Technical Guidelines Development Committee Meeting
December 4 and 5, 2006

Update on VVSG 2007 Security Requirements

Presentation for the
Technical Guidelines Development Committee (TGDC)

Nelson Hastings

December 4, 2006
National Institute of Standards and Technology

Agenda

- Status of security requirements
- Approach to wireless communications
- New and modified requirements
  - Voter verifiable paper records (VVPR)
  - Securing electronic records
  - Setup validation

Status of Security Requirements

Development Process

- Draft requirements created based on research
  - Talk with vendor, election, and security communities
- Distribution within NIST for review
  - Draft requirements revised based on comments
- Distribution to Security and Transparency Subcommittee (STS) for review
  - Draft requirements revised based on comments
- Distribution to TGDC for review and comment

Security Related Material

- Two draft white papers
  - Approach to tie together the security aspects of the VVSG 2007
  - Open ended vulnerability testing approach
- Seven draft sections of VVSG 2007 related to security requirements

Draft VVSG 2007 Sections

- Draft Access Control Requirements
- Draft Cryptography Requirements
- Draft Setup Validation Requirements
- Draft Software Distribution and Installation Requirements

Draft VVSG 2007 Sections

- Draft System Event Logging Requirements
- Draft Physical Security Requirements
- Draft System Integrity Management Requirements

Continuation of Development

- Create draft requirements
- Circulate draft requirement for review
- Modify and refine requirements based on comments
- Integrate requirements into the VVSG 2007
  - Harmonize with other sections as needed
  - Move documentation requirements to appropriate section

Approach to Wireless Communications

Background

- "Draft white paper on wireless issues and STS recommendations for the TGDC"
- VVSG 2005 defines wireless communication as any communication that travels over the air
  - No recognition of the different levels of difficulty needed to secure different wireless technologies
- Focus on infrared (IR) and radio frequency (RF)

Wireless Communication Usage

- Installation of software (including ballot information) on voting equipment (RF and IR)
- Transmission of unofficial election results (RF)
- Opening/Closing the polls (RF)

Wireless Communication Usage

- Collection of cast ballots after polls close (RF)
- Wireless headsets (T-coil only)
- Ballot activation (IR)

Wireless Communication Issues

- Wireless signals vulnerable to interception, insertion, and disruption
  - Leads to reliability issues
  - VVSG 2005 requires backup method
- Technology to attack wireless (RF) signals easily obtained and hidden
  - Attack software is widely available
  - Portable devices (cell phones, PDAs, etc.) can be used to attack

Wireless Communications Issues

- Security measures for wireless communications complicated
  - Difficult to correctly configure wireless devices securely
- Lack of maturity of security measures for wireless communications
- Creates a path for attack

STS Recommendations

- IR wireless communications
  - Restricted as per VVSG 2005
- RF wireless communications
  - Wireless LANs and other RF NOT permitted on voting equipment (that capture voter cast ballots)
  - Separate communication devices could be used to transmit unofficial election results

STS Recommendations

- Impact on wireless usage
  - T-coil wireless headsets - No impact
  - Installation of software - Limited to IR
  - Transmission of unofficial election results - Requires new separate communications devices

Recommendations

- Impact on wireless usage (con't)
  - Collection of cast ballots after polls close - Prohibited
  - Opening/closing polls - Prohibited
  - Upgrade IR communication as per VVSG 2005
    - Loading of software
    - Ballot activation

Discussion

New and Modified Requirements

Voter Verifiable Paper Records

Voter Verifiable Paper Records

- Draft white paper titled “VVPR Issues and STS Recommendations for the TGDC”
- Voter Verifiable Paper Records (VVPR) support the ability to perform independent audits
- Op Scan, EBM/EBP, VVPAT

Voter Verifiable Paper Records

- VVSG 2005 discussed only VVPAT
- VVSG 2007 addresses all VVPR systems
- Goal
  - Ease of use by voters and poll workers
  - Easy to audit by election officials
- Specific implementation issues
  - Paper Rolls
  - Bar Codes

Voter Verifiable Paper Records

- Paper Rolls
  - Pro: Difficult to add or remove cast ballots
  - Con: Potential violation of privacy; and usability/accessibility issues
  - STS Recommendation: Allow paper rolls with improved security and usability

Voter Verifiable Paper Records

- Bar Codes
  - Pro: Makes scanning paper simpler
  - Con: Voter cannot verify contents
  - STS Recommendation: Allow bar codes
    - Audit procedures must not depend on bar codes

Voter Verifiable Paper Records

- Additional STS Recommendations
  - Require better documentation and tools including auditing software
  - Look at entire voter process accessibility
  - Enhance reliability of printers and associated mechanisms

Securing Electronic Records

Securing Electronic Records

- Goals
  - Secure electronic records from voting equipment to central tabulation equipment
  - Prevent alteration or backdating of electronic records
  - Provide signed cast ballots and totals from voting equipment to support canvassing

Securing Electronic Records

- Fully specify electronic record formats
  - Individual and composite cast ballot records
  - Electronic records of voting equipment totals
  - System event log records
- Electronic records require
  - Digital signatures
  - Timestamps
  - Information on software versions and configuration files

Securing Electronic Records

- Hardware crypto module in each voting machine
  - Hardware module not removable from voting machine
  - Software attacks are limited by hardware module protecting keys

Securing Electronic Records

- Cryptographic key management
  - A permanent signing key for each voting machine linked to its serial number
  - Each voting machine generates a signature and verification key pair for each election
    - Used to digitally sign electronic records for the election
  - Destruction of election specific signature keys after each election

Securing Electronic Records

- Results of approach
  - Signed electronic record prevents tampering of electronic records
  - Once election specific signature key destroyed prevents backdating of electronic records
  - Permanent voting machine signing key prevents substitution of machines or its electronic records
  - Central tabulation machine, auditors, and public can verify digital signatures of electronic records

Setup Validation Requirements

Setup Validation Requirements

- The goal is to determine that voting equipment is in a “proper initial state”
- Addresses TGDC resolution #16-05: Setup Validation
  - Only authorized voting system software installed
  - No unauthorized software installed
- Based on VVSG 2005 Section 7.4.6: Software Setup Validation

Setup Validation Requirements

- Modified and extended requirements found in VVSG 2005
  - Inspection of software installed on voting system
  - Inspection of voting system register and variable values

Setup Validation Requirements

- New requirements cover
  - Documentation requirements
  - A model setup validation process
  - Inspection of backup power supply
  - Inspection of cabling connectivity
  - Inspection of communications

Setup Validation Requirements

- New requirements cover (con't)
  - Inspection of consumables
  - Inspection of calibration of components
  - Inspection of external interfaces
  - Checklist of other voting equipment properties to be inspected
  - Record creation of the inspection results

Discussion