Security, Auditability, and Threats: The VVSG2007 Security Architecture

Presentation for the
Technical Guidelines Development Committee (TGDC)

John Kelsey

Dec 4/5, 2006

National Institute of Standards and Technology

Security Requirements

- Goal: Write a standard that leads to secure voting systems!
- We need to understand:
  - Security requirements and attacker goals/resources
  - Voting system architectures
  - Threats to voting systems
- Write requirements to block attacks
  - Ensure those requirements are testable!

Looking at the big picture

Roadmap: Attackers->Threats->Standard

- Understand attacker goals and resources
- Determine how attacker might accomplish those goals
  --> Threats
- *Determine defenses to block threats*
- *Write testable requirements to ensure presence and effectiveness of these defenses*

How Does VVSG2007 Address Threats?

- For each voting system architecture:
  - Identify significant threats
  - Block threats (ideally, block whole classes of threat)
- Blocking = Prevention or Detection

  Example: paper ballots in ballot box
  - Prevention: Padlock on ballot box
  - Detection: Tamper-evident seal on box

Current Voting System Architectures

- Precinct Count Optical Scan
  - Hand-marked
  - Ballot marking devices/ ballot printing devices
- DRE+VVPAT
  - Paper-roll
  - Cut-sheet
- DRE

What are the attacker's goals?

- Change outcome of election
  - This is where we spend most of our analysis!
- Defeat ballot secrecy
  - With or without voter's help
- Disrupt election
  - Force election to be re-run or decided in courts

How Do We Know About Threats?

- History and folklore about voting systems
  - Harris book, election officials, voting people
- Current information on computer attacks
  - Computer security literature, CERT, security people
- Analysis of voting system components in the lab
  - Hopkins, RABA, Hursti, Princeton, Compuware,...
- Analysis of voting systems w/ procedures
  - Brennan Center, NIST Threats Workshops

Threat Methodology

Wrong question: *Can I tamper with a voting machine?*

Right question: *Can I tamper with an election?*

- Consider a close statewide election: Look for ways to tamper with outcome!
  - Parameters like #voting machines, #polling places, how big change can be before noticed
  - Consider procedural defenses!
  - Evaluate attacks based on attack team size

Roadmap: Attackers->Threats->Standard

- Understand attacker goals and resources
- Determine how attacker might accomplish those goals
  --> Threats
- *Determine defenses to block threats*
- *Write testable requirements to ensure presence and effectiveness of these defenses*

Requiring Security Controls

- Some threats can be prevented or detected by specific security controls
  - Event logs
  - Access control
  - Software distribtution
  - System configuration management
  - Digital signatures on electronic records

Procedural Defenses

- Some threats blocked by procedural defenses:
  - *Example Threat*: Tampering PCOS scanner software
  - *Procedural Defense:* Random auditing recount of ballots from a few precincts

Procedures in an Equipment Standard?

- Require equipment to support the procedures it needs to address threats for its architecture:
  - Specific hardware/software requirements to ensure that procedure can function effectively.
  - Documentation requirements: user documentation must show how to do procedure.
  - Technical documentation must show lab why procedure accomplishes desired security goals.

Example: Parallel Testing

- Determine if the voting machines are misbehaving on election day.
- Procedure: Isolate a few random voting machines, run an all-day test on them.
- Requirement: The voting machine must never be able to find out it's being tested.

This Leads to Equipment Req'ts

- Voting machines....
  - Must not receive signals during voting.
  - Must not learn they are being tested by authorizations to vote.
  - Must not have any observable change between test and voting environment
- These are equipment requirements, needed to support parallel testing!

And to Other Requirements

- The voting machine documentation must explain how to carry out a parallel test
- VSTL verifies that documentation gives a good parallel test--accomplishes security goals.
- In open-ended testing, VSTL attempts to find:
  - Ways for voting machine to notice test environment
  - Ways for anyone to get message into voting machine

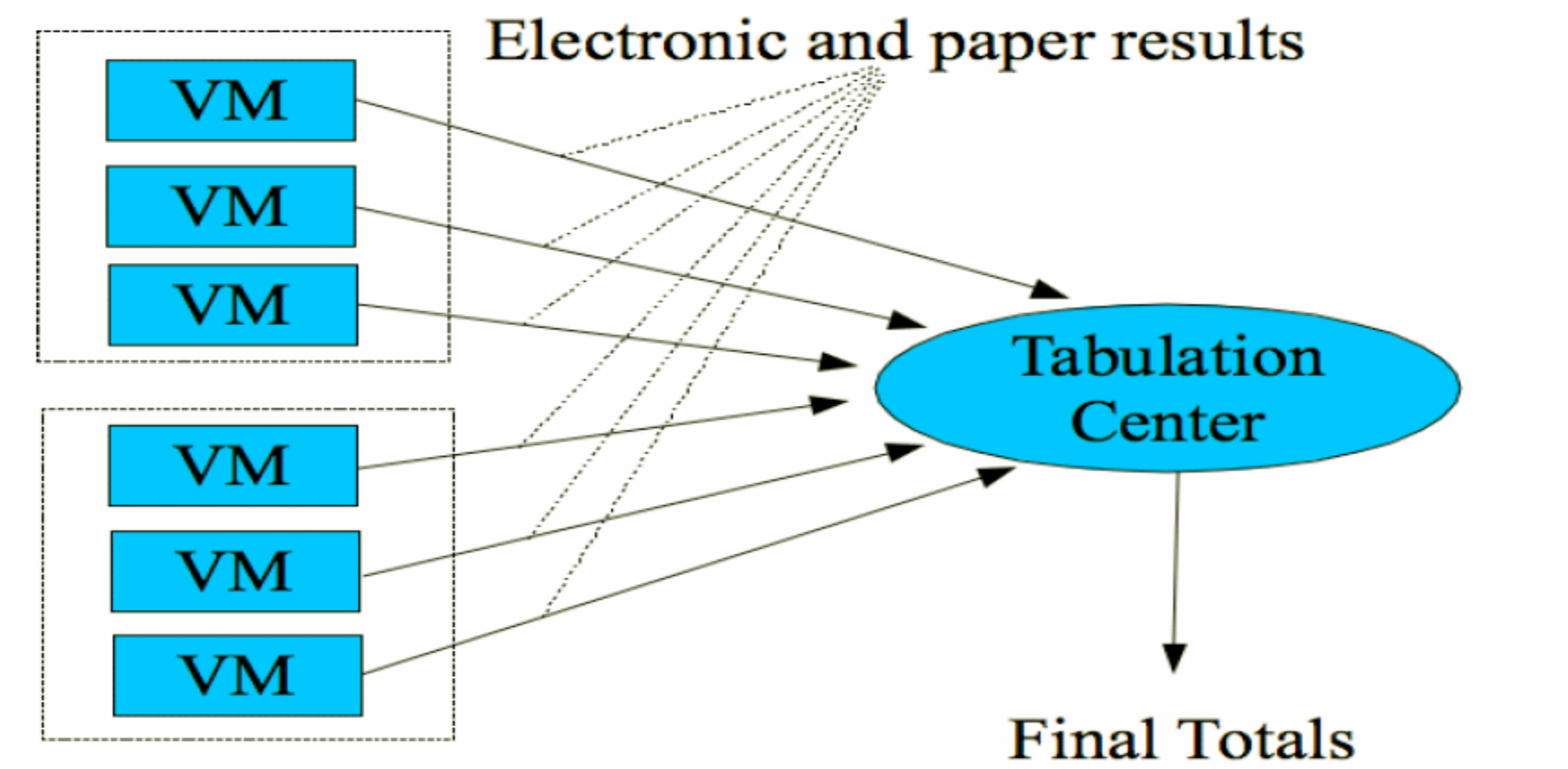
How Are Requirements Enforced?

Checklist -> Documentation -> OEVT

- VSTL checks to make sure required security controls are present and correctly used.
- Documentation requirements--VSTL reads and verifies correctness of documentation
- OEVT--open-ended testing, VSTL attempts to find ways in which security of voting system can be violated.

Conclusions

- VVSG2007 security standards based heavily on threat analysis
  - Drawn from extensive literature review, historical data, and internal and external analysis, and workshops
- Procedural requirements -> equipment and documentation requirements
- Equipment, Documentation, and OEVT requirements fit together to improve chances of getting secure voting systems.


Electronic and paper results
VM
VM
VM
VM
VM
VM
Tabulation Center
Final Totals