

Software Assurance and the new Voluntary Voting System Guidelines

Andrew Regenscheid

Computer Security Division

National Institute of Standards and Technology

vote.nist.gov

Voting Systems Overview

- E-voting machines (DREs)
 - Some produce voter-verified paper audit trails
- Optical scan systems
- Must be highly accurate and reliable
- Challenging to support needs of 50 different states
- SwA an important issue

Background

- Previous standard: **VSS**
- 2000 elections generated concerns over voting system integrity, usability, and security
- Current voting standards lack:
 - Precision and clarity of requirements
 - Consistent test methodologies
- 2002 Help America Vote Act (**HAVA**) was passed to address these concerns

NIST and the VVSG

- NIST provides technical support in the development of the Voluntary Voting System Guidelines (**VVSG**)
- NIST works with the EAC, state election officials, industry, academia
- VVSG includes a testing and certification component
- Accrediting test labs (NVLAP)

The New VVSG

- A more precise, detailed standard for voting systems
- Addresses software assurance via various requirements for testing and security
- Does not require formal methods or formal design analysis
- Will be accompanied by test suites

How is SWA addressed?

1. Improved Software Workmanship
2. Logic Verification
3. Open Ended Vulnerability Testing
4. System Integrity Management
5. Software Independence

Software Quality

- Previous versions of standards required coding standard that worked against commonly-accepted conventions
- New VVSG permits newer coding standards
- Requires better programming constructs, e.g.
 - Block structured exception handling
 - Separation of code and data
 - Mandatory internal error checking
 - No buffer overflows

Logic Verification

- Manufacturer has to show that logic of system satisfies certain constraints in a logic model
- Addresses core logic of voting system
 - Vote recording
 - Vote tabulation
- Code has to be designed in such a way that it can be verifiably shown to be correct
 - Less rigorous than formal analysis
 - Uses informal arguments and limitations on complexity

Open Ended Vulnerability Testing

- Essentially an expert review of system security
- Similar to penetration testing, a robust check on voting system's capability to withstand various attacks
- Targets issues that could remain after conformance testing
- Already conducted by some states

Software/System Integrity

- Voting SW cannot be installed without hash check with reference archive versions
- SW cannot be executed without similar check
 - Code must be digitally signed and signatures must verify
 - Prevents loading unauthorized versions of software or patches
 - No guarantees that code is correct, but that it is the authorized version

Software Independence

- Software Independence (SI): A change in software cannot cause an undetectable change in election vote totals
 - Voting systems are unique due to the secret ballot
 - Difficulty of proving correctness of software
- Voting systems must be SI to conform
 - Need independent audit of electronic records
 - Systems that do this **currently** are paper-based e.g., optical scan, VVPAT

NIST voting site

- **<http://vote.nist.gov>**

- Includes:
 - Overview of NIST voting project
 - VVSG versions, presentations, white papers
 - New VVSG tutorials and overview information
 - Test suite information