VVSG 2.0
Security Requirements Updates

Gema Howell
Security Engineer
Co-Chair of the VVSG Election Cybersecurity Working Group
November 1, 2019

Agenda

- E2E Verifiable
- Wireless
- Internet
- Unique Identifiers Added for Auditing
- Random Number Generation
- Preserving Log Integrity
- Password Complexity

E2E Verifiable Requirements

- In Section 9.1.6 *E2E Verifiable*
  - Use an external process for evaluation and validation of cryptographic E2E protocols
  - Cast-as-intended verification
  - Ballot receipts are accessible, verifiable, and preserve voter privacy
  - Export ballot tabulation evidence
  - Publicly available reference implementation of the validated E2E cryptographic protocol used within the voting system

E2E Verifiable Requirements Continued

- 10.2.1-F - *Confidentiality for indirect association*
  - Encrypt ballots that use indirect associations
  - Indirect associations are not encrypted with the ballot
- 13.3-B - *E2E cryptographic voting protocols*
  - E2E cryptographic protocols are omitted from the FIPS 140-2 validation requirement
  - Subject to requirements in 9.1.6-A
  - Commonplace cryptographic operations used within E2E systems, such as encryption, decryption, and hashing, are subject to the FIPS 140-2 validation requirement

Wireless

- 14.2-D – *No wireless networking*
  - Incapable of establishing wireless connections
  - This does not disallow the use of assistive technology (AT) within the polling place
    - Wireless AT may be used with an adapter for the 3.5 mm jack (see 8.1-E – Standard audio connectors)
- 14.2-D.1 – *Wireless network status indicator*
  - Renumbered, still included to inform if wireless is enabled
- 15.4-C.1 – *Documentation for disabled wireless*
  - Information about how the wireless is disabled within the voting system

Internet

- 14.2-E – *No internet by design*
  - Unable to connect to external networks
  - Unable to connect devices that allow connections to external networks
- 15.4-B - *Secure configuration documentation*
  - Documentation may include how external network services are not included as part of the voting system and must be handled through a separate air-gapped process
- Deleted the old 15.4-B
  - Removed requirement about the use of public telecommunications

Unique Identifiers Added for Auditing

- 9.1.5-F - *Unique identifier*
  - Removed “or affixed by some other external mechanism”
- 9.1.1.C - *Mechanism documentation*
  - Documentation needed to describe how software independence is preserved
- *9.1.5-G Printing on a paper ballot*
  - Unable to physically print in the ballot selection area

Random Number Generation

- 10.2.2-F – *Random number generation*
  - Random numbers are generated using guidance from NIST SP 800-90A rev. 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*
  - Submit to the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) for conformance testing
- 9.1.7-C – *Random number usage*
  - *Documentation of how random numbers are used and created*

Preserving Log Integrity

- 11.1-C – *Preserving log integrity*
  - Updated the title
  - Prevents the deletion of logs; except for log rotation
  - Log rotation is when the stored logs are rotated out to create more space for continuous logging

Password Complexity

- 11.3.2-B – *Minimum password complexity*
  - At minimum, follow NIST 800-63B password complexity guidance
  - Recommended minimum password length is 8 characters
- 11.3.2-B.1 – *Specify password complexity*
  - Only administrators can specify password strength
- 11.3.2-C – *Password blacklist*
  - *retitled*

VVSG 2.0
Core Requirements Updates

John Wack
November 1, 2019

Contents

- Update of bar code-related requirements
- Upgrade to recent version of MIL standard for environmental testing
- Testing for dust contamination

Updates to Transparency Requirements 1

Requirements made more clear to require

- Associated document to be publicly available
- Barcode is a public standard
- Packing of barcoded-data is documented
- Codes in barcodes are documented

3.3-A – System security, system event logging

The voting system's manufacturer must provide documentation to be publicly available at no cost that:

1. describes system event logging capabilities and usage
2. fully documents the log format information

Discussion

The log format and the meaning of all possible types of log entries must be fully documented in sufficient detail to allow independent manufacturers to implement utilities to parse the log file. This documentation must be publicly available, free of charge, and not just in the TDP. The documentation may be housed by the EAC.

Updates to Transparency Requirements 2

3.3-B – Specification of common data format usage

The voting system's manufacturer must provide documentation to be publicly available at no cost describing how the manufacturer has implemented a NIST CDF specification for a particular device or function. This includes such items as:

1. descriptions of how elements and attributes are used
2. constraints on data elements
3. extensions as well as any constraints

Discussion

Conformance to a common data format does not guarantee data interoperability. The manufacturer needs to document fully how it has interpreted and implemented a NIST CDF specification for its voting devices and the types of data exchanged or exported.

3.3-C Bar and other codes

The voting system's manufacturer must provide documentation to be publicly available at no cost that fully specifies the bar code or other encoding standards or algorithms used on ballots or audit material.

Discussion

The voting system documentation needs to include the name and version of the standard used for bar codes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election.

Updates to Transparency Requirements 3

3.3-D Encodings

The voting system's manufacturer must provide documentation to be publicly available at no cost that fully specifies any compression, packing, or otherwise encodings of data used on ballots, including how data may be compressed or otherwise altered prior to encoding within a bar code.

Discussion

The voting system documentation needs to include the name and version of the standard used for bar codes or for any other codes that encode information that the public sees on ballots or other material that can be used in audits or verification of the election. The documentation also needs to include how the data may be packed or compressed within the encoding. The report should be sufficient for a voter to understand the barcoded contents and for an auditor to develop applications that examine the barcoded contents.

3.3-E Ballot selection codes

The voting system must be capable of producing a report to be publicly available at no cost to show the meaning of codes and other data used within a bar code to represent ballot selections and ballot style information.

Discussion

Codes are commonly used with bar codes that represent a voter's ballot selections. The codes are meaningless to a voter or an auditor unless the voting system can produce a report that shows all codes possible and what contests and ballot selections they represent. If, for example, a code of 90 is used to represent a particular contest, then the report must show that 90 refers to the title or description of that particular contest. This includes other information within the bar code generally found on clear-text ballots to identify the ballot style.

MIL-STD-810 Update

- Contains tests for wide range of environmental issues, e.g., temp, humidity, shock, vibration
- Sometimes the 810D tests are modified in prior VVSGs where reasonable
- NIST in 2007 undertook study of differences between 810D and current versions, differences are relatively minor
- Next VVSG now references 810H, Jan, 2019
- Next update to 810H slated for 2024 (5-year cycle)

Changes Made to Requirements in 2.7

2.7-A – Ability to support maintenance and repair physical environment conditions – non-operating

All voting systems must be able to withstand non-operating physical environmental conditions exercised in accordance with MIL-STD-810H, Method 516.6. Procedure VI [MIL19].

Discussion

This test simulates stresses faced during maintenance and repair.

External reference: MIL-STD-810H

Prior VVSG source: VVSG-2007 - 5.1.4-A.1

- **Similar mods made to other requirements in 2.7**

Testing for Dust Contamination

- Dust contamination issue raised by Neal Kelly
- Prior VVSGs do not require testing
- MIL-STD-810H contains tests which likely need to be made less stringent for voting devices
- Tests would add expense to certification testing
- No data yet on degree to which voting devices are affected by dust contamination
- Issue needs further study, will discuss in VVSG Testing PWG and ask EOs for more data
- Changes to VVSG could be made post review cycle