Technical Guidelines Development Committee
March 22, 2007, Plenary Meeting

Security Requirements:
Progress Report

Overview

- Draft requirement development process
- Status of security requirements
- Discussion

Requirement Development Process

- Draft requirements created based on TGDC resolutions and telecons
- Distributed to NIST staff for review
  - Draft requirements revised based on comments
- Distributed to Security and Transparency Subcommittee (STS) for review
  - Draft requirements revised based on comments
- Distributed to TGDC for review
  - Draft requirements revised based on comments

Security Requirements Status

- Physical Security
- System Integrity Management
- Innovation Class
- Security Documentation
- Software Distribution & Installation
- System Event Logging
- Access Control
- Setup Validation
- Auditing
- Cryptography

Physical Security Requirements

- Requirements developed since December TGDC meeting
  - Tamper proof seals
  - Physical keys
  - Door cover and panels
  - External ports
  - Encasements
- In the process of being reviewed by NIST staff
- To be distributed to STS for review

System Integrity Management Requirements

- Requirements developed since December TGDC meeting
  - Communication security
  - Malicious software protection
  - Platform configuration
  - Error conditions

System Integrity Management Requirements

- Requirements need to be
  - Mapped to VVSG 2005 requirements for impact analysis
  - Harmonized with security and non-security related requirements
- In the process of being reviewed and updated by NIST staff
- To be distributed to STS for review

Innovation Class

- Initial requirements being researched and developed
  - High level requirements
  - Entry criteria
- Working with EAC to address how innovation class system could be certified
  - Integration with EAC testing and certification program
  - How are innovative techniques to be reviewed and tested?
- Discussion paper recently distributed to STS for review

Security Documentation Requirements

- High level requirements developed since December TGDC meeting
  - Requirements needs to be polished and mapped to VVSG 2005 requirements for impact analysis
- Low level requirements developed as part of specific security topics
  - To be consolidated as security topics become stable

Security Documentation Requirements

- General documentation
  - Security architecture and threats
- Technical documentation
  - Related to design and implementation
- Users documentation
  - Related to how to use voting equipment features
  - Includes assumed policies and procedures
- To be distributed to STS for review

Software Distribution and Installation Requirements

- Requirements developed since December TGDC meeting
  - Creation of software distribution packages master copies
  - Witness build of software
  - Digital signatures requirements for software creation and installation
  - Types of repositories based on service provided
  - Access control for software installation
  - Limit software installation to pre-voting mode
- Requirements need to be
  - Mapped to VVSG 2005 requirements for impact analysis
  - Harmonized with security and non-security related requirements
- Recently distributed to STS for review

System Event Logging Requirements

- Requirements developed since December TGDC meeting
  - Events to be captured by log
  - Log entry information
  - Log protection by use of cryptography
  - Log management

System Event Logging Requirements

- Distributed to STS for review
  - Updated based on feedback received
    - Added event to be logged in tabular form
  - How configurable should system event logging be?
    - General purpose operating systems have these capabilities
    - Limited (single process/user) operating systems may not have these capabilities
    - STS working on how to scope these requirements appropriately
- Once scoping issue addressed, to be re-distributed to STS for review

Access Control Requirements

- Requirements updated since December TGDC meeting
  - Authentication mechanisms
  - Enforcement mechanisms
  - Management of identities and rights
  - Limitation of rights during voting modes and accessed remotely
- Mapped to requirements in VVSG 2005 for impact analysis
- Reviewed impact of software independence: NONE

Access Control Requirements

- Distributed to STS for review
  - Updated based on feedback received
  - Why should the access control policy be so configurable?
    - General purpose (multi process/user) operating systems have these capabilities
    - Limited (single process/user) operating systems may not have these capabilities
    - STS working on how to scope these requirements appropriately
- Once scoping issue addressed, to be re-distributed to STS for review

Setup Validation Requirements

- Requirements updated since December TGDC meeting
  - Software identification and verification
  - Register and variable inspection
  - Other voting equipment property inspections
    - Backup power supply
    - On/off status of communications
    - Components requiring calibration
    - Equipment consumables
- Mapped to requirements in VVSG 2005 for impact analysis

Setup Validation Requirements

- Reviewed impact of software independence
  - Software identification requirements: NONE
  - Software verification requirements: SOME
    - External verification required for election management systems and networked vote capture devices are acceptable
      - External interface to installed software required
    - Internal verification acceptable for non-networked vote capture devices
      - External interface to installed software not required

Setup Validation Requirements

- Distributed to STS for review
  - Updated based on feedback received
  - Discussed merits of reducing requirement granularity
    - Cryptographic based technique requirements to be included
    - Non-cryptographic based technique requirement to be eliminated
- To be re-distributed to STS for review

Auditing Requirements

- Focuses on achieving software independence through auditing
- Requirements developed since December TGDC meeting
  - Equipment capabilities to support auditing
  - Electronic record requirements
  - Paper record requirements
- Recently distributed to STS for feedback

- Separate Presentation on this topic

Cryptography Requirements

- Requirements updated since December TGDC meeting
  - Eliminate tutorial of cryptography
  - Use of FIPS 140-2 validated cryptographic modules
  - Key management requirements
- Recently distributed to STS for feedback

- Separate Presentation on this topic

Discussion