EAC Standards Board / Board of Advisors Meeting

December 12, 2007

Nelson Hastings
Barbara Guttman
National Institute of Standards and Technology
nelson.hastings@nist.gov
barbara.guttman@nist.gov

Agenda

- Background
- Software Independence
- Innovation Class
- Cryptography, Communication Security, and System Event Logging
- Open Ended Vulnerability Testing (OEVT)
- Other Security Requirements

Background

- The security requirements of the next VVSG work together to support equipment security
- Difficult to understand security provided by a single requirement or set of requirements without understanding how requirements relate to each other

Types of Security Controls

- Procedural verses Technical Controls
- Voting equipment requirements is about
  - Technical controls
  - Technical components used to realize management and/or operational (procedural) controls

Security Controls of VVSG

- General technical security controls
  - Based NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems
- Voting equipment specific technical security controls

Defense in Depth

- Strategy of multiple layers of defense are placed on a system
- Attackers should have to break through multiple defensive countermeasures in order to be successful

Software Independence

- TGDC Resolution 06-06 requires software independence (SI)
- Software Independence means that changes must be detectable
- Detectable, in practice, means auditable

SI = Auditable

Why Does the TGDC Want SI?

- With software, it is pretty easy to make a screen say one thing, but record another thing inside the computer.
- The hard part is making plausible, directed changes.

Auditing Records

- Two types of records
  - Electronic records
  - Independent records

How Does the VVSG Address Auditability?

- Requires equipment to have features that can be used for various types of audits
- Requires documentation
- NOTE – The VVSG itself does not require auditing – This is procedural and outside the scope.

Independent Voter Verifiable Records (IVVR)

- What is an independent voter verifiable record?
  - Direct verification by voter
  - Support for hand auditing
  - Various security and operational properties (can be rejected/durable)
- Doesn't this mean paper?

Independent Voter Verifiable Records (IVVR)

- Direct review (by voter & election official)
- Can support a hand audit
- Can support a recount
- Durable
- Tamper evidence
- Support for Privacy

Independent Voter Verifiable Records (IVVR)

- Public Format
- Sufficient Information (ballot configuration, not just selections)
- No codebook required
- Support for multiple physical media
- Able to be accepted or reject (per media)
- Non-human readable allowed (public format)

Independent Voter Verifiable Records (IVVR)

- Two current types of IVVR
  - Voter Verifiable Paper Audit Trail (VVPAT)
  - Optical Scan

Voter Verifiable Paper Audit Trail (VVPAT)

- VVPAT & Accessibility addressed by HFP
- Note need for observational testing
- Many operational requirements
- Paper rolls allowed

Voter Verifiable Paper Audit Trail (VVPAT)

- Components and definitions
- Printer/computer interactions
- Protocol of operations
- Human readable contents
- Linking electronic and paper records
- Paper roll privacy

Innovation Class

- All voting systems must be software independent (SI)
- 2 Paths:
  - Independent Voter Verifiable Record (IVVR)
    - Voter Verifiable Paper Record (VVPR)
    - Non paper
  - Innovation Class

Innovation Class

- Meet software independence (SI) without Independent Voter Verifiable Record (IVVR)
- Promote innovation
  - Better security
  - Better accessibility
  - Better usability

Innovation Class

- Innovation class (IC) procedures are role of EAC
- TGDC provided some advice:
  - Technologies must be new and different
  - Meet goal of fair, accurate, transparent elections
  - Meet all relevant VVSG requirements

Cryptography

- Powerful security technique
  - Information Integrity
  - Information Authentication
- Requirements developed to provide easy use and maintenance
  - Key management particularly
- Use strength of existing federal standards

Cryptography

- Cryptographic voting protocols (a.k.a End-to-End voting systems) not yet mature enough for standardization
- Many sections of the next VVSG leverage the security capabilities that cryptography provides

Cryptography

- FIPS 140-2 validated cryptographic module
- Minimum strength of cryptography
- Signature Module
  - A hardware cryptographic module
  - Generates digital signatures
  - Generates and stores private signature keys
  - Permanently attached to voting equipment

Cryptography

- Key management is critical in achieving the expected security properties of cryptography
  - Generation of keys - part of voting equipment setup process
  - Destruction of keys - part of election close out process for voting equipment
  - Distribution of keys - limited

Communication Security

- Protection of voting system communications
  - Transmission of information
  - Communications based threats
- No use of wireless technology
  - Exception for infrared technology

Communication Security

- Communication within polling place allowed
- No remote communication to voting devices during election day
  - Exceptions for devices used to transmit end of day results and communication with voter registration databases
  - However, these devices cannot be connected to other polling place devices

Communication Security

- Disable physical network interfaces when not required
- Monitor network interfaces for evidence of attack
- Integrity information for data via cryptography
- Mutual authentication between devices before exchange of information

Communication Security

- Limit communications to only devices that are required to communicate with each other
  - List of all network communication required for processes and applications
  - List of all network ports, shares, services, and protocols used

System Event Logging

- Provides accountability and supports the ability to reconstruct events and detect intrusions
- Electronic audit trail
  - Information to be generated
  - Integrity protection of the information
  - Management of system event log information

System Event Logging

- Log information must maintain voter privacy and ballot secrecy
- Basic log entry information
  - System Identifier
  - Event Identifier
  - Time Stamp
  - Result of event
  - When applicable, user that triggered event and requested resource

System Event Logging

- Time Stamp requirements
  - Format of time stamp
    - Day, month, and four digit year
    - Hours, minutes, seconds, and time zone
  - Clock drift
  - Limits on who can adjust clock

System Event Logging

- Minimum list of events to be logged
  - General system functions events
  - Authentication and access control events
  - Software events
  - Cryptographic events
  - Voting events

System Event Logging

- Management requirements
  - Default setting of system event log
  - Storage of log information in a publicly documented format such as XML
  - Event logs separable on an election and device basis
  - Retention of event log data from previous elections

System Event Logging

- Management requirements (continued)
  - Export of log information with digital signature
  - Log capacity management
  - Tools to view, analyze, and search system event log while on voting device
  - Halt vote capturing when system log malfunctions or is disabled
  - Limits on who can configure and clear system event logs

System Event Logging

- Protection of log information
  - Unauthorized access
  - Unauthorized modification
  - Unauthorized deletion
  - Integrity and availability protection of archived log information

Open Ended Vulnerability Testing(OEVT)

- Attempts to bypass the security of a system
- Discover flaws that could be used to
  - change the outcome of an election,
  - interfere with voters' ability to cast ballots or have their votes counted
  - compromise the secrecy of the vote

Open Ended Vulnerability Testing(OEVT)

- NOT a way to prove that a system is secure
- NOT bound by a pre-determined test plan
- Specific findings may differ between test teams
- Consistent framework for discussing flaws that are found

Open Ended Vulnerability Testing (OEVT)

- The test team
  - Figures out how the system works
  - Identifies the vulnerabilities – actual and potential
  - Attempts to break-in using a variety of different approaches

Open Ended Vulnerability Testing (OEVT)

- Team made up of security and election management experts
- Minimum of 12 staff weeks of testing
- Team given a voting device and associated technical data package (TDP) and user documentation

Open Ended Vulnerability Testing (OEVT)

- Team given a description of how significant plausible threats are addressed
- Team examines system within the context of a process model with plausible threats

Open Ended Vulnerability Testing (OEVT)

- Reasons for failure:
  - A violation of mandatory VVSG requirements
  - Inadequate means to mitigate a significant plausible known threat
  - Flaws that could be used to change outcome of election, compromise the secrecy of the vote, or interfere with voter's ability to cast ballot or vote counted

Open Ended Vulnerability Testing (OEVT)

- Report documents information associated with testing effort including
  - Threat scenarios considered
  - Threat scenarios identified but not investigated
  - Discussion of remaining vulnerabilities
  - Level of effort and qualifications of each team member

Other General Security Requirements

- Security Documentation
- Setup Inspection
- Software Installation
- Access Control
- System Integrity Management
- Physical Security

Security Documentation

- Technical Data Package
  - Provided to test lab to assist in the testing campaign
  - General security documentation about
    - Security Architecture
    - Security Threat Controls
    - Security Testing and Vulnerability Analysis
  - Detailed implementation specification for each security mechanism

Security Documentation

- User Documentation
  - Provided to user of the voting system
  - How security mechanism are to be used
  - Information needed to support security features

Setup Inspection

- Requirements related to the capabilities to inspect properties of voting devices
- Inspections generate system event log entries
- Software identification verification

Setup Inspections

- Software integrity verification
  - SI approach allows for internal verification
  - NO external interface requirement unlike VVSG 2005
- Voting device election information inspection
  - Generalized register and variable terminology from VVSG 2005
  - Support zero total inspections prior to use in election

Setup Inspection

- Inspection of properties of voting device components
  - Backup power supply level
  - Cabling connectivity indicator
  - Communications operational status and on/off indicators
  - Consumables remaining indicator
  - Calibration determination and adjustments

Software Installation

- Requirements related to the installation of software on voting devices
  - Including access and modification of configuration files
- Software installation generates system event log entries

Software Installation

- Digital signature verification of software before installation
  - National Software Reference Library (NSRL)
  - Designated repositories
- Externally visible alert when software installation fails

Software Installation

- Software installation only when in pre-voting state
- Limits on who can perform software installation
- Software to only be able to be installed using documented procedures

Access Control

- Supports the ability of the voting system to
  - Account for users actions
  - Limits use of resources
- Applies to individuals, applications, and processes of the voting system
- Requirements focus on
  - Logical access control
  - Technical aspects of physical access controls of the voting equipment

Access Control

- The management of three basic elements of access control
  - Identification - distinguishing between different users
  - Authentication - proving a user is who they claim to be
  - Authorization - permission to use a resource

Access Control

- Role identification
  - Required for voting devices and election management systems
  - Roles specified: Voter, Election Judge, Poll Worker, Central Election Official, and Administrator
- Individual identification
  - Required by election management systems

Physical Security

- Requirements to ensure that sufficient controls are in place to prevent undetected, unauthorized physical access.
- Requirements recognize use of a combination of procedures and physical countermeasures without prescribing either

Physical Security

- Unauthorized physical access must leave physical evidence
- Control and use procedures for door covers and panels must be sufficient to monitor access
- Ballot boxes must be tamper evident
- Physical locks and keys used for security purposes must meet UL standards and be tamper evident
  - They must also be keyed per System Owner's preference

Physical Security

- If the power disrupted or fails, physical countermeasures should not fail
- Control and use procedures for physical port access and least functionality must be sufficient to monitor access
  - Physical ports must be able to be manually disabled
  - Broken connections between components must result in automatically disabling the relevant port, setting off an alarm, creating an event log, and only re-enabling with appropriate authorization

System Integrity Management

- Security controls that do not fit into other sections of the VVSG
  - Boot, load, and execute process protection
  - Removable media interface protection
  - Backup and recovery capabilities
  - Malicious software protection