Introduction & VVPR

May 21, 2007

Bill Burr
Computer Security Division

Background: Basic Voting Security Problem

- Apparent vulnerability of some computerized voting systems to undetected fraud
    - Malicious code
    - Many different kinds of computer systems have been successfully hacked in one way or another
        - Sometimes very sophisticated attacks
    - Public sensitivity to attacks on computer systems
- Security critical IT systems usually rely on a strong audit system
    - How do you meaningfully audit a DRE?

General Approach

- Simplify – complexity greatly complicates security analysis
  - No Internet connection of voting stations during polling
  - No wireless (except for IR when shielded) for voting stations
- Software Independence
  - Detect election fraud or errors even if code has bugs or is tampered
    - A good metric for this is the size of the conspiracy needed to defeat the audit system
  - Need a strong audit system
  - Paper audit trails – we think we know how to do these
    - Voter verification
- Weren't able to develop standards we were happy with for all-electronic, or paper free voting systems (e.g., IDV)

Approach

- Do the obvious: design and configure voting systems to make it harder to attack them
  - Setup Validation
  - Physical Security
  - Documentation
  - Software Distribution
  - *System Integrity Management*
  - *Communications Requirements*

Approach

- A strong (paper centric) audit regime
  - Security and Audit Architecture
  - Electronic Records
  - Voter Verified Paper Records
  - Cryptography – mainly intended to secure electronic records
  - System Event Logging
  - Voter Verifiable Paper Records (VVPR)

VVPR Section: Requirements for Voter Verifiable Paper Records

VVPR includes:

- Paper-roll VVPAT
- Cut sheet VVPAT
- Hand marked PCOS ballots
- Machine marked PCOS ballots

Summary

- VVPR requirements in this chapter support auditing and address attacks from threat work.
- Human-readable VVPR sufficient to count votes
- Machine-readable information allowed with restrictions
- New requirements on VVPAT
  - VVPAT contents
  - Error handling/recovery
  - Paper-roll privacy requirements
- New SHOULD for PCOS
  - Breaking into batches for easier auditing

General Requirements on VVPR

These apply to ALL VVPR

- **Human readable record contains enough information to count**
  - No hidden information (like precinct/election district) that isn't also human-readable
- **Paper record is also machine-readable**
  - Support for auditing human-readable vs what machine reads.
- **May use some non human-readable encoding like a barcode.**
  - Public, standard format.
  - Barcode (etc.) contains copy of human-readable part.
  - May also contain limited kinds of other data.

VVPAT Requirements--Overview

- VVPAT is fairly new architecture
  - As experience grows, we learn more requirements.
- Major goal: Make VVPR useful for audits that detect attacks
  - Human readable content
  - Sequence of steps for voting
  - Interactions between printer and voting machine/DRE
- Sources: Election officials, ESI report, Brennan Center report, NIST Voting Threats Workshop, NIST/GWU Threats Workshop, Various state laws and proposed laws about VVPAT

VVPAT--Definitions and Basics

- VVPAT = DRE + printer
  - Voter casts vote using some electronic interface
  - Printer produces summary of the voter's choices
  - Voter able to verify choices
  - Voter may accept or reject ballot

VVPAT: DRE-Printer Interactions

- **Printer connected over standard interface**
- **Printer detects and handles common errors**
  (out of supplies, paper jam)
  - *Election official must be able to determine whether voter's vote has been cast or not*
  - Documentation shows how to recover from errors
- **Voter error / malice must not create discrepancy between paper and electronic records.**

VVPAT: Protocol of Operations

Ensure VVPR is meaningful for audit

- **Paper and electronic record visible side-by-side.**
- **Accepted paper record:**
  - Marked as accepted in voter's sight
- **Rejected paper record:**
  - Marked as rejected in voter's sight
  - Can be set up to allow revote by voter
  - Can be set up to require election official intervention

Paper Roll VVPAT Record Contents

- **Each paper roll contains**:
  - Voting machine, election, precinct, roll # (e.g. Roll #2)
  - Summary line--total # CVRs on roll, total # accepted
- **Each vote summary contains**:
  - Which ballot is being voted, including precinct/district.
  - Type of voting (provisional, early)
  - Summary of votes cast, clearly showing undervotes.
  - Clear indication that vote was accepted/rejected
- **Vote summaries not split across rolls**

Cut Sheet VVPAT Record Requirements

- **Each Vote Summary Contains**:
  - Voting machine, election, precinct
  - Which ballot is being voted, including precinct/district.
  - Type of voting (provisional, early)
  - Summary of votes cast, clearly showing undervotes.
- **Vote summary not split across sheets of paper**
  - NOTE: This has an impact on designers' flexibility

Discussion Point: Should cut-sheet VVPAT allow multi-sheet vote summaries?

Support for Linking Paper / Electronic Records

Some states require linking paper and electronic records 1:1

- **VVPAT shall support linking records**
  - Linking information should be hard for voter to read
  - Linking information readable by auditors
- **VVPAT shall allow linking to be turned off**

Discussion Point: Procedures for using linkage not currently required or discussed in VVSG.

Paper-Roll Privacy Issues

Paper-roll VVPAT raises potential privacy issues which must be addressed procedurally. VVPAT design must support procedural defenses.

- **Secure container for rolls containing vote summaries**
- **Container supports secure use of locks and tamper seals**
- **Vote summaries put in container immediately after cast**
- **Printer error doesn't compromise previous summaries.**
- **Documentation shows how to protect voter privacy**

Discussion point: Is anything else needed to ensure voter privacy?

PCOS Requirements

Few new requirements needed--PCOS is well-understood technology!

- **General VVPR requirements apply**
  - Do these require any changes at all?

- **Should support breaking records into batches:**
  - PCOS separates cast ballots into batches of, e.g., 50
  - PCOS produces end-of-day report including counts of each batch.
  - Hand-audit can choose one batch randomly and recount it, instead of recounting whole set of ballots for day.

Summary

- VVPR requirements in this chapter support auditing and address attacks from threat work.
- Human-readable VVPR sufficient to count votes
- Machine-readable information allowed with restrictions
- New requirements on VVPAT
  - VVPAT contents
  - Error handling/recovery
  - Paper-roll privacy requirements
- New SHOULD for PCOS
  - Breaking into batches for easier auditing

Discussion