Electronic IDV--Status Report

Presentation for the
Technical Guidelines Development Committee (TGDC)

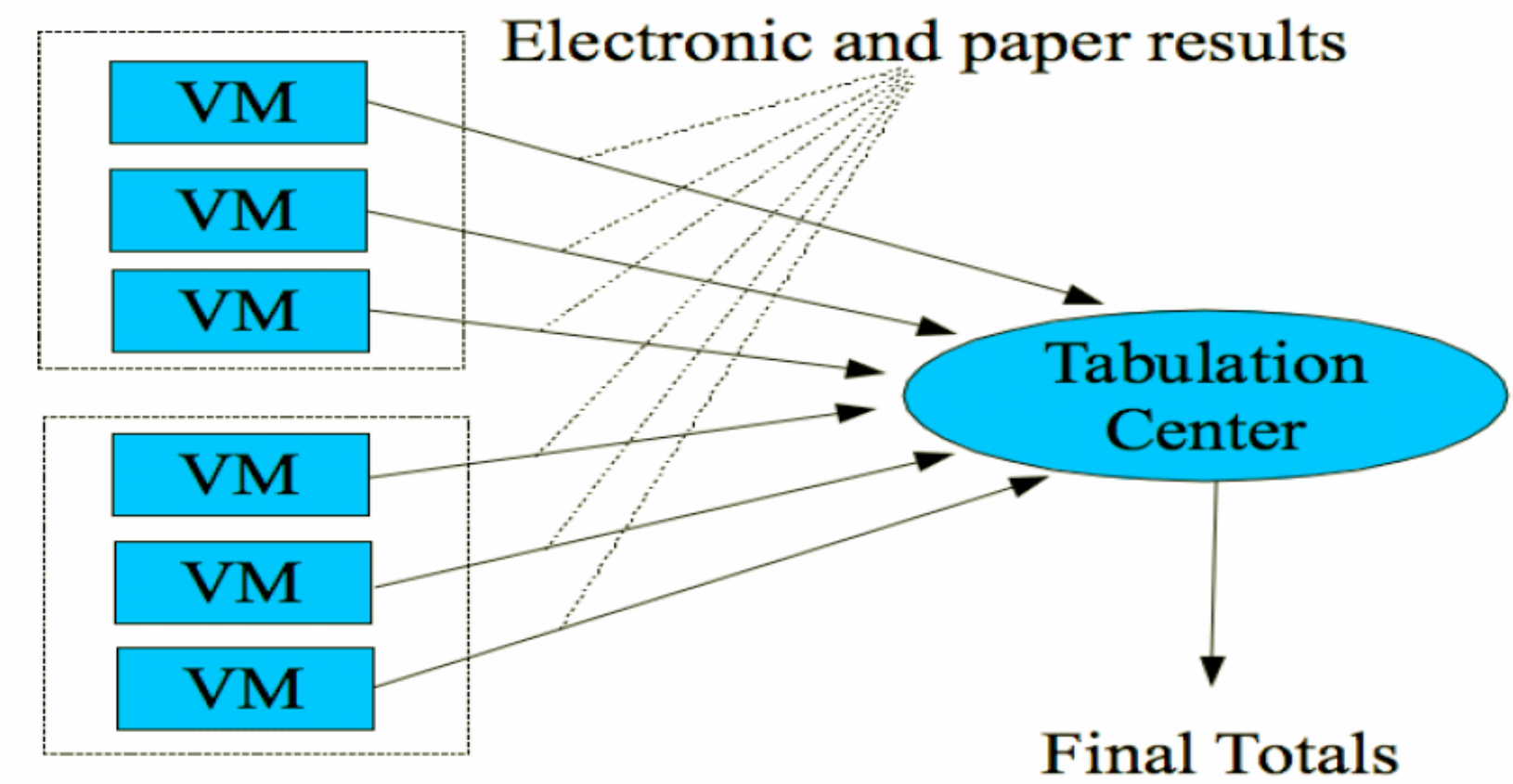
John Kelsey

Dec 4/5, 2006

National Institute of Standards and Technology

Overview

- **Question:** Can we write standards for all-electronic voting systems that are auditable?
- **Answer #1:** We think it's possible to design such a system, but it's a research problem.
- **Answer #2:** Even if we can design one such system, we need to know a lot more to write standards for all such systems.


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

How To Make It Auditable

- Obvious solution is paper--this is what we have now
  - *Can we do better?*
- Non-Paper IV = Independent Verification:
  - Dual Process: Multiple computers record vote
  - Witness: Independent record made of voter/voting machine interaction
  - Non-paper physical system: audit from some non-paper physical record
  - Many combinations possible

Dual Process

- Idea: Have two or more machines interact with voter, making independent record of votes for audit.
  - Very similar to DRE+VVPAT
- Examples: Frog, Viewscreen, One-way IDV
- Threats:
  - Compromise of both machines kills security
  - System getting vote can misread voter choice, if voter doesn't notice during verification, this leads to a change.

Example: DRE+Viewscreen

- Normal DRE + second independent Viewscreen connected over USB
- Voting Process:
  - Vote on DRE
  - Verify on Viewscreen
- Auditing:
  - Records from both machines are compared.

Attacking the Viewscreen

- DRE can “accidentally” misrecord vote--if voter doesn’t notice, vote is changed.
  - Similar attack on VVPAT, but Viewscreen should be easier to read!
- Compromising both destroys all security in this system
  - Audit is no longer meaningful

Witness System

- Idea: Put “witness” into channel with voter, so it can record interaction between voting system and voter
  - Somewhat similar to ballot-markers
- Examples: VGA tap, Selker’s audio ballot*
- Threats:
  - Voting machine may try to cause witness to see something different from voter
  - If witness and voting machine both compromised, all is lost.

Example: DRE with VGA tap

- DRE uses a standard analog VGA screen and buttons.
- Witness device taps into VGA line and line back from buttons. Records each new screen image and each set of buttons pushed.
- Auditing step checks sequence of images and buttons against sequence of votes--probably requires human intervention.

Attacking DRE+VGA Tap

- DRE can try to flicker screen to show VGA tap different image than vote
- If VGA monitor hardware tampered, DRE can use some in-band signaling to tell VGA monitor to show something different from what witness sees.
- If witness and DRE conspire, all is lost.

Non-Paper Physical Record

- Idea: Use some physical record not susceptible to software tampering to record votes.
  - Similar to hand-marked paper ballots
- Examples: Selker's audio ballot
- Threats:
  - Physical record can be tampered
  - Mechanism to make physical record can be tampered

Example: DRE+audio ballot

- Ted Selker (MIT) proposed DRE+audio ballot, audio is always used.
- Witness device records audio onto standard magnetic tape--no software or complex hardware need be involved.
- Important distinction: witness device can be physically checked!
- But this needs a time-consuming human audit, just like paper

Attacking Audio Scheme

- Replace recorder with something controlled by attacker
  - Patch attacker-controlled device in position to intercept and replace audio signal from headphones.
- Damage recorder hardware or tape in machines to be attacked
- Replace audiotape in transit
- Mislead voter by giving video feedback different from audio

Why Can't We Standardize Yet?

- These are research ideas, a few with prototypes built.
  - No operational experience
- These require independence of records, which for software systems is very hard to achieve
  - DRE and witness device or viewscreen probably bought from same company, stored in same warehouse, etc.
- What will these systems look like in five years? We don't know enough to standardize

Conclusions

- We think auditable electronic voting systems are worth investigating
- We don't know how to write standards with enough specificity to get secure systems

Discussion