

In the context of this report we define a "Vulnerability" to mean any technology-based condition of software, system, or data such that a chain of events or actions initiated by a 3rd party or a malicious insider could inflict damage to the accuracy, reliability, or completeness of an election.

Operating System

A complex body of software that provides controls over, and services for, hardware, application software, and input and output devices for a computer. Operating Systems are necessary to make computers useful, and to make application software easy to write and easy to install. Thus, Operating Systems, by their very nature, are major contributors to Vulnerabilities in election systems and all other forms of Information Technology. Microsoft Windows is widely held to be the least secure (most vulnerable) Operating System.

Application

An application is a body of software, much smaller and less complex than an Operating System, which provides a specific purpose. Microsoft Excel, WinEDS, iTunes, Adobe Acrobat, and the HPX host application in an Optech Insight device are all examples of Applications.

Some Applications require an underlying operating system to function (Adobe Reader, Microsoft Excel, iTunes, and WinEDS). Others do not (HPX and AVC Edge).

Embedded Application

This is a special kind of application that does not reside on a hard disk and require an Operating System to run. Embedded Applications are burned into firmware in devices known as NVRAM, Flash, PROM, or even Static RAM in some cases. They are non-volatile devices that retain memory contents between power cycles.

Embedded Applications are all around us, in our cars, dishwashers, alarm systems, printers, and even our toasters. They serve one purpose and one purpose only, and are often extraordinarily difficult to alter for other purposes.

Attack Vector

The specific line of attack, or series of events that, if successfully completed, would gain access to, or create the ability to manipulate data successfully on an Electronic Voting System. The term "Attack

Vector" is used in virtually the same sense as a Virus Vector in Epidemiology and Virology.

Trust

An Information Technology term referring to whether an IT system treats information from another source as "known good" or valid, or treats it as suspect information that must be validated via a pre-determined mechanism.

Checksum

A checksum is a mathematical relationship between a group of numbers or characters that compose a message or document, and a resultant single number. Checksums are commonly used in telecommunications to ensure transmitted data arrives intact and unaltered. Simple checksums involve adding bit positions or blocks of values in a document to produce a result, but these checksums offer poor security. Polynomial checksums are far more secure, as they offer a One-To-One relationship between a document and the resultant checksum value that cannot practically be produced from an altered form of the document.

Electronic Voting System Architecture

Through a series of interviews with Sequoia Systems staff, PDE examined the development process and system architecture for the AVC Edge touch screen devices, the Insight optical scanners, and WinEDS management software.

The following areas were analyzed to determine what potential security risks existed in the design, manufacture, and operation of Sequoia Systems Electronic Voting System devices:

- AVC Edge Touch Screen Systems with VeriVote Printer
- Optech Insight Optical Scanners
- Optech Insight 400C Central Count Scanners
- WinEDS Election Management Software

Vote Count Room Security

PDE performed a security audit of the Alameda County Vote Count Room to determine if any physical or electronic threats remained unaddressed. This audit consisted of interviews with Alameda County staff, a physical inspection of the Vote Count room, a vulnerability scan performed by automated security software, a review of the system configuration of each class of electronic voting system, and an analysis of the configuration files of several network devices.

The following areas were analyzed to determine potential security risks that may exist in the Vote Count Room:

- Unauthorized Physical Access to Vote Count Room
- Unauthorized Physical Access to Vote Count Room Computers
- Unauthorized Physical Access to Vote Count Room Optical Scanners
- Network Cable Infrastructure
- Phone Cable Infrastructure
- Host-Based Security Vulnerabilities
- Network-Based Security Vulnerabilities
- Communication Security

Electronic Voting System Process

PDE reviewed the processes and procedures used to manage and operate the systems used for the County election. Through interviews with county election officials and reviews of process diagrams and training materials, PDE examined the entire county election process for security weaknesses.

The following processes were analyzed to determine if potential weaknesses were evident:

- Inventory
- Machine Assignments – WinEDS Asset Tracking
- Generation of Precinct Cards
- Programming of Equipment for Precincts
- Assignment of Equipment to Precincts
- Pre-Logic & Accuracy Testing
- Equipment Seal and Checkout
- Setup and Opening of Polling Station
- Poll Operation
- Poll Closing
- Equipment Check-In and Asset Tracking
- Vote Counting

Electronic Voting System Architecture

AVC Edge Touch Screen with VeriVote Printer

The AVC Edge is a touch screen voting system used by the County to comply with federal requirements for disabled voters (HAVA). Voters access the machine by inserting a voter access card into the machine's smart card reader. The voter then makes selections using the touch screen. The unit also includes keypad and audio functionality for the visually impaired. A printer is attached to the unit to provide voters with a voter verifiable paper record of their votes and to provide a printed summary report at the end of the election. This printer, known as a VVPAT, meets a State of California mandated requirement.

System Architecture

The AVC Edge is an embedded application that performs election operations based on configurations obtained from files loaded on PCMCIA memory cards. The election configuration files are generated by the WinEDS election management software. These configuration files are hashed using a SHA1 hash with a 160-bit key.

Election results and audit logs are stored by the AVC Edge on the PCMCIA memory card, and stored internally on the AVC Edge machine for redundancy, and put through the same hashing process as the configuration files. These cards are transported to the Vote Count room to be decrypted, verified, and uploaded to the WinEDS software.

System Operation

- a) System is configured with a PCMCIA card in a secure environment with the proper election configuration for the destination precinct. Machine remains guarded and protected until delivered to precinct with the memory card already installed.
- b) Trained election worker initializes machine, runs self-tests, and ensures AVC Edge system initializes properly. The worker then switches to Election mode, which disables all testing, diagnostic, and validation capabilities.
- c) AVC Edge system checks itself (verifies its own firmware at startup), and verifies all election configuration and results files before starting. The firmware computes a SHA-1 checksum of itself during Power-On-Self-Test and reports this value, and indicates if the checksum is not correct.
- d) Voters gain access to AVC Edge through a Voter Access Card (VAC). This is a simple card with a 256-byte memory containing DES-encrypted (using a 56-bit key) information authorizing this voter to vote for the next 60 minutes (this is a configuration value set for Alameda County). Voters receive these cards from election workers when they register at the precinct.
- e) Voter interacts with AVC Edge system until voter is confident the votes cast match his/her wishes. Then the voter confirms the ballot and the results are written to the election file on the memory card, the SHA1 hash value is

updated, read back to the AVC Edge, and re-validated. After the ballot is cast, the AVC Edge invalidates the Voter Access Card. The VVPAT (Voter Verification Printer) retains a paper record of the ballot cast in a secure physical chamber inside of the VVPAT. The system then waits for the next voter.

- f) Step (e) is repeated until the election is closed.
- g) When the election is closed, the machine exits Election Mode and enters Polls Closed Mode where further voting or reopening of the polls is forbidden. It outputs final election summary information (total votes cast, date, time, etc.) on the VVPAT, and the AVC Edge generates summary information, writing the summary to the VVPAT printer, and then the VVPAT printer is disabled.
- h) Poll workers (using the Two-Person rule) take the PCMCIA memory card out of the AVC Edge, gather the summary tallies and the VVPAT voter records, and place them in the Ballot Bag for delivery to a Collection Center. The Collection Center workers (using the Two-Person rule) deliver the results from their assigned precincts to the Vote Count Room.
- i) WinEDS client PC's read the PCMCIA card for each precinct and verify their legitimacy by checking the SHA1 hash value and successfully validating the results file(s). The results for each precinct are uploaded to the central WinEDS server and tallied.

Optech Insight

The Optech Insight is an optical scanner that reads marks on paper ballots. Voters mark their ballots in voting booths and insert their completed ballot into the Optech scanner and the voter's choices are recorded on a memory card. At the close of polls the Optech's memory card is placed into the Ballot Bag and sent to the central Vote Count Room for tallying.

System Architecture

The Optech Insight is a very simple two-part Embedded Application. The core system, known as HPX, resides in firmware on the Optech scanner. The HPX code is very stable and changes infrequently. The HPX code is written into non-writeable memory (a PROM – Programmable Read Only Memory) that cannot be modified programmatically. The only way HPX updates can occur is to change the physical PROM device in the Optech Insight machine. The HPX code performs paper-handling operations and invokes election specific code, called APX, for ballot definition files and precinct identifiers. The APX code resides on a MemoryPack installed in each scanner. The MemoryPack is a special memory card that contains three components:

1. A static RAM backed-up by battery that contains election results and election information files. These files also are accompanied by a CRC16 checksum of the files at the time they were written to memory.
2. An EEPROM that contains the APX application software, with a CRC16 checksum of the APX software file.

3. A clock module that is backed up by redundant lithium batteries

The APX application memory has special signaling lines that make it extremely difficult for another type of physical device to alter the memory, and thus the APX program. In other words, should an attacker somehow gain access to APX firmware, be able to interpret it, modify it, and generate useful assembly language code, they would have to understand and properly use the memory line signaling required to actually alter a MemoryPack memory contents. This is a very rare skill, and requires unfettered, extended access to both Optech Insight devices and MemoryPacks, since standards-based microprocessors and memory devices simply will not work the same way.

System Operation

1. A MemoryPack is initialized with election-appropriate software, called APX, and election definitions that specify how to interpret scans of ballots to produce accurate voting results.
2. The MemoryPack is inserted into the Optech Insight at the secure, County-controlled warehouse. Once the Insight is started up on Election Day, the Insight analyzes the MemoryPack, validates all of its contents through checksum comparisons, and starts executing the code.
3. A poll worker runs through a series of self-diagnostic tests to ensure that the scanner is operating normally. When the tests are complete, the scanner is put into election mode and is ready to accept ballots.
4. As each ballot is scanned, the result is written to the MemoryPack in the Results file (and the CRC16 hash value is appropriately updated). This process step (4) is repeated for each ballot introduced.
5. When the election is over, a poll worker ends the election mode and removes the MemoryPack. The MemoryPack is placed into an anti-static bag and placed into the Ballot Bag for transport to the central Vote Count Room. Two results reports are then written, one posted at the precinct, and the other placed in the election bag for return to the Voting Room.
6. The MemoryPack is read by a MPR (MemoryPack Reader), where the results files are first validated by verifying the checksum value for the election results. The MPR transmits the results over a physically secured, isolated local area network to the WinEDS server where the results are tallied into the election totals.

Optech 400C

The Optech 400C is a high capacity scanner used to rapidly count ballots in the Vote Count Room. The system is composed of a high-capacity scanner and an underlying Windows operating system. Results from a scanning operation are moved to the WinEDS Tally Count machine for inclusion in election results by physically removing a memory cartridge from the Optech 400C and inserting it into a

WinEDS client PC, which in turn, transmits the results over a physically secured, isolated network to the WinEDS central tally server.

It is important to observe that the Optech 400C high capacity scanner is not publicly accessible at any time, as the device resides in a highly secure physical environment, the County Vote Count Room.

WinEDS

WinEDS is a Windows operating system-based application that performs election initialization and tallying operations. The system is composed of .exe, .obj, .ppd, .ocx, .dll, and .sys files located in a well-defined directory under Windows.

WinEDS is responsible for creating the ballot definition files for each precinct and putting them onto the appropriate Optech MemoryPack or AVC Edge memory card. An asset tracking system within the application keeps track of the status of each memory device to ensure that memory cards are not skipped or duplicated. After the election is closed, the WinEDS system returns to service and tallies ballot results and determines election results.

Central Facility Security Assessment

Vote Count Room Security

Unauthorized Physical Access to Vote Count Room

To ensure the integrity of the central vote counting and reporting systems, unauthorized users cannot access the room undetected. If an intruder were able to gain unauthorized access to the room, attacks could be initiated against the high-speed optical scanners, the computers used to upload vote counts from memory cards, the tally servers, or network infrastructure devices.

Current Countermeasures

Alameda County has taken great care to secure the Vote Count Room against unauthorized access. Accessing the Vote Count Room requires knowledge of a door code as well as a key. Motion detectors in the room and an alarm system alerts the County if an intruder attempts to access the room.

Recommended Improvements

The outer wall of the Vote Count Room does not extend entirely to the ceiling. It only extends a foot or two beyond the raised ceiling. The motion detectors inside the room would make it difficult for an attacker to get over the outside wall undetected.

There are, however, several sets of network cables that could theoretically be accessed in the raised ceiling above the Vote Count Room. Devices exist that could be connected to these cables and give the attacker the ability to access the network and alter data.

PDE recommends the following steps be taken to ensure that no data can be altered by external access to the network cables:

- Use of "ARP detection" features in Cisco network devices (details below)
- Use of encrypted networking protocols such as IPSEC between network nodes (details below)

Unauthorized Physical Access to Vote Count Room Computers

To prevent an attacker from tampering with the internal components of the computers, physical access to the systems should be restricted as much as possible. We recommend steps be taken to ensure that if an attacker has successfully accessed the inside of election system computers, administrators will be alerted to the tampering. BIOS alerts, for example, are capable of providing such notification.

Current Countermeasures

Vote Tally Servers and all network infrastructure components are secured inside a locked server cabinet. The manufacturer's lock on the cabinet has been replaced. The Sequoia Optech 400c optical vote scanner has a locked compartment that contains the PC used to manage the system.

Recommended Improvements

Most modern PCs have a feature in the computer BIOS that will alert the administrator if the case has been opened. If the desktop computers used by the County support this feature, administrators can ensure that it is operational. Tamper-evident seals can be applied to the computer at certification to make it more difficult for an attacker to hide a tampering attempt.

Unauthorized Physical Access to Vote Count Room Optical Scanners

To ensure the integrity of the components inside the scanner, an attacker must not gain unauthorized access to the inside of the scanner.

Current Countermeasures

A lock secures all internal compartments of the 400C scanner. Tamper-evident seals will be placed on compartment doors to ensure that administrators will notice any access to the internal components. These seals are checked at the beginning and end of Election Day.

Network Cable Infrastructure

The network cable infrastructure inside the Vote Count Room should be secured to prevent the isolated vote count network from being connected to other county networks. Additional network cables should not be connected to Vote Count Room network equipment without administrative approval.

Current Countermeasures

All network cables terminate inside the locked server cabinet. None of the jacks inside the room connect to any outside county networks, making it virtually impossible for an intruder to bridge the gap between the isolated Vote Count Room network and other county networks.

Recommended Improvements

As mentioned previously, a number of the network cables are routed above the false ceiling, making it difficult for administrators to monitor them for rogue devices. To prevent any vulnerability from an admittedly unlikely access to these cables, PDE recommends that IPSEC security be used for data transmissions across the physically secured, isolated Vote Count Room network. In addition, PDE recommends using ARP detection features of Alameda County's existing Vote Count Room Cisco networking components.

Phone Cable Infrastructure

In order to prevent an attacker from gaining remote access to computers in the Vote Count Room, PDE recommends that phone lines be strictly secured. The Vote Count Room will require several active phone connections to allow Vote Count Room ROV employees to have voice communication capabilities.

Current Countermeasures

All unnecessary analog and digital phone lines that terminate inside the Vote Count Room will be disconnected from the patch panel prior to Election Day. Any modems that exist in Vote Count Room PC's will be disabled as described in the Host-Based Security Vulnerabilities section that follows.

Host-Based Security Vulnerabilities

An exhaustive description of all potential attacks against Windows-based PCs is beyond the scope of this document. To create a highly secure PC, a number of steps are recommended:

- 1) Anti-virus software is now capable of detecting a wide variety of viruses, trojan horses, spyware, malware, and other malicious software, including viruses and malware not previously known to the anti-virus software ("zero-day" attacks). A host-based firewall solution, such as the native Windows Firewall, can be enabled and configured to block all non-essential inbound and outbound traffic. This combination would improve overall security of the Windows PCs.
- 2) The host can be "hardened" in a process that disables unnecessary device drivers, Windows services, and unnecessary applications. The Windows Local Security Policy applet can be used to enforce robust password policies, restrict sensitive user permissions, and audit critical system events. Any computers that do have modem hardware will have this hardware disabled as part of this hardening process.
- 3) Patches from Windows and 3rd party vendors can be applied to these systems regularly to reduce the risk of unauthorized access or denial of service.

4) Remote Assistance and Remote Desktop features can be disabled to prevent an attacker from remotely viewing or controlling a secured PC.

Current Countermeasures

The WinEDS client laptops are running a Windows Firewall and do not advertise any open ports to the physically secured, isolated Vote Count Room network.

Recommended Improvements

All of the Vote Count Room Windows systems could benefit from anti-virus and firewall software and intrusion detection software tools.

3rd party host-based firewall and intrusion detection solution (IDS) can be installed on all of the Windows systems. High-quality commercial firewall and IDS packages contain a number of features that will reduce the risk of “zero day” attacks or risks from unpatched vulnerabilities, provide file integrity protections for election software, and lock down a number of Windows components.

Many of the Windows systems audited were not fully up-to-date on Microsoft security patches. These machines would be more secure with the latest security patches applied.

All of the Windows machines would be more secure after going through a hardening procedure. At a minimum, a hardening procedure consists of using the native Windows Security Configuration & Analysis applet to apply the Windows hisecws.inf “best practices” security template to each machine. This template will implement secure policies for system auditing, passwords, account lockouts, and advanced security settings.

Windows machines are most secure when unnecessary installed software, such as MSN Messenger, DVD burning software, Windows Media Player, and Outlook Express are not present. All applications that are not required to meet the certification standard of Sequoia Systems can be removed as part of the hardening process.

By default, Windows systems run a variety of unnecessary services such as Alerter, Messenger, Task Scheduler, and Fax. All unnecessary services can be stopped and administratively disabled as part of the hardening process.

To reduce the risk of an attacker introducing malicious software or gaining remote control of the machine, all unnecessary device drivers can be disabled. Modems, floppy drives, USB drives, serial ports, parallel ports, and infrared ports can all be disabled in the Windows device manager. For added security, the device driver files can be removed from the machines completely.

Windows computers with the Remote Assistance feature enabled pose a greater security risk than those without Remote Assistance enabled. Remote Assistance allows a computer to share its desktop with another Windows system. This feature could be used by an attacker to gain remote control of a Windows system.

Network-Based Security Vulnerabilities

Like host-based vulnerabilities, there are thousands of potential attacks against computers that can be attempted over the network. The overwhelming majority of these attacks can be successfully mitigated using a combination of network devices and host-based security efforts.

Current Countermeasures

The Vote Count Room networks for the WinEDS stations and the high-speed optical scanners are physically separate from the County network and each other. The network switches are housed in a locked server cabinet. Unused ports are administratively disabled and placed in an unused VLAN to prevent unauthorized systems from plugging into the network.

Recommended Improvements

PDE recommends that a network intrusion detection sensor (NIDS) be installed in the Vote Count Room and configured to monitor both network switches. The NIDS will provide the County with a full audit trail of all network communications that take place in the Vote Count Room and provide a console for analyzing potential security violations.

There are several security features available in the most recent Cisco IOS versions that can be used to thwart a variety of network attacks. Both Dynamic ARP Inspection and storm control features can be enabled on the Vote Count Room switches to improve physical network access security.

Communication Security

PDE recommends that the systems responsible for reading the vote counts from the Sequoia memory cards send the vote count to the tally server using an encrypted channel. This ensures that usernames and passwords are never sent in clear text and that data cannot be modified by an attacker while it traverses the physically secured, isolated Vote Count Room network.

The WinEDS clients use the Tabular Data Stream (TDS) protocol to communicate with the tally servers. TDS was a protocol originally developed by Sybase and licensed to Microsoft in a technology sharing agreement.

During its research into security vulnerabilities in the computers operating on the Vote Count Room physically secured, isolated network, PDE discovered that the WinEDS clients send usernames, passwords, and election data to the tally servers without encryption.

Recommended Improvements

Although the use of unencrypted communications over the physically secured, isolated Vote Count Room network between the WinEDS clients and the tally server represents a security risk to the voting system, it is a risk that can be easily mitigated using native Windows or 3rd party tools. Windows computers are capable of encrypting network traffic using the IPSEC protocol.

By placing the unencrypted TDS traffic inside an encrypted IPSEC tunnel, no sensitive data will traverse the network unencrypted. Breaking the security of the Windows IPSEC implementation would be extremely difficult for an attacker to do successfully.

Another option would be to use a Windows implementation of the Secure Shell Protocol (SSH) to encrypt the traffic between WinEDS clients and server. Both of these options would provide sufficient protection for the physically secured, isolated Vote Count Room network traffic.

Voting Process Assessment

Electronic Voting System Process

Inventory

When electronic voting systems are received from the vendor, the County Asset Tracking System generates Asset ID barcode labels. Barcode labels are applied to the AVC Edge and Insight machines. The barcode ID and serial number of each machine are added to Asset Tracking System.

Current Countermeasures

This is the beginning of the “chain of custody” that will follow the equipment through the election process. Strict control of the asset management system makes it difficult for an attacker to insert a compromised MemoryPack or memory card at the beginning stage of the process.

PDE noted that the serial number for printers, HAAT card activators, memory cartridges, and scanner MemoryPacks are used as part of the asset tracking process, thereby creating a strong Chain of Custody.

Machine Assignments to WinEDS

Each AVC Edge machine and Insight scanner are assigned to a precinct in WinEDS. When all of the machines have been assigned to precincts by WinEDS, the assignments are exported to a file and then imported into the County Asset Tracking System. As a point of clarity, WinEDS maintains its own internal asset tracking system that matches AVC Edge and Insight devices to precincts.

Current Countermeasures

Since the WinEDS system is responsible for randomly assigning voting machines to each precinct, it would be virtually impossible for an attacker to target a specific precinct with a compromised AVC Edge or Optech Insight device inserted during the inventory process.

Generation of Precinct Cards

Each Ballot Bag, HAAT case, and VVPAT case contains a Precinct Card in a clear pouch on the outside of the case. The Precinct Cards are barcoded with a prefix to identify whether it is for a HAAT case (“H”), a VVPAT case (“P”), or a Ballot Bag (“B”). These cards are generated by a Windows application.

Current Countermeasures

The Precinct Cards are created and printed by two staff members to ensure that duplicate cards are not created. The WinEDS software will alert staff if an attempt is made to create a duplicate card. If duplicate cards were created, they could be used by an attacker to substitute compromised HAAT or printer devices later in the equipment provisioning process. Thus, the County countermeasure is an important one.

Programming of Equipment for Precincts

Precinct assignment labels for the AVC Edge memory cartridges are printed by the WinEDS software. The memory cartridges have the unique precinct data written into the memory cartridge. When the write process is complete, the assignment label is affixed to the memory cartridge.

WinEDS copies the precinct information files to a USB flash drive for use in programming the HAAT Card Activator device. When the HAAT Card Activator has been successfully configured, the precinct assignment label is attached.

WinEDS prints precinct assignment labels for the Insight scanner MemoryPacks. The data files for each precinct are written into the MemoryPacks using the MemoryPack Reader (MPR). Precinct assignment labels are attached to each MemoryPack.

Current Countermeasures

Multiple county staff members are responsible for the printing of precinct assignment labels and the programming of memory devices and HAAT Card Activators to reduce the risk of deliberate or accidental misconfiguration of the devices from a single individual.

Assignment of Equipment to Precincts

In this phase, barcode readers are used to assign electronic voting systems from the warehouse to individual precincts. AVC Edge touch screen machines are associated with a memory cartridge and assigned to each precinct. Insight scanners and MemoryPacks are associated with each other and assigned to precincts. The VVPAT printers and HAAT Card Activators are also assigned to each precinct.

Current Countermeasures

Multiple county staff members are involved in each phase of the precinct assignment and asset tracking steps to reduce the risk of a single individual accidentally or

deliberately breaking the chain of custody. If a system does not properly match its serial number with the asset tag or appears to have had its asset tag tampered with, the system is not assigned to any precinct until any inconsistencies have been resolved.

Pre-Logic & Accuracy Testing

Pre-Logic and Accuracy tests are performed on each device at the warehouse. The Optech Insight scanner is powered on and run through a simple series of diagnostic tests to confirm that the device is operational. Then a test deck of four ballots is fed into the system. These ballots contain two error conditions and a write in vote to ensure that the machine will properly handle all of the potential ballot states. After the test is performed, the audit log is verified to see if any internal errors were generated.

The AVC Edge devices are powered on, the system time is verified, and the device is calibrated. A results cartridge is inserted into the system and an election definition file is loaded. The device is placed into Pre-LAT mode and a number of simulated votes are processed by the system. After those results are verified on the memory card and the VVPAT printout, a series of manual votes are entered and verified. Finally, the audio unit is enabled and audio votes are entered and verified.

The memory cards from the Optech and Edge devices are uploaded into the WinEDS software and validated. If a machine fails the Pre-LAT process, the machine is excluded from the election and will have its software and/or firmware reinstalled.

Current Countermeasures

The Pre-LAT procedures should be able to detect virtually any tampering with election configuration files on the electronic voting systems. While it is theoretically possible that an attacker could write malicious software or firmware that would be able to identify the testing procedures and deactivate itself until the day of the election, no such attack has ever been demonstrated to date for Sequoia Electronic Voting System components. The encryption and authentication mechanisms described earlier in the System Architecture section would make such attacks virtually impossible.

In addition, the County currently generates an ad-hoc test ballot set that is used to do Pre-LAT testing after the internal Electronic Voting System Pre-LAT tests have been successfully run. The County test cases are generated just prior to an election to ensure that no attacker could gain access to the test cases.

Seal and Check-Out

During this phase, tamper-evident seals with barcodes are placed on each VVPAT printer, AVC Edge touch screen device, and Insight optical scanner. These seals are scanned into the Asset Tracking System to ensure that the proper seal is associated with the proper device.

Checkout and Print Reports for each precinct are generated and each asset is checked against the report to ensure that it has been assigned to the proper precinct. Upon successful verification, Delivery and Seal Verification sheets for each precinct are created.

All of the electronic voting systems for each precinct are shrink-wrapped on a cart or shipping palate. Tamper-evident seals are placed on each shrink-wrapped cart to be delivered. A 3rd party shipping company is responsible for the delivery of the shrink-wrapped carts to the polling stations.

Precinct Cards are inserted into Ballot Bags and sent to the distribution center.

Current Countermeasures

The application of tamper-evident seals following the Pre-LAT tests ensures that an attacker cannot open the housing of the electronic voting device to insert malicious firmware or software into the system without being discovered. Associating the tamper-evident seal with the asset tag of the device in the Asset Tracking System reduces the risk that an attacker could steal a tamper-evident seal and install it after tampering with the contents of the electronic voting device.

Multiple county election workers are involved with each step of the process to reduce the likelihood that any malicious activity or human errors impact the operation of the voting machines.

Poll Operation

A lengthy discussion of all of the processes and procedures used at each polling station is outside the scope of this document. It should be noted that if any of the AVC Edge or Insight devices appear to be malfunctioning during the operating hours of the polling station, the devices will be taken off-line and paper ballots will be processed on the high-speed optical scanners in the Vote Count Room.

Current Countermeasures

Tamper-evident seals on the AVC Edge devices will be inspected when the polls are opened and closed to ensure the devices have not been tampered with. If signs of tampering exist, the paper ballots will be used instead to determine the correct election tally. The same process will be applied to the Optech Insight PCOS

machines. If tampering is suspected, the physical ballots will be counted by scanning them through the Optech 400C high-capacity scanner in the Vote Count Room.

The 1% manual recount will validate results for both AVC Edge and Optech Insight device results at those randomly selected precincts. This is done after all votes have been tallied, including absentee ballots. This is the State of California requirement that 1% of precincts be randomly selected for inclusion in the manual recount process. This 1% manual recount acts as a second line of defense against unauthorized modification of an Electronic Voting System component or data file.

It is noteworthy that the Optech Insight, which is the device performing the bulk of the election for Alameda County (Edge devices are for HAVA-compliance only), does not have the ability to propagate changes from MemoryPack to MemoryPack, because there is no writeable persistent memory within the Optech Insight device. The HPX firmware is stored on a Programmable Read-Only Memory (PROM) chip.

PDE notes that there are certain countermeasures being discussed in public forums, which are not practical for counties with limited numbers of poll workers available on an election day. Our charter for this engagement is thus restricted to practical countermeasures that can actually be implemented by Alameda County.

Poll Closing

After the polls are closed, the memory cartridges from the AVC Edge touch screen systems and the MemoryPacks from the Insight optical scanners are removed from the machines and placed into anti-static memory card bags. The anti-static memory bag is placed in the Ballot Bag along with the various ballots and log.

The Ballot Bag is inspected by both a Poll Worker and Captain and then sealed at the polling station and delivered by two polling station workers to a collection center. Ballot Bags from multiple precincts are transported from the collection centers to the Vote Count Room.

The AVC Edge touch screen machine is closed and sealed. All of the electronic voting system components are packed and delivered by truck to the warehouse for storage.

Current Countermeasures

The two-person rule is followed when poll workers perform the inspection, packaging, and transportation of memory cards and audit logs, making it very difficult for an attacker to manipulate or destroy memory cards and audit logs in transit.

Check-In Assets

The Ballot Bag and VVPAT case from each polling station is received at the Registrar of Voters staff room. The barcode on the VVPAT case is scanned to check it back into the Asset Tracking System and then sent to a holding area before being returned to the warehouse.

The seal is broken on the Ballot Bag and the roster, memory card, and MemoryPack are removed. The barcode on the Ballot Bag is scanned and checked into the Asset Tracking System. The barcodes on the roster, memory card, and MemoryPack are scanned and checked into the Asset Tracking System with an "Asset Received" status.

The memory cards and MemoryPacks are taken to the Vote Count Room for upload to the tally servers by Registrar of Voters workers on Election Day in the presence of many other people, including independent observers. The votes are then uploaded to the WinEDS system from secure computers in the Vote Count Room.

After the votes have been successfully uploaded to the tally servers, the memory card and MemoryPack are checked into the Asset Tracking System with an "Asset Uploaded" status.

Current Countermeasures

Multiple poll workers handle the memory cards and MemoryPacks at all times to ensure that the chain of custody has not been broken. The Asset Tracking System and WinEDS software ensure that memory cards and MemoryPacks cannot be uploaded more than one time. If the barcode of any memory cards or MemoryPacks fails to match the code registered in the Asset Tracking System, the VVPAT paper trail or paper ballots are used as the authoritative vote count.

Vote Counting

After the memory cards from the Insight and AVC Edge devices have been uploaded to the WinEDS server, the votes are tallied and reports are generated.

Current Countermeasures

1% of precincts are randomly selected for a manual recount to ensure that the election results on the memory devices are accurate.

Diebold and Sequoia Vulnerability Table Details

The following vulnerability list was used to assess vulnerability levels for current Diebold and Sequoia Electronic Voting System equipment:

Vulnerability	Description
Boot Loader Attack	Ability to “trap” the booting process and insert malicious software that will alter operating system or application software
Paper Trail Attack	Replace or alter the paper trail from the VVPAT to permit alteration of votes, or cast doubt on the accuracy of electronic votes
Microsoft Windows Vulnerabilities	List of known vulnerabilities of MS Windows
Malicious Code (Trojans or viruses)	Code that could be inserted into a system and alter the operation in a predictable and externally controllable fashion
Memory Card Tampering	Altering contents of a memory card used in election results tabulation
Known Software Bugs	Relative incidence of known bugs causing defects in the behavior of the DRE or PCOS
VVPAT or Printout Attacks	Attacks involving denial of service or alteration of external voter verification printer contents
Cryptographic Key Attacks	Attacks that can discover the cryptographic keys and give the attacker the ability to generate false election information and potentially insert it into the election Chain of Custody process
Windows Manager Attacks	Attacks that alter the DRE windowing system behavior to systemically alter the results of an election
Miscalibration Attacks	Attacks that alter touch-screen (DRE) or ballot interpretation in scanners (PCOS) to change election results
I/O Port Attacks	Attacks that gain access or control over a DRE or PCOS by altering or manipulating an Input/Output Port that exists on the hardware.
Network Communications Attacks	Attacks that can alter data communicated between Electronic Voting System components, in particular

Election Software Tampering	the Central Server and other Electronic Voting System devices Attacks that involve altering the software on the Central Tally Server in order to alter election results
-----------------------------	--