Technical Guidelines Development Committee
May 21-22, 2007, Plenary Meeting

Review of STS changes from the March 2007 TGDC meeting

Nelson Hastings
Electronics Engineer

Overview

- General Update
- Cryptography Requirements
- Setup Validation Requirements
- Software Distribution and Installation Requirements
- Access Control Requirements
- System Integrity Management Requirements - NEW
- Communications Requirements - NEW
- System Event Logging Requirements
- Physical Security Requirements - NEW
- Security Documentation Requirements - NEW

General Update

- Requirements distributed to STS for review and comment
  - Exceptions: System Integrity Management and Communications
  - Major modifications discussed with STS and other subcommittees (as needed) before changes made
- Harmonization with other parts of the guidelines
- Modified fields: “Applies to”, “Test References”, “Sources”, and “Impact”

Cryptography Requirements

- NO MODIFCATIONS
- A FIPS 140-2 hardware cryptographic module for each voting system
  - Election management systems (EMS)
  - Vote capture devices
- Key management
  - Long term key associated with the equipment
  - Election specific key

Setup Validation Requirements

- MODIFIED
- Software verification via an external device requirement
  - Election management systems (EMS)
  - Networked vote capture devices
    - Vote capture devices are considered networked if they communicate with more than one election management system or other vote capture device.
    - Non-networked vote capture devices still must support the general requirement of verifying software installed on the device but can use verification techniques that do not require a separate verification device.

Software Distribution and Installation Requirements

- MODIFIED
- Requirements added
  - Build of previously certified voting system software
  - Replication of voting equipment configuration
- Many requirements are procedural in nature
  - Vendors, Voting System Testing Laboratories (VSTLs), and Repositories
  - Jurisdictions
- Recently distributed to STS for review and comment

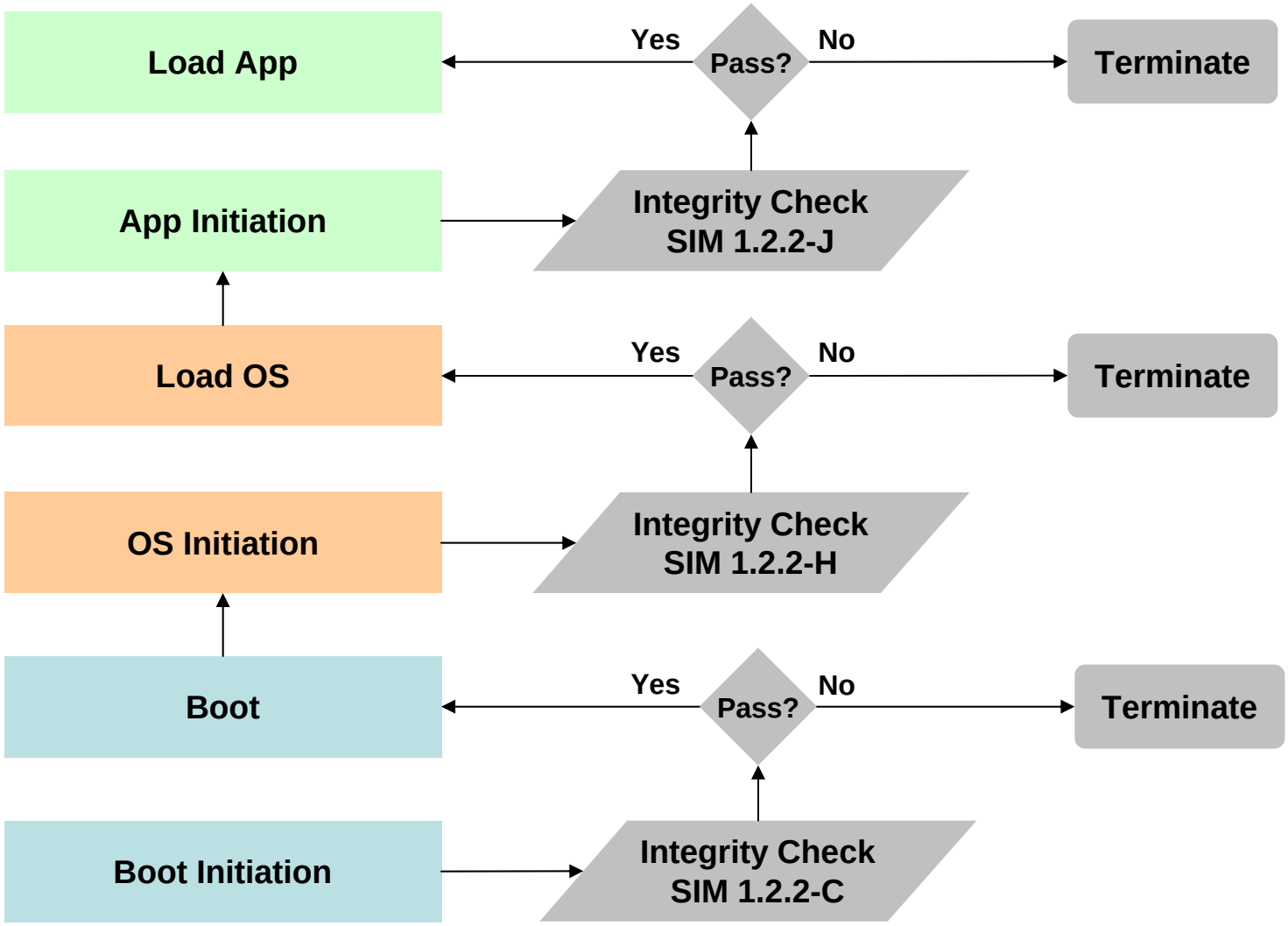
Access Control Requirements

- NO MODIFICATION
- Requirements being updated
  - Based on feedback received from STS
  - General purpose verses limited operating system environments
  - “Applies to” fields of requirements to limit scope where appropriate

System Integrity Management Requirements

- NEW
- Requirements related to
  - Initiation integrity checks at different points
    - Initiation check of boot before booting the equipment
    - Initiation check of operating system before loading of operating system
    - Initiation check of voting application software before loading of voting application software

Technical Guidelines Development Committee
May 21-22, 2007, Plenary Meeting



System Integrity Management Requirements

  - Monitoring of the voting equipment
    - Software integrity checks
    - Restricting execution of processes
    - Mal-ware/Virus scanning
  - Limiting execution of software stored on removable media
    - No automatic execution of software
    - Authentication of removable media
- Working to scope requirements appropriately based on concerns of equipment capability
  - General purpose verses limited operating systems
- To be distributed to STS for review and comment

Communication Requirements

- NEW
- No wireless except for inferred with shielded signal path
- Introduction of three level communication model
  - Physical Level - communication medium used
  - Network Level - communication protocol used
  - Application Level - communication between different applications
- Requirements developed based on securing different levels within the communication model

Communication Requirements

- Most requirements for network and application level
  - Unique identifiers of network interfaces
  - Authentication of network data packets (i.e. SSL, TLS)
  - Monitoring of inbound and outbound network traffic
- Working to scope requirements appropriately based on concerns of equipment capability
  - General purpose verses limited operating systems
- To be distributed to STS for review and comment

System Event Logging Requirements

- NO MODIFICATION
- Requirements being updated to address scoping concerns
  - General voting events that must be logged (manually or automated)
    - Open and close of polls
    - Result of zero total check
    - Changes to cryptographic keys
  - Events logged based on the capability of the voting equipment (automated)
    - Authentication events
    - Database connection events

Physical Security Requirements

- NEW
- Developed requirements resulting in tamper evidence and disabling physical ports of voting equipment
- Lock requirements
  - Strength based on UL 437 standard
  - Key Management
    - Unique key NOT required for each piece of voting equipment
    - Equipment must be able to supplied with a unique key for a jurisdictions' equipment
    - Allows for the ability of jurisdictions to have a unique key for their equipment, but does not prohibit the use of a common key across jurisdictions

Security Documentation Requirements

- NEW
- Created Security Documentation section
  - Two general high level requirements
  - Access Control documentation requirements
  - Place holder for other low level security related documentation requirements

Overall Security Documentation Requirement

Vendors shall document in the TDP all aspects of system design, development, and proper usage that are relevant to system security. This includes, but is not limited to the following:

- System security objectives
- All hardware and software security mechanisms
- Development procedures employed to ensure absence of malicious code
- Initialization, usage, and maintenance procedures necessary to secure operation
- All attacks the system is designed to resist or detect
- Any security vulnerabilities known to the vendor.

High Level Security Documentation Requirement

Vendors shall provide at a minimum the high level documents listed in Table 1 as part of the TDP.

- Security Threats Controls document that identifies the threats the voting system protects against and the implemented security controls on voting system and system components.
- Security Architecture document that provides an architecture level description of how the security requirements are met, to include the various authentication, access control, audit, confidentiality, integrity, and availability requirements.
- Security Testing and Vulnerability Analysis document that describe security tests performed to identify vulnerabilities and the results of the testing including testing performed as part of software development, such as unit, module, and subsystem testing.

High Level Security Documentation Requirement

- Interface Specification document that describes external interfaces (programmatic, human, and network) provided by each of the computer components of the voting system (examples of components are DRE, Central Tabulator, Independent Audit machine).
- Design Specification document that provides a high-level design of each voting system component.
- Development Environment Specification document that provides descriptions of the physical, personnel, procedural, and technical security of the development environment including configuration management, tools used, coding standards used, software engineering model used, and description of developer and independent testing

Discussion