

Technical Guidelines Development Committee
April 20, 2005 Plenary Meeting

Software Distribution and Setup
Validation Requirements

Nelson Hastings

National Institute of Standards and Technology

TGDC Meeting, April 20, 2005

Technical Guidelines Development Committee

April 20, 2005 Plenary Meeting

Overview

- Background
- Software Distribution Methodology Requirements
- Reference Information Requirements
- Setup Validation Methodology Requirements
- Discussion

Technical Guidelines Development Committee

April 20, 2005 Plenary Meeting

Background

- TGDC Resolution 15-05: Software Distribution
 - To determine whether the identified voting system software has been distributed without modification
- TGDC Resolution 16-05: Setup Validation
 - To ensure voting systems contain only authorized voting system software, have no unauthorized software installed, and are in the proper initial state

Technical Guidelines Development Committee

April 20, 2005 Plenary Meeting

Background

- Two original documents combined to form one section
- Detailed analysis of scope and approach removed to improve readability
- Refinement and addition of requirements
- Correspondence of requirements to VSS and IEEE not included to reduce complexity but considered during development

Software Distribution Requirements

- Vendor documentation to enumerate all software including third party software required by the voting equipment (6.0.4.1.1)
 - Detailed information to be documented (6.0.4.1.1.1)
 - Software files that never change, change based on the election, or change during ballot casting are identified. (6.0.4.1.1.2)

Software Distribution Requirements

- Testing authorities to the witness of the final build of the qualified voting system software (6.0.4.1.2)
 - Complete record of the final build (6.0.4.1.2.1)
 - Source code and executables placed on write once media with unique labeling (6.0.4.1.2.2)
 - Records kept by testing authority until de-qualification of voting system (6.0.4.1.2.3)

Software Distribution Requirements

- Testing authorities distribution subset of the final build record (6.0.4.1.2.4)
 - Only build executables and installation programs placed on write once media with unique labeling (6.0.4.1.2.4 and 6.0.4.1.2.5)
 - Vendors, NSRL, and other repositories receive copies (6.0.4.1.2.6)
 - Subset of record kept by testing authority until de-qualification of voting system (6.0.4.1.2.7)

Technical Guidelines Development Committee

April 20, 2005 Plenary Meeting

Software Distribution Requirements

- Vendor responsible for providing repositories with a copy of all required third party software (6.0.4.1.3)

Software Distribution Requirements

- Distribution of voting system and installation software using write once media (6.0.4.1.4)
 - Software sources: vendors, testing authorities, and voting officials (6.0.4.1.4.1)
 - Vendors and testing authorities document to whom they provide software (6.0.4.1.4.5)

Software Distribution Requirements

- Verification of voting system and installation software on write once media using reference information
 - Vendors document process to verify qualified software using reference information (6.0.4.1.4.2)
 - Election officials verify write once media containing qualified software (6.0.4.1.4.3)
 - Voting equipment verify qualified software before installation (6.0.4.1.4.4)

Reference Information Requirements

- Most requirements apply to repositories that generate reference information
- Reference information will be generated by repositories (6.0.4.2.1)
 - Voting system software received from testing authorities
 - Election specific software from jurisdictions

Reference Information Requirements

- Reference information can be either complete binary images, cryptographic hash values, or digital signatures (6.0.4.2.1.1)
 - Repositories create record of reference information generation (6.0.4.2.1.1.1)
 - Records kept by repository until de-qualification of voting system (6.0.4.2.1.1.2)
 - FIPS approved algorithms for hashing and signing (6.0.4.2.1.1.3)

Reference Information Requirements

- FIPS 140-2 level 1 or higher cryptographic module for generation of hash values, digital signatures, and cryptographic keys (6.0.4.2.1.1.4)
- Hash value or digital signature covering reference information sets of hash values or digital signatures (6.0.4.2.1.1.5)
- Additional public key technology requirements (6.0.4.2.1.1.6)
 - Key pairs to be 2048-bits in length (6.0.4.2.1.1.6.1)
 - Private keys used for no more than three years (6.0.4.2.1.1.6.1)

Reference Information Requirements

- Distribution of public keys via write once media or a non-propriety signed format (6.0.4.2.1.1.7)
- Labeling of copies write once media containing public keys (6.0.4.2.1.1.8)
- Repositories document to whom they provide public keys (6.0.4.2.1.1.9)
- When a private key becomes compromised, Repositories notify recipients of the associated public key (6.0.4.2.1.1.10)

Reference Information Requirements

- Repositories to distribute reference information on uniquely labeled write once media and its associated documentation (6.0.4.2.2)
- Reference information without a digital signature stored in secure container when not used (6.0.4.2.2.1)

Technical Guidelines Development Committee

April 20, 2005 Plenary Meeting

Setup Validation Requirements

- Setup validation methods verify no unauthorized software is on the voting equipment (6.0.4.3.1)
 - Vendors provide a process to determine no unauthorized or modified software is present on voting equipment (6.0.4.3.1.1)
 - Process cannot execute or modify installed software (6.0.4.3.1.1.1 and 6.0.4.3.1.1.3)
 - Vendor documents process to verify software has not been modified (6.0.4.3.1.1.2)
 - Vendor provides a means to list all installed software files (6.0.4.3.1.2)

Technical Guidelines Development Committee

April 20, 2005 Plenary Meeting

Setup Validation Requirements

- Use of software and hardware from sources other than the voting system vendor to perform the verification process (6.0.4.3.1.2.1)
- FIPS 140-2 level 1 or higher cryptographic module used during verification with hashes or digital signatures (6.0.4.3.1.2.2)
- Reference information either from a write once media or other media with a digital signature (6.0.4.3.1.2.3)

Setup Validation Requirements

- A read-only external interface on the voting system equipment to access software for verification (6.0.4.3.1.2.4)
 - Tamper evident techniques to protect external interface
 - Physical indicator shows when interface enabled and disabled
 - Disabled during ballot casting
 - *Should directly access software locations without use of installed software*

Technical Guidelines Development Committee

April 20, 2005 Plenary Meeting

Setup Validation Requirements

- Setup validation methods verify registers and variable of voting equipment contain proper initial and static values (6.0.4.3.2)
 - Vendors provide a method to inspect the register and variable values (6.0.4.3.2.1)
 - Vendors document the initial values of dynamic registers and variable except for values set by jurisdictions (6.0.4.3.2.2)
 - Modify to include static registers and variables and election specific values
 - Suggest deleting 6.0.4.3.2.3 and 6.0.4.3.2.4 – already covered in 6.0.4.3.3

Technical Guidelines Development Committee

April 20, 2005 Plenary Meeting

Setup Validation Requirements

- Election officials run verification process before each election (6.0.4.3.3)
 - Modify to clarify both software and register/variable verification processes to be conducted on all voting equipment
- Election officials document results of the verification process (6.0.4.3.3.1)
- Anomalies in the verification process analyzed and resolved before the election (6.0.4.3.3.2)

Technical Guidelines Development Committee
April 20, 2005 Plenary Meeting

Discussion