Draft Recommendations for Software Distribution and Setup Validation: Augmenting the 2002 Voting Systems Standard

Nelson Hastings

National Institute of Standards and Technology

TGDC Meeting, March 9, 2005

Overview

- Software Distribution Resolution
  - Goal and Methodology
  - Scope
  - Sample Draft Recommendations
- Setup Validation Resolution
  - Goal and Methodology
  - Scope
  - Sample Draft Recommendations
- Discussion

Software Distribution: Goal and Methodology

- To determine whether the identified voting system software has been distributed without modification
- Voting System Software Reference Information
  - Binary Images
  - Hash Values
  - Digital Signatures

Software Distribution: Goal and Methodology

- Reference Information Sources
  - Vendors
  - Independent Testing Authorities (ITAs)/Voting System Testing Laboratories (VSTLs)
  - Jurisdictions – states, counties, and localities
  - National Software Reference Library (NSRL)

Software Distribution: Scope

- All executable code and associated configuration files of the voting system software
  - Polling place systems
  - Central counting/aggregation systems
  - Election management systems
- Third party software such as operating systems, drivers, etc. critical to the proper operation of the voting system
- Determining the correct operation of the voting system software is beyond the scope

Software Distribution: Sample Draft Recommendations

- The ITA shall witness the final build of the executable version of the qualified voting system performed by the vendor.
  - Related to VSS Volume I, Section 9.4.1.4
- Complete binary images of voting system software including installation programs shall be distributed on a "write once" by authoritative sources (vendors, ITAs/VSTL, and jurisdictions)
  - From Item 1 of Resolution 15-05: Software Distribution
- The "write once" media containing binary images and hash values of the voting system software shall be labeled by authoritative sources (vendors, ITAs/VSTLs, NSRL, and jurisdictions) so that is uniquely identifiable (including the authoritative source and date created.)
  - VSS Volume I, Section 3.4.6

Software Distribution: Sample Draft Recommendations

- The authoritative sources (vendors, ITAs/VSTLs, NSRL, and jurisdictions) that generate hash value and digital signature reference information shall use a FIPS approved hash function
  - Related to IEEE 5.1.3.4.1 (a) and (b)
- The authoritative sources (vendors, ITAs/VSTLs, NSRL, and jurisdictions) that generate digital signature reference information shall used a FIPS approved digital signature scheme
  - Related to IEEE 5.1.3.4.1 (a) and (b)
- Hash values and digital signatures used for reference information shall be generated by authoritative sources (vendors, ITAs/VSTLs, NSRL, and jurisdictions) using a FIPS 140-2 level 1 validated cryptographic module.
  - Related to IEEE 5.1.3.4.1 (a) and (b)

Setup Validation:
Goal and Methodology

- To ensure voting systems
  - Contain only authorized voting system software
  - Have no unauthorized software installed
  - Are in the proper initial state
- Voting system software items to be inspected to determine the voting machine is in a "proper initial state"

Setup Validation: Goal and Methodology

- Leverage the software distribution requirements
- More process oriented, guidelines
  - However, there are some additional technical requirements
- The current two documents for software distribution and setup validation may be merged

Setup Validation: Scope

- Focus on voting system software
  - Polling place systems
  - Central counting/aggregation systems
  - Election management systems
- General voting system hardware setup is beyond the scope
  - Jurisdictions shall verify the voting system is connected to an appropriate backup power supply
  - Jurisdictions shall verify the display is set to the appropriate level of contrast

Setup Validation: Scope

- Also beyond the scope:
  - How authorized software is installed on the voting system
  - How unauthorized software prevented from being installed on the voting system
  - How a voting system reaches the “proper initial state”

Setup Validation: Sample Draft Recommendations

- The vendors shall identify and document all voting system software required to be installed on voting system for proper operation including the software jurisdictions are required to modify to conduct a specific election.
  - Related to VSS Volume I, Section 8
- Jurisdictions shall obtain reference information (binary images, hash values, digital signatures) for the software listed by the vendors from an authoritative source.
  - Related to IEEE 5.1.3.4.1 (a) and (b)
- Jurisdictions shall verify that all software on the voting system has not been modified using the reference information
  - Related to IEEE 5.1.3.4.1 (a) and (b)

Setup Validation:
Sample Draft Recommendations

- The vendors shall document the values for all the static registers and variables; and initial starting values of all dynamic registers and variables listed for voting system software except for the values set by jurisdictions.
  - Related to VSS Volume I, Section 2.3.5
- Jurisdictions shall document the values for all the static registers and variables; and initial starting values of all dynamic registers and variables listed for voting system software it customizes for an election
  - Related to VSS Volume I, Section 2.3.5
- Jurisdictions shall verify that all the static registers and variables; and initial starting values of all dynamic registers and variables are consistent with the documented values provided by the vendors and jurisdictions.
  - Relate to VSS Volume I, Section 2.3.5

Discussion