Common Software Weaknesses Reported in Evoting Systems

Michael Kass

Joshua Franklin

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Disclaimer

Certain commercial entities, equipment, or materials may be identified in this presentation in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

National Institute of Standards and Technology

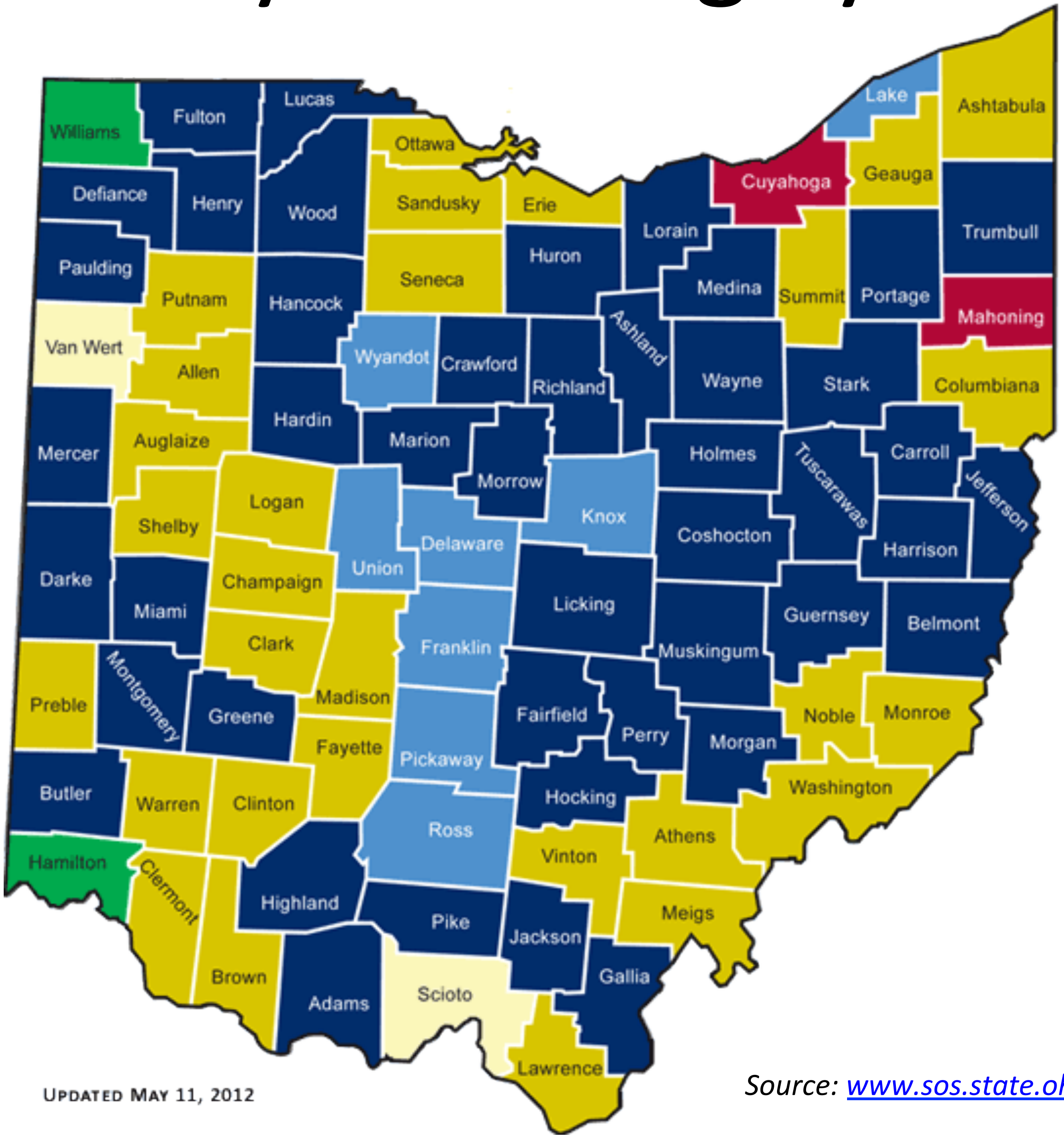
Overview

- Elections in the U.S.
- Types of Voting Systems
- Election Workflow
- Background (TTBR & EVEREST)
- Vulnerability Reports
- Mapping CWE to Reported Weaknesses
- Conclusions

Voting in the US

- Elections are run at the State & Local level
  - NOT federal
  - Top down vs. Bottom up organization
  - Secretary of State usually head election official
- States purchases their own voting systems
  - No two states are exactly alike
  - Few minimum federal machine requirements
  - Election Officials use them for as long as possible (10+ years)

Diversity of Voting Systems

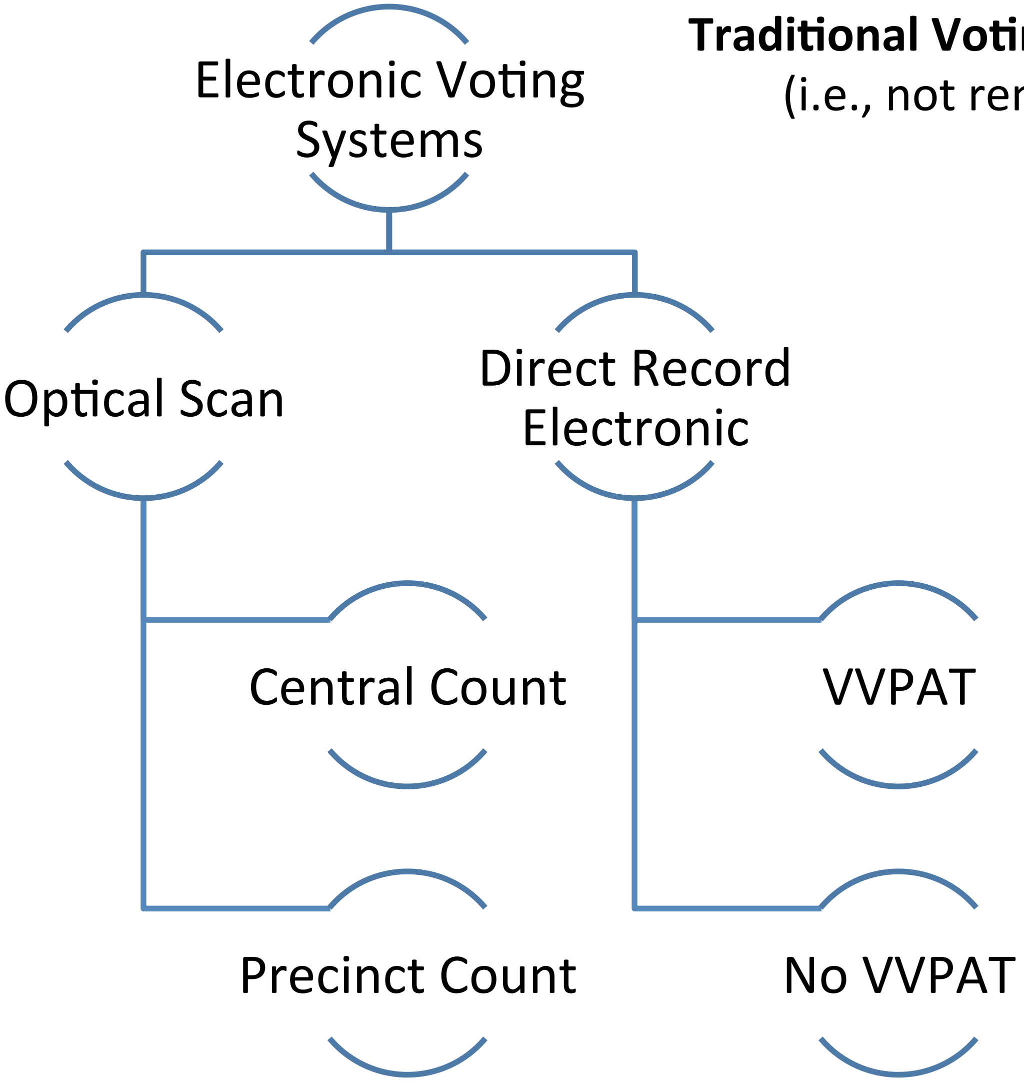


UPDATED MAY 11, 2012

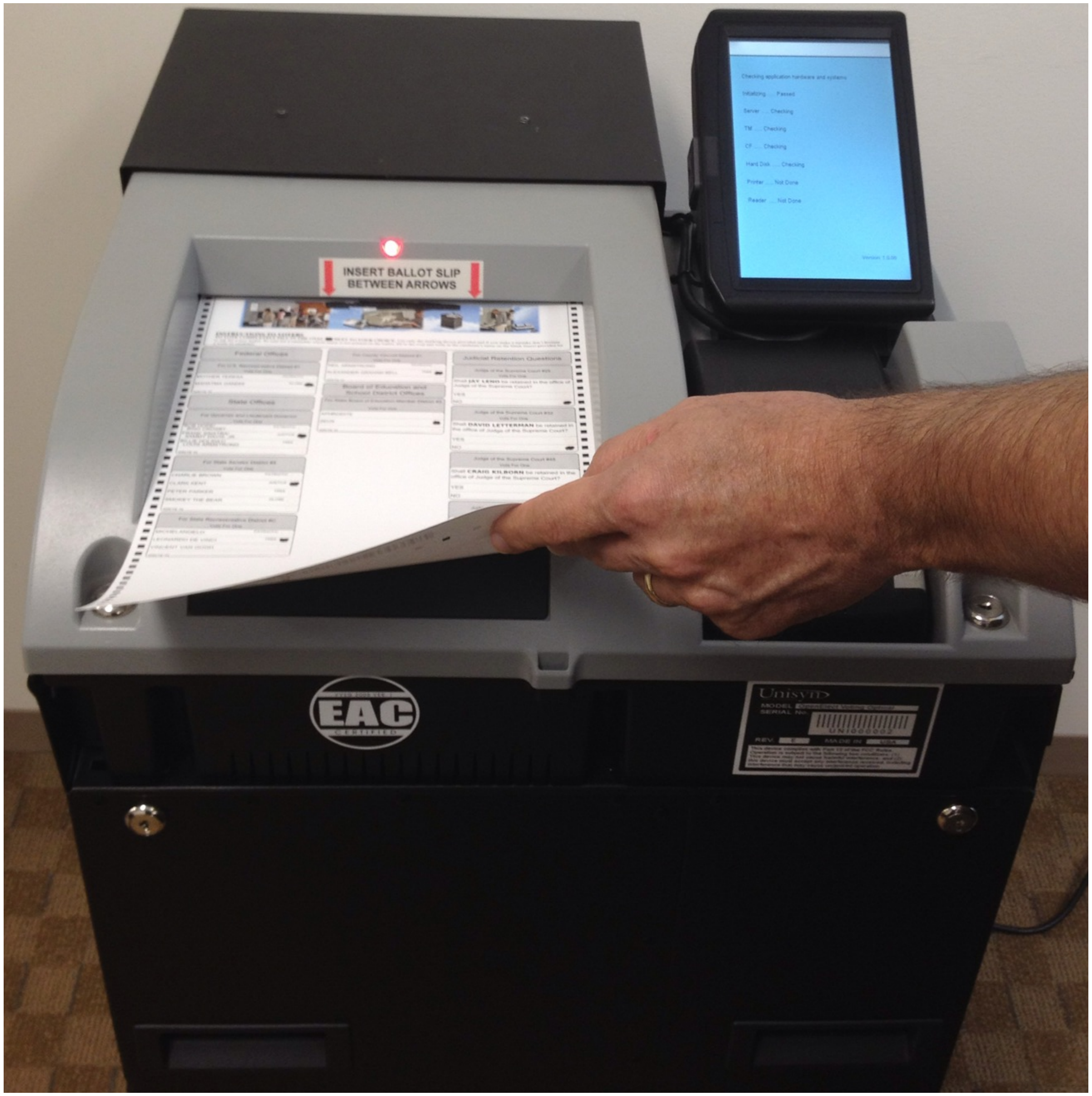
Source: www.sos.state.oh.us/

Voting System Taxonomy

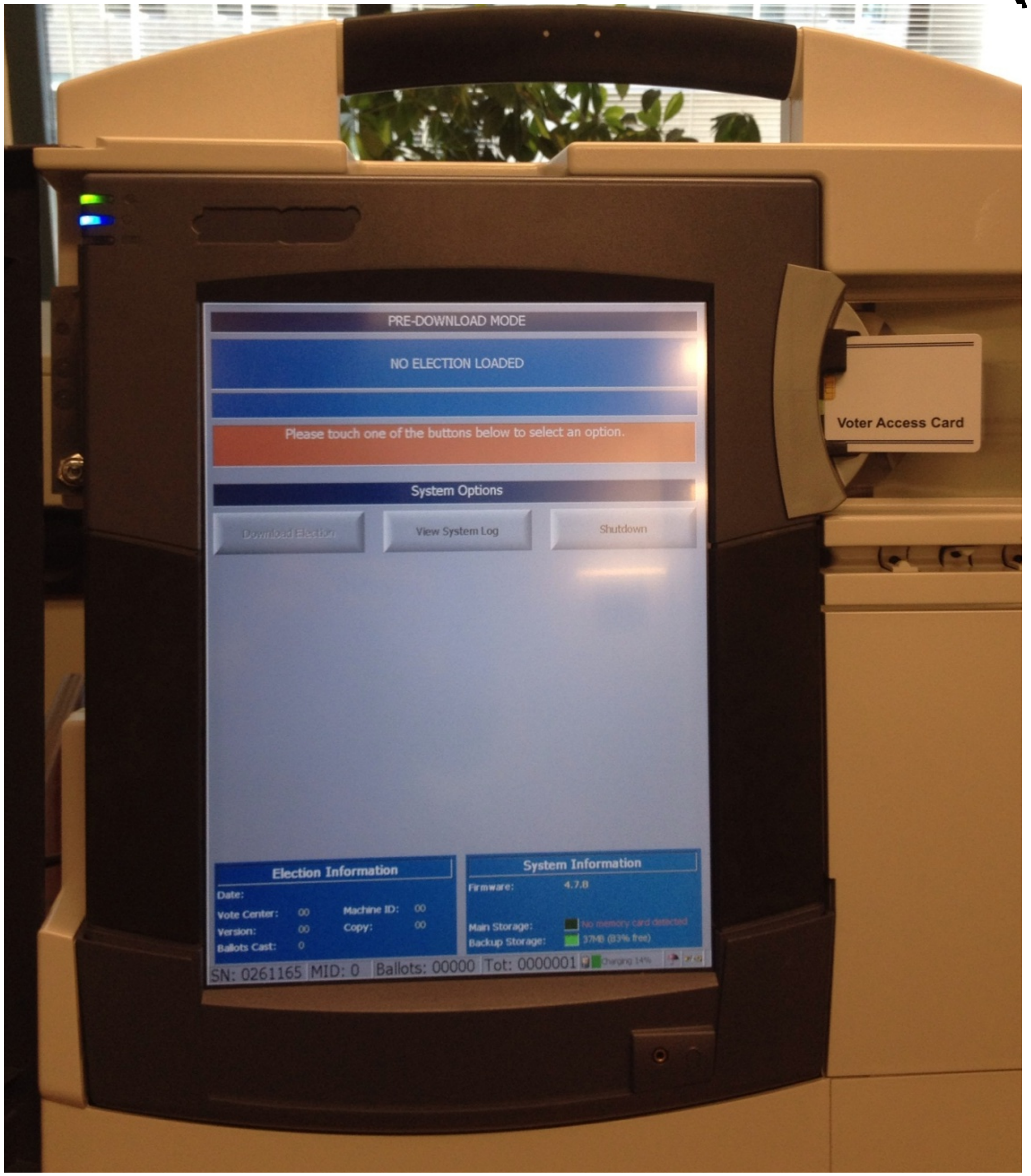
Traditional Voting/Polling Place
(i.e., not remote voting)



Optical Scan (OS)



Direct Record Electronic (DRE)



PRE-DOWNLOAD MODE

NO ELECTION LOADED

Please touch one of the buttons below to select an option.

System Options

Election Information

Date:

Vote Center: 00 Machine ID: 00

Version: 00 Copy: 00

Ballots Cast: 0

System Information

Firmware: 4.7.8

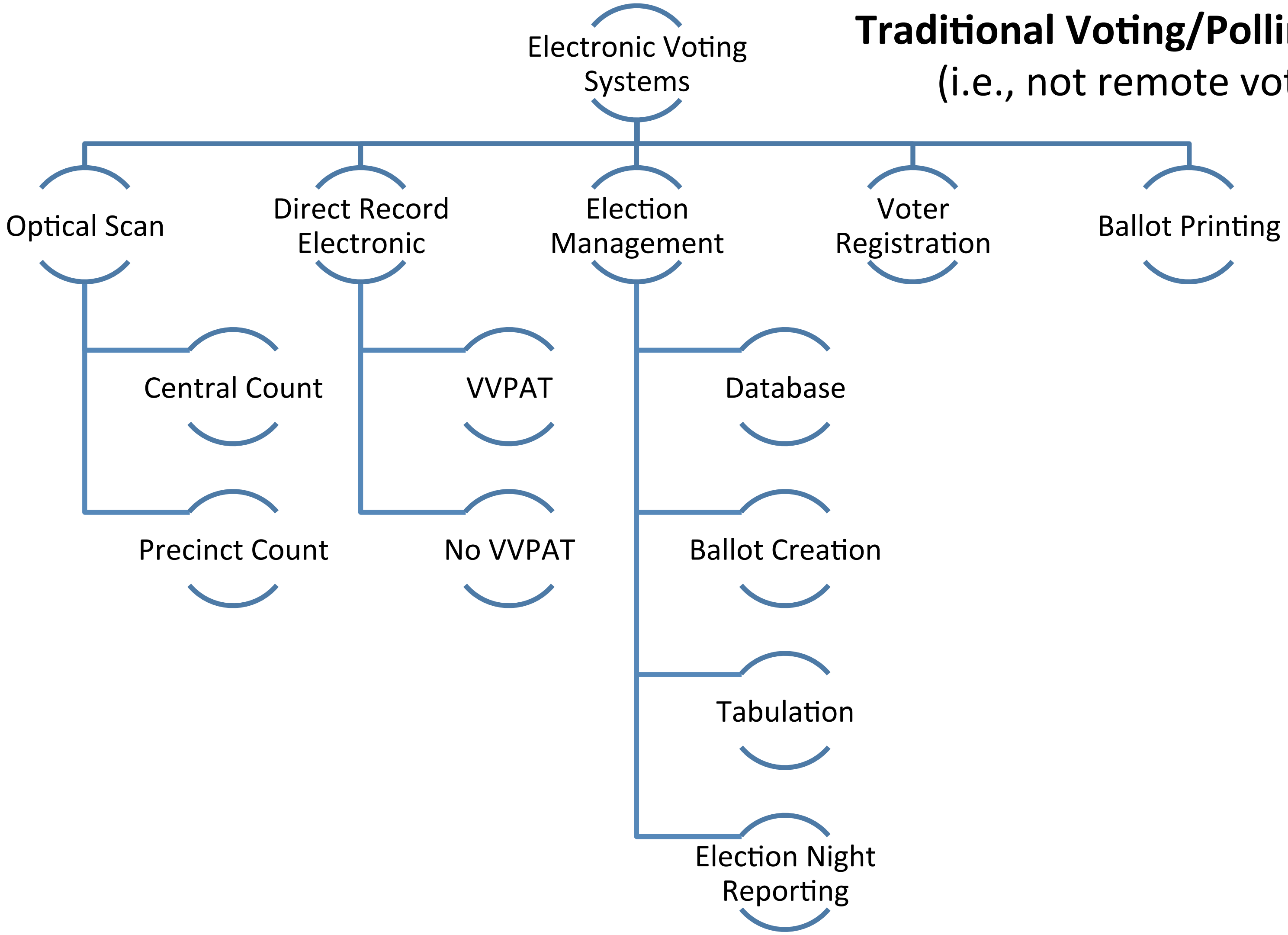
Main Storage: No memory card detected

Backup Storage: 37MB (83% free)

SN: 0261165 MID: 0 Ballots: 00000 Tot: 0000001 Charging 14%

Voting System Taxonomy

Traditional Voting/Polling Place
(i.e., not remote voting)



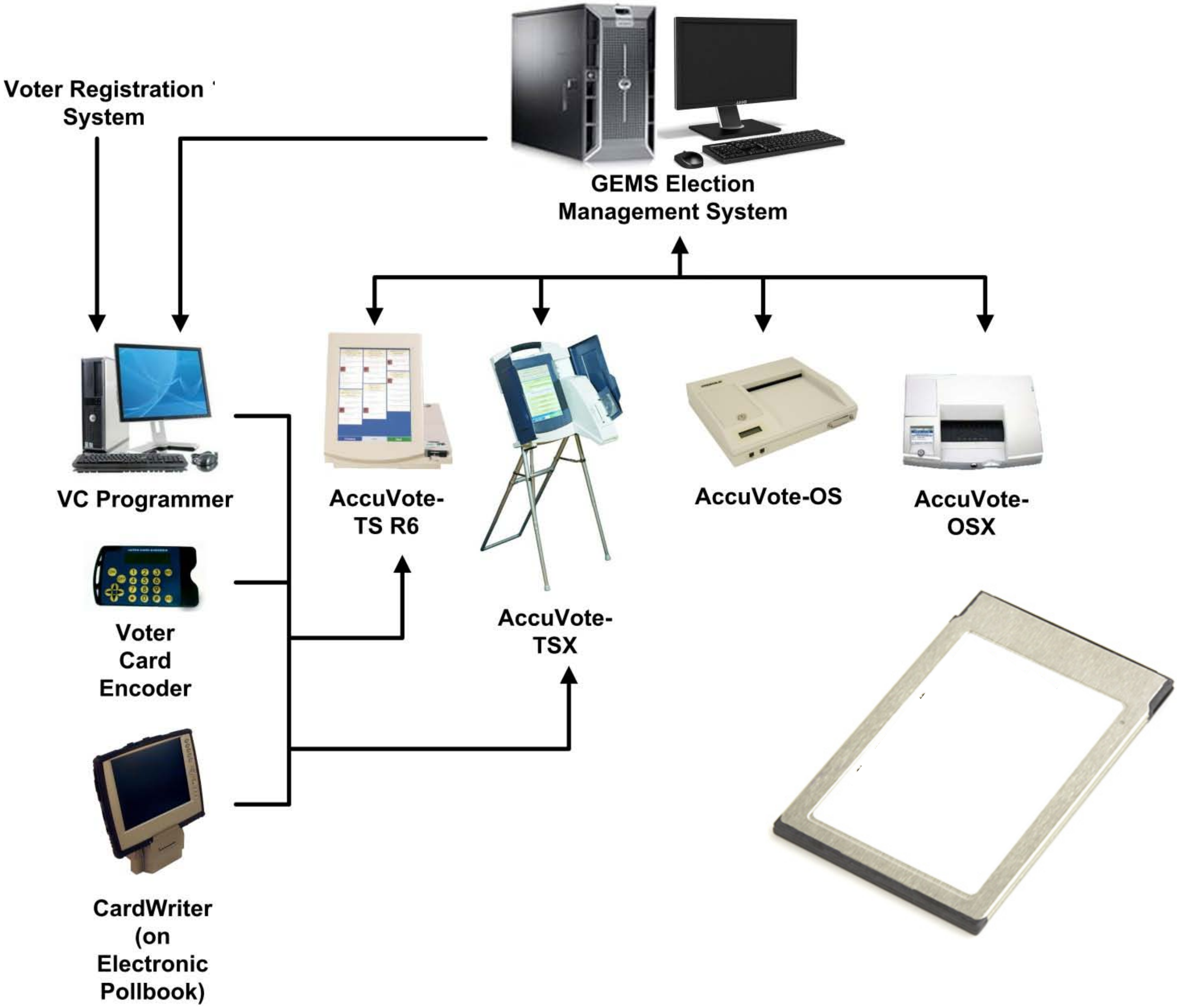
- Electronic Voting Systems
  - Optical Scan
    - Central Count
    - Precinct Count
  - Direct Record Electronic
    - VVPAT
    - No VVPAT
  - Election Management
    - Database
    - Ballot Creation
    - Tabulation
    - Election Night Reporting
  - Voter Registration
  - Ballot Printing

Example: Memory Devices

MEMORY CARD
Accu-Vote
PRECINCT IDENTIFICATION MEMORY CARD
RA-005
AccuVote
PRECINCT IDENTIFICATION MEMORY CARD
THIS SIDE UP
B20420

Source: www.eac.gov

Component Interactions



Voter Registration System

GEMS Election Management System

VC Programmer

Voter Card Encoder

CardWriter (on Electronic Pollbook)

AccuVote-TS R6

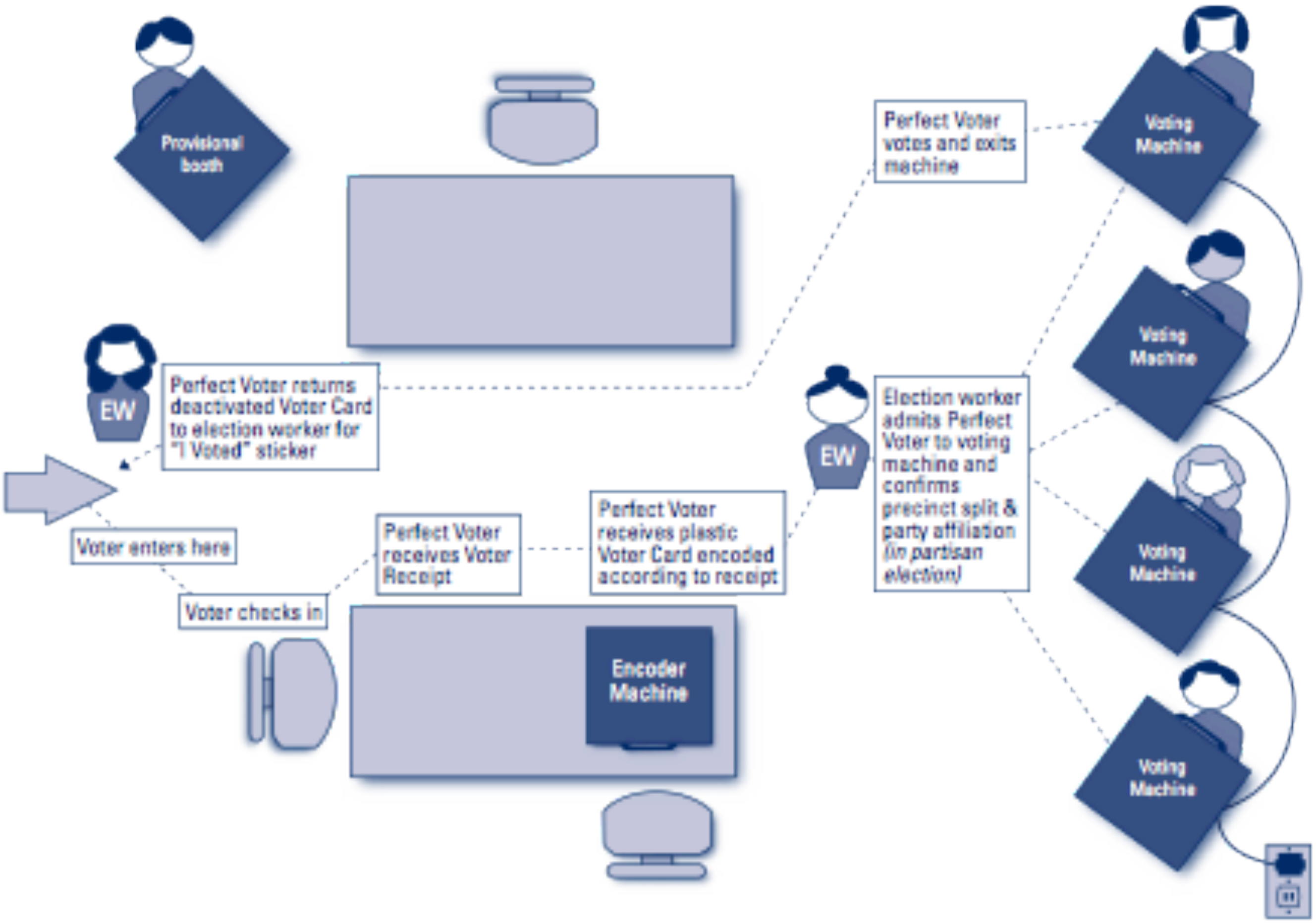
AccuVote-TSX

AccuVote-OS

AccuVote-OSX

Source: www.eac.gov (for diagram)
Source: www.printelect.com (for card)

Polling Place Layout



Voter enters here

Voter checks in

Perfect Voter receives Voter Receipt

Perfect Voter receives plastic Voter Card encoded according to receipt

Election worker admits Perfect Voter to voting machine and confirms precinct split & party affiliation *(in partisan election)*

Perfect Voter votes and exits machine

Perfect Voter returns deactivated Voter Card to election worker for "I Voted" sticker

Source: www.eac.gov

Background on TTBR & EVEREST

- NIST studied two “benchmark” state-sponsored vulnerability testing and analysis campaigns:
  - 2007 California Top To Bottom Review (TTBR)
  - 2007 Ohio EVEREST
- Goal of NIST Study:
  - Inform future federal voting standards in the area of Open Ended Vulnerability Testing (OEVT) , i.e. penetration testing
  - Identify methods and resources used in TTBR and EVEREST to assess voting system security
  - Make recommendations for future OEVT testing requirements in future federal voting standards

As part of this study, we cataloged exploitable software weaknesses identified in the (redacted) TTBR and EVEREST vulnerability reports

Systems Assessed in TTBR and EVEREST

- California TTBR (2007)
  - Premiere Election Solutions (formerly Diebold)
  - Hart InterCivic
  - Sequoia Voting Systems
  - InkaVote
- Ohio EVEREST (2007)
  - Premiere Election Solutions
  - ES&S
  - Sequoia

TTBR & EVEREST Team Composition

- Red Teams
  - Averaged 8 investigators per team/per system
  - PhD-level CS investigators min. 6 years experience in IT security
  - Source code “informed” red team penetration testing
- Source Code Analysis Teams
  - Averaged 7 investigators per team/per system
  - PhD-level CS investigators min. 6 years experience in IT security
  - Automated tool and manual source code review
- Documentation Analysis Teams
  - Averaged 2 Jurist Doctors (JD) with experience in election law and voting policy and procedures
  - Focused on document usability with respect to security and contingency handling
  - Also addressed system configuration management

Fundamental Principles in Team Analysis

- All teams based their vulnerability search upon 3 principles:
  - **Privacy of the voter and the voted ballot**
  - **Availability to vote**
  - **Integrity of the vote**
- Not to be violated
- Hardware, software, and documentation was explored to identify any vulnerabilities that may violate these principles

Vulnerability Reports

- NIST worked with the *redacted TTBR and EVEREST* vulnerability assessment reports.
- Information available in the reports included:
  - Summary of the vulnerability, along with the "end result" if the vulnerability is exploited
  - Impact (vote privacy, availability, integrity)
  - Attack prerequisites (access, knowledge, other weaknesses)
  - Attack scenario
  - Mitigation suggestions (procedural, implementation or design)
  - Confirmation status (yes/no) and verification method (e.g. source code review or penetration test)

National Institute of
Standards and Technology

Components with Reported Vulnerabilities

- Election Management Systems (EMS)
- Direct Record Electronic (DRE)
- Optical Scanner (OS)
- Memory Devices (MD)
  - Used to transfer electronic ballot definitions and vote results between machines and EMS

Exploitable Weaknesses

- ***Physical security –*** compromise of hardware security locks, panels or tamper proof devices on voting devices
- ***Poor use of , or lack of cryptography -*** Ineffective or insecure use, such as hard-coding static keys in software, insecure key management, lack of cryptography in communications or binding of files
- ***Poor implementation of cryptography -*** Use of older, insecure versions of cryptographic software packages
- ***Poor password use or lack of password –*** storing passwords with inadequate protection, hard coding passwords in software binaries, lack of password usage where appropriate
- ***Poor password implementation -*** Poorly implemented password scheme, permitting "guessing" of passwords including using known "default" passwords, or using the same password across all system devices or use of a weak password generation algorithms.

Exploitable Weaknesses

- ***Full system attacks*** - Potential for cascading viral propagation of malware attacks through removable storage media or via network propagation across the voting system
- ***Least privilege violations –*** execution of commands or having access to data beyond what is required for a particular class of voting system user, such as a poll worker being able to execute administrator-level commands
- ***Configuration –*** lack of vulnerability patching , OS security features turned off, undocumented software on the voting system, system or application event logging turned off
- ***Trust –*** implicit trust in a device without authentication, such as unauthenticated network communication between devices
- ***Auditing –*** lack of a voting application event logging capability, the capability to tamper with audit logs, or no authentication of audit logs
- ***Lack of defensive programming –*** no data input validation, failure to check for potential buffer overflows or integer overflows, poor or missing fault handling

Reported Weaknesses Expressed in CWE

- NIST catalogued unique exploitable weaknesses identified in TTBR and EVEREST
- We grouped a small number of those weaknesses (for this presentation) as follows:
  - Cryptographic Issues
  - Permissions, Privileges and Access Control
  - Omission of Security-relevant Information
  - Malware
  - Data Handling

CWE Mapping of Reported Weaknesses

CWE	Name	Voting Device	Description and Consequences
	Cryptographic Issues		
320	Key Management Errors	DRE	Manufacturer uses a commonly known, default static encryption keys in all of their DRE products. An attacker could use the information being leaked by the DRE unit to craft more specific attacks for the system.
319	Cleartext Transmission of Sensitive Data	EMS	Database queries and responses are transmitted in the clear (i. e. without encryption) and without authentication between EMS and the Microsoft SQL database. If EMS is a client (on a different computer), communication can be intercepted and altered in transit, with potential alteration of election database .
327	Use of a Broken or Risky Cryptographic Algorithm	EMS, MD	CRC used as a MAC: provides no defense against malicious tampering of memory device content. DES used in ECB mode is now obsolete and insecure.
321	Use of Hard-coded cryptographic key	DRE, OS, EMS	Cryptographic key material is permanently hardcoded into the source code or all devices. Attackers can possess the encryption keys for every county that utilizes that voting system and could craft attacks using that those keys: Undetected tampering with data on MD possible.

CWE Mapping of Reported Weaknesses

CWE	Name	Voting Device	Description and Consequences
	Permissions, Privileges and Access Control		
266	Incorrect Privilege Assignment	EMS	For every EMS user account, the system creates a corresponding account on the database server with full administrator privileges: Alternate channel access (e.g. a SQL client) gives EMS users ability to execute arbitrary SQL and system commands via EXEC statement.
287	Improper Authentication	OS, EMS	The connection between the EMS and OS device is unauthenticated: Allows "spoofing" an EMS to write to memory card fields on an OS.
	Omission of Security-relevant Information		
778	Insufficient Logging	EMS	Windows event logging was either disabled or in a very limited state: Preventing the identification of malicious activity.
	Malware		
509	Replicating Malicious Code (Virus or Worm)	EMS, MC	The introduction of malware into a DRE unit (via a Memory Cartridge) could spread virally from the DRE into the GEMS [EMS] server via format string errors in the EMS software: This scope of this attack could extend county-wide in an actual election.

CWE Mapping of Reported Weaknesses

CWE	Name	Voting Device	Description and Consequences
	Data Handling		
20	Improper Input Validation	DRE	Voter-accessible input fields on the DRE are susceptible to malicious input: Susceptibility to (at a minimum) a denial of service attack.
134	Uncontrolled Format String	DRE	Buffer overflows in unchecked string operation (sprintf) in DRE source code : Potential denial or service or arbitrary code execution.
22	Path Traversal	DRE	The DRE firmware is vulnerable to a directory traversal attack that can name, and hence overwrite, the files containing the boot loader and the system firmware.

How SoS of California Reduced Risk of Reported Vulnerabilities

- Decertified three Evoting systems and conditionally approved the fourth
- To be recertified, voting system manufacturers were required to develop a plan and procedures) to:
  - **"Air gap"** two parallel EMS 1 for election definition only, 1 solely for vote tabulation, a second solely for reading vote results from memory devices
  - **Provide a dedicated device** for reformatting memory cartridges before they are reconnected to the voting system
  - **Reformat disks, reinstall all OS and application software** on voting devices before every primary and general election
  - **Harden voting system configuration** – essential services, ports and software, least privilege for roles, audit logging, password policies, security updates and patching
  - **Increase security training for election poll workers** in storage, chain of custody , tamper seals, handling failures, logging events
  - **Address physical, network and data security**
  - **Separate roles and responsibilities**
  - **Prevent internet connectivity at any time**

National Institute of Standards and Technology

Conclusions

- Software security of Evoting systems in 2007 was poor
  - Older/weaker Evoting standards
  - Legacy systems not designed with security in mind
- Stronger Evoting standards are required
  - VVSG version 1.1 available for comment at http://www.eac.gov/open/comment.aspx
- OEVT is an effective testing methodology for assessing the security of Evoting systems
- Numbers and diversity of reported vulnerabilities in TTBR and EVEREST reports support this observation
- CWE ID would be a useful OEVT reporting requirement, providing a meaningful understanding of risk (e.g. likelihood of exploit, common consequences – scope and effect, related attacks, mitigations)

NIST

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Thank you.
Questions?

Michael Kass - michael.kass@nist.gov

Joshua Franklin - joshua.franklin@nist.gov