Security Issues in Voting Systems:
A Panel Session

Ed Roback

Chief, Computer Security Division

December 10, 2003

Overview

- NIST
  - Security role
  - Current projects/competencies
  - Responsibilities under the Help America Vote Act (HAVA)
- Security Challenges
- Panel Focus
- Logistics

NIST's Overall Security Role

- Federal Information Security Management Act of 2002
  - Scope: Non-national security systems
  - Minimum requirements for all Federal systems (Draft NIST 800-53 out for public comment; Via http://csrc.nist.gov/publications/drafts.html)
- Cyber Security Act of 2002

NIST's Cyber Security Related Activities Include…

- Security Standards and Guidelines
  - Management and Technical topics
  - Cryptography, incl. Advanced Encryption Standard
  - Contingency Planning, Risk Management, Security Metrics
  - Smart Cards
- Security Testing, e.g.:
  - Cryptographic Module Validation Program
- Security Research
  - Authorization, PDA security
- Software quality
- Biometrics and smartcards
- Vulnerabilities and countermeasures

NIST's Computer Security Resource Center: http://csrc.nist.gov

NIST and HAVA

- NIST will provide technical *support* for security R&D in voting standards undertaken by the Technical Guidelines Development Committee
- NIST not in an *oversight* role
- Facilitation – a key NIST contribution
- Fiscal constraints on NIST

Security challenges in HAVA

1. Security of computers, networks, and data in voting systems
2. Methods to detect fraud and abuse
3. Protection of voter privacy

Security of Computers, Networks, Data

- Our security research and guidance encompasses:
  - Techniques to help secure systems and applications
  - Security product settings
  - Risks and vulnerabilities in new technologies
  - System accreditation and certification
  - Authentication and cryptographic procedures

Detecting Fraud and Abuse

- Fraud and abuse can be prevented through robust controls and detected by auditing
- NIST has conducted R&D in authentication and access control, e.g., smartcards, RBAC, encryption products
- NIST has produced guidance in management practices and training, which can be mapped to voting management

Protecting Voter Privacy

- Auditing in voting is more difficult due to requirement of voter privacy
- Robust auditing while protecting privacy can be achieved, may require independent auditing, spot checks, cryptographic solutions
- NIST often plays key neutral 3rd party role to facilitate solutions

A Core NIST Security Competency: Cryptographic Standards Development

- Cryptography uses include access control, confidentiality of votes, integrity of voter counts and software
- Strong cryptography rendered weak via poor management practices
- NIST’s security guidance emphasizes use of tested algorithms, modules, and procedures

Panel Focus: Security in E-Voting Systems

- Purpose of the panel is to discuss primary security needs and issues in e-voting
- To educate and inform community at large
- To highlight needed improvements in standards and procedures
- The focus is on next steps and solutions
- 5 speakers with expertise in specification, implementation, testing, and management

A Few Logistics

- 3 presentations
- 30 minute break
- 2 presentations
- Each presenter may speak for 20 minutes

  Q&A for 8 minutes
- Panel Discussion at end

Panelists

- Brit Williams, Kennesaw State, Georgia
- David Dill, Stanford University
- Avi Rubin, Johns Hopkins University
- Jim Adler, Vote Here, Inc.
- Donetta Davidson, Sec of State, Colorado