Technical Guidelines Development Committee
August 17, 2007, Plenary Meeting

Review of STS Modifications

Nelson Hastings
Electronics Engineer

Technical Guidelines Development Committee
August 17, 2007, Plenary Meeting

Agenda

- General Modifications
- Part 1: Equipment Requirements
  - Chapter 4: Security and Audit Architecture
    - Section 4.2 Requirements for Supporting Auditing
    - Section 4.3: Requirements on Electronic Records
    - Section 4.4: Independent Voter Verifiable Records (IVVR)
      - Section 4.4.1: General Requirements on IVVR
      - Section 4.4.2: VVPAT Systems
      - Section 4.4.3: PCOS Systems
  - Chapter 5: General Security Requirements
    - Section 5.1: Cryptography
    - Section 5.2: Setup Inspection
    - Section 5.3: Software Installation
    - Section 5.4: Access Control
    - Section 5.5: System Integrity Management

Technical Guidelines Development Committee
August 17, 2007, Plenary Meeting

Agenda

    - Section 5.6: Communications Security
    - Section 5.7: System Event Logging
    - Section 5.8: Physical Security
- Part 3: Testing Requirements
  - Chapter 2: Conformity Assessment Process
    - Section 2.4: Pre-Test Activities
      - Section 2.4.3: Initial System Build by Test Lab
      - Section 2.4.4: Unmodified COTS Verification
    - Section 2.6: Post Test Activities
      - Section 2.6.1.1: Voting System Software Version
      - Section 2.6.2: Software Distribution Requirements for Repositories, Test Labs, and Manufacturers
  - Chapter 5: Test Methods
    - Section 5.5 Open Ended Vulnerability Testing (OEVT)

General Modifications

- Harmonized language
  - Removed use of term “voting equipment”
  - Deleted “requirement” from short title of requirements
  - Changed references from “Vendors shall…” to “the manufacturer shall…”
  - Changed references from “Voting system test laboratory” or “VSTLs” to “test lab”
- Security documentation requirements moved to Part 2: Documentation Requirements
  - Chapter 3: Technical Data Package (TDP)
    - Section 3.5 System Security Specification
  - Chapter 4: Voting Equipment User Documentation
    - Section 4.3 System Security Specification

Security and Audit Architecture: General Changes

- Part 1, Chapter 4, page 66
- Single chapter “Security and Audit Architecture” that covers the following chapters from May 2007 version:
  - Volume III, Chapter 4: Security and Audit Architecture Requirements now in Part 1, Chapter 4
  - Volume III, Chapter 5: Electronic Records Requirements now in Part 1, Section 4.3
  - Volume III, Chapter 6: Voter Verified Paper Records (VVPR) Requirements now in Part 1, Section 4.4.2 and 4.4.3
    - Subsections of Section 4.4: Independent Voter Verifiable Record (IVVR) of the new chapter
    - Section 4.4.2: Voter Verifiable Paper Audit Trail (VVPAT) systems
    - Section 4.4.3: Precinct Count Optical Scan (PCOS) systems

Security and Audit Architecture: General Changes

- Eliminated
  - Duplicate material in Electronic Records and IVVR/VVPR
  - Election administration descriptions from requirements
    - Removed description of “how to” for auditing steps
    - Each step starts with high-level requirements as a SHALL statement
- OEVT is no longer primary testing method
  - High-level requirements scope OEVT team activities

Audit Steps Removed and Retained

- Part 1, Chapter 4, Section 4.2, page 66
- Eliminated parallel and spot parallel testing
  - Existing procedures (California) don't require any equipment requirements
  - Use of voter-verifiable records/Software Independence eliminates need for aggressive, expensive parallel testing
- Retained pollbook audit, hand-audit, and ballot count and vote total audit
  - Impose requirements on equipment
  - Different audit support each other.
- Retained observational testing
  - Required for achieving Software Independence for the Accessible Voting System
  - Imposes equipment and documentation requirements

Electronic Records

- Part 1, Chapter 4, Section 4.3, page 72
- Cleaned up requirement text and fixed terminology
  - Coordinated terminology with glossary
- Removed overlap with Cryptography section
- Separated final reports (in CRT) from audit records produced throughout the voting process
  - For example, the Tabulator Summary Count Record (Part 1, Chapter 4, page 74) could be used to support a hand audit of a DRE+VVPAT

Independent Voter Verifiable Records (IVVR)

- Part 1, Chapter 4, Section 4.4, page 81
- High level requirements for independent voter verifiable records (IVVR)
  - Added to allow non-paper based voting systems to conform
  - Consistent with TGDC Resolution #06-06: Software Independence of Voting Systems
  - Based on the voter verified paper records (VVPR) requirements which were eliminated
  - Do not effect the Voter Verifiable Paper Audit Trail (VVPAT) and Precinct Count Optical Scan (PCOS) requirements

Independent Voter Verifiable Records (IVVR)

- A single IVVR record needs to be created that meets the general requirements
- Current general IVVR requirements 4.4.1-A through 4.4.1-K (Part 1, Chapter 4, page 82-87)
  - **Renumber** to 4.4.1-B through 4.4.1-L
  - **Replace**: "create records" with "create a record"
- 4.4.1-A Independent voter verifiable record creation - **to be added**
  - The voting system shall create an independent voter verifiable record.
  - Discussion: While multiple copies of a voter's choices may be kept, there must be a single record that satisfies 4.4.1-B through 4.4.1-L

Voter Verifiable Paper Audit Trail (VVPAT)

- Part 1, Chapter 4, Section 4.4.2, page 87
- Updated machine readability requirements
  - Paper records must be OCR readable
  - Non-human-readable encodings must be in a publicly available format
- No codebooks required to interpret paper record
  - Implied in requirements before; made explicit
- Voter rejection of VVPAT changed
  Two tunable parameters set by election officials:
  - Number of times voter may reject paper record without intervention by election official
  - Number of times paper record may be rejected on one voting machine without intervention by election official

Voter Verifiable Paper Audit Trail (VVPAT)

- Cut-sheet VVPAT may split CVR across pages
  - Each sheet must be accepted or rejected independently
  - Ballot questions must never be split across pages
- CVR correspondence between electronic and paper records:
  - Minor fixes to requirements when capability enabled
  - Election officials may turn it on/off

Precinct Count Optical Scan (PCOS)

- Part 1, Chapter 4, Section 4.4.3, page 101
- Eliminated requirements to support batching of paper records

Cryptography

- Part 1, Chapter 5, Section 5.1, page 103
- Changed the term “audit records” to “election records”
- Discussed the impact of a voting device in a multi-precinct polling place or polling center
  - Do **not** need multiple election keys for a voting device
  - When a voting device supports multiple precincts, the device needs only a single election key

Setup Inspection

- Part 1, Chapter 5, Section 5.2, page 114
- Removed requirements for software verification by external hardware device
- System Integrity Management requirements meet the need for software verification
  - Software integrity verification on boot up and loading into memory before execution using a tamper resistant hardware module
- Refocused chapter on the inspection (versus verification) of voting device properties
  - Changed chapter name from "Setup Validation Requirements" to "Setup Inspection"
  - Introduction was rewritten to reflect new chapter focus
- Eliminated the terms "registers" and "variables"
  - Inspection of storage locations that hold election information

Software Installation

- Part 1, Chapter 5, Section 5.3, page 120
- Refocused chapter to only software installation capabilities
  - Renamed chapter from "Software Distribution and Installation Requirements" to "Software Installation"
  - Introduction was rewritten to reflect new chapter focus
  - Removed background section and distributed information as needed
  - Moved software build requirements to Part 3: Testing Requirements, Section 2.4.3: Initial System Build by Test Lab
    - Changed term "witness build" to "test lab build"
  - Moved software distribution requirements to Part 3: Testing Requirements, Section 2.6.2: Software Distribution Requirements for Repositories, Test Labs, and Manufacturers
    - Removed software distribution requirements related to jurisdictions

Technical Guidelines Development Committee August 17, 2007, Plenary Meeting

Access Control

- Part 1, Chapter 5, Section 5.4, page 126
- Refocused requirements to administrator authentication
  - Voter authentication related requirements moved to e-pollbook requirements
  - Remote administration of voting devices not allowed, so remote access control requirements removed
- Re-scoped requirements
  - Added "if possible by the voting system architecture" clause to access control requirements to allow for limited resource systems since May 2007 and part of the August 7th version
  - STS proposes having minimum levels of identification and authentication for all voting systems
    - All voting devices must be able to identify and authenticate at least to general role(s)
    - Election management systems must be able to identify and authenticate down to an individual

Access Control

- 5.4.1-A Access control mechanisms - Part 1, Chapter 5, page 127
  - The voting device shall provide access control mechanisms designed to permit authorized access to the voting system and to prevent unauthorized access to the voting system.
- 5.4.1-A.1 Voting device access control - **to be added**
  - The access control mechanisms of the voting device shall be capable of identifying roles permitted to perform operations on the voting device.
- 5.4.1-A.2 EMS access control - **to be added**
  - The access control mechanisms of the EMS shall be capable of identifying individuals permitted to perform operations on the EMS.
- **Remove** “if possible by the voting system architecture” clauses not related to access control

Access Control

- Re-scoped requirements (continued)
  - Changed “Applies to” field from “Voting system” to
    - “Voting device”
    - “Vote capture device” and
    - “EMS”

System Integrity Management

- Part 1, Chapter 5, Section 5.5, page 140
- Software integrity verification on boot up and loading into memory before execution using a tamper resistant hardware module supports the refocusing of the setup validation chapter
- Several requirements covered by other chapters deleted
- Re-scoped malicious code detection (real-time) and backup and recovery requirements
  - Changed “Applies to” field from “Electronic device” to “Election management system”
- Re-scoped the logical separation of applications requirement
  - Added clause “if possible by the voting system architecture”
  - Allows voting system architectures without logical separation of applications capabilities

Communications Security

- Part 1, Chapter 5, Section 5.6, page 146
- Deleted requirement related to limiting remote activities
  - Remote access is not allowed
  - Access control remote access requirements removed
- Deleted requirement related to limiting the number of active network interfaces
  - Covered by requirements documenting required ports and disabling of ports when not used
- Added new requirements related to an “air gap” between networked voting devices at a polling site and polling site devices networked externally to the site

System Event Logging

- Part 1, Chapter 5, Section 5.7, page 154
- Re-scoped requirements
  - Changed “Applies to” field from “voting system” to “programmed device”
- Added clause “if possible by the voting system architecture” to security requirements related to information to be logged
  - Allows voting system architectures without full logging capabilities due to resource constraints
- Added to the list of items to be logged
  - Opening polls
  - Closing polls
  - Casting a vote

Physical Security

- Part 1, Chapter 5, Section 5.8, page 166
- Requirements 5.8.7, 5.8.8, and 5.8.9 were added or modified to address comments from the TGDC on locks
  - Locks that are used for security purposes must meet UL standards and locks which are not used for security purposes, if bypassed, must not give access to critical components.
- Requirement 5.8.5-A statement clarified
  - In addition to locks, allows for tamper evident or tamper resistant countermeasures to be used to protect access points (panels and covers)
- Source references put into standard format

Pre-Test Activities

- Added Section 2.4.3: Initial system build by test lab
  - Part 3, Chapter 2, page 8
  - “Witness build” requirements moved from Chapter 9: Software Distribution and Installation of the May version of document
  - Changed the term “witness build” to “test lab build”
- Added Section 2.4.4: Unmodified COTS verification
  - Part 3, Chapter 2, page 18
  - Created new requirements for determining use of unmodified COTS by the voting systems
  - Requirement based on approach agreed upon by CRT and STS
    - Manufacturer provide voting device without COTS products
    - Test lab obtains COTS products from usual sources
    - Test lab integrates COTS products with manufacturer provided voting device

Post-Test Activities

- Added Section 2.6.1.1: Voting system software version
  - Part 3, Chapter 2, page 25
  - Created requirements for test lab build of voting system software after the test campaign
- Added Section 2.6.2: Software distribution requirements for repositories, test labs, and manufacturers
  - Part 3, Chapter 2, page 26
  - Software distribution requirements moved from Chapter 9: Software Distribution and Installation of the May version of document
  - Removed software distribution requirements related to jurisdictions

Open Ended Vulnerability Testing

- Part 3, Chapter 5, Section 5.4, page 83
- Enumerated requirements in current version
- Scope, focus and priorities of OEVT
  - Examination of voting device and vendor supplied use procedures
  - Access to entire Technical Data Package
- OEVT team composition
  - At least 3 security experts and at least one election management expert
  - Team knowledge base
- Rules of engagement
  - Process model describing a specific implementation of the voting system
  - Plausible threats

Open Ended Vulnerability Testing

- Level of effort and failure criteria
  - Minimum of 12 staff weeks
  - Failure to meet a mandatory requirement
  - Critical flaws
    - Change the outcome of an election
    - Interfere with ability to cast ballots or count votes
    - Compromise secrecy of the vote
- Reporting requirements