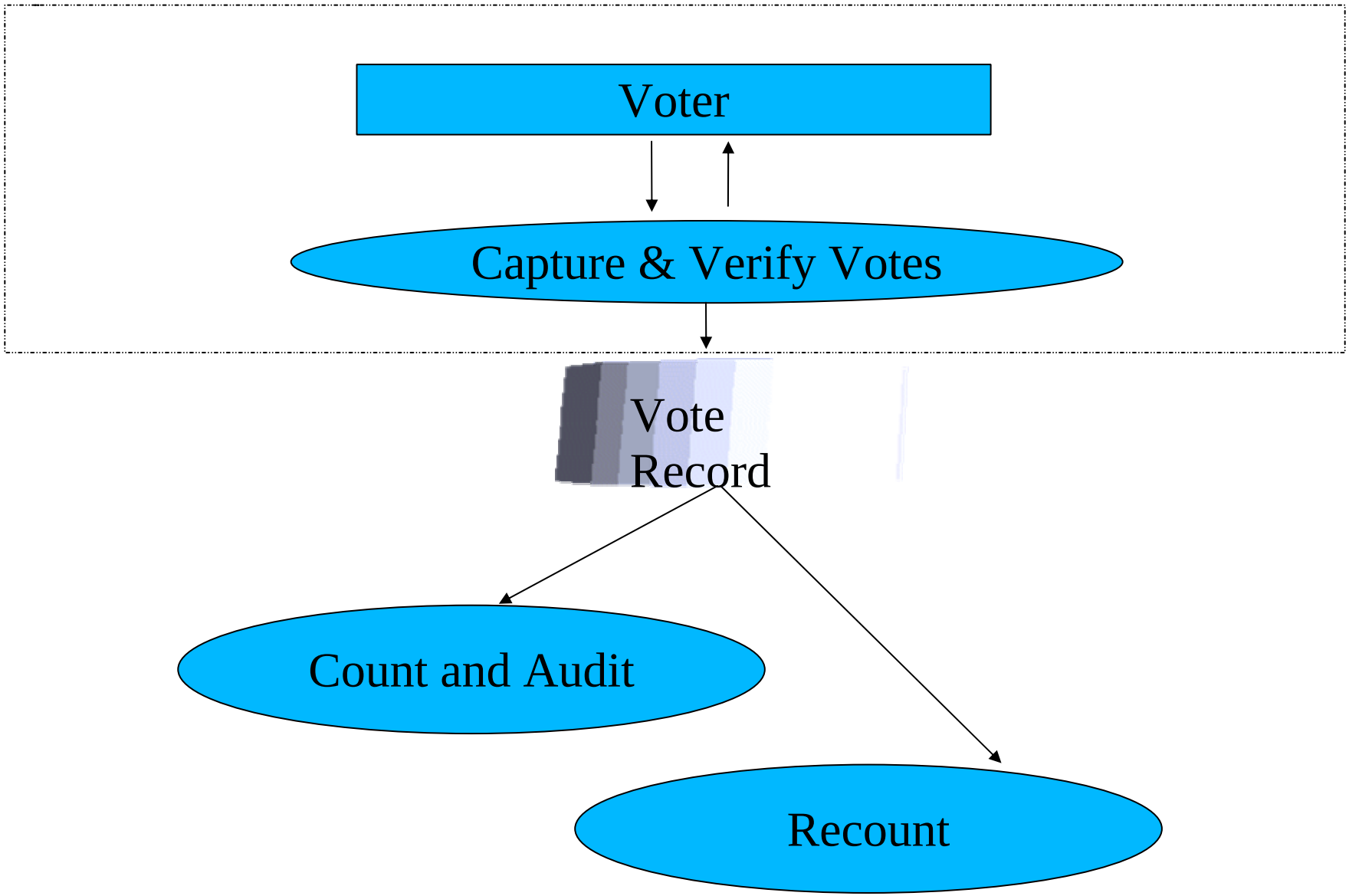
DV/IV Systems (12-05) and Multiple Representations (21-05)

John Kelsey
NIST Computer Security Division
TGDC Meeting March 9, 2005

Overview

- Our Security Framework
  - How can we write standards that will lead to secure voting systems?
- DV and IV(12-05)
- Multiple Representations(21-05)
- Conclusions

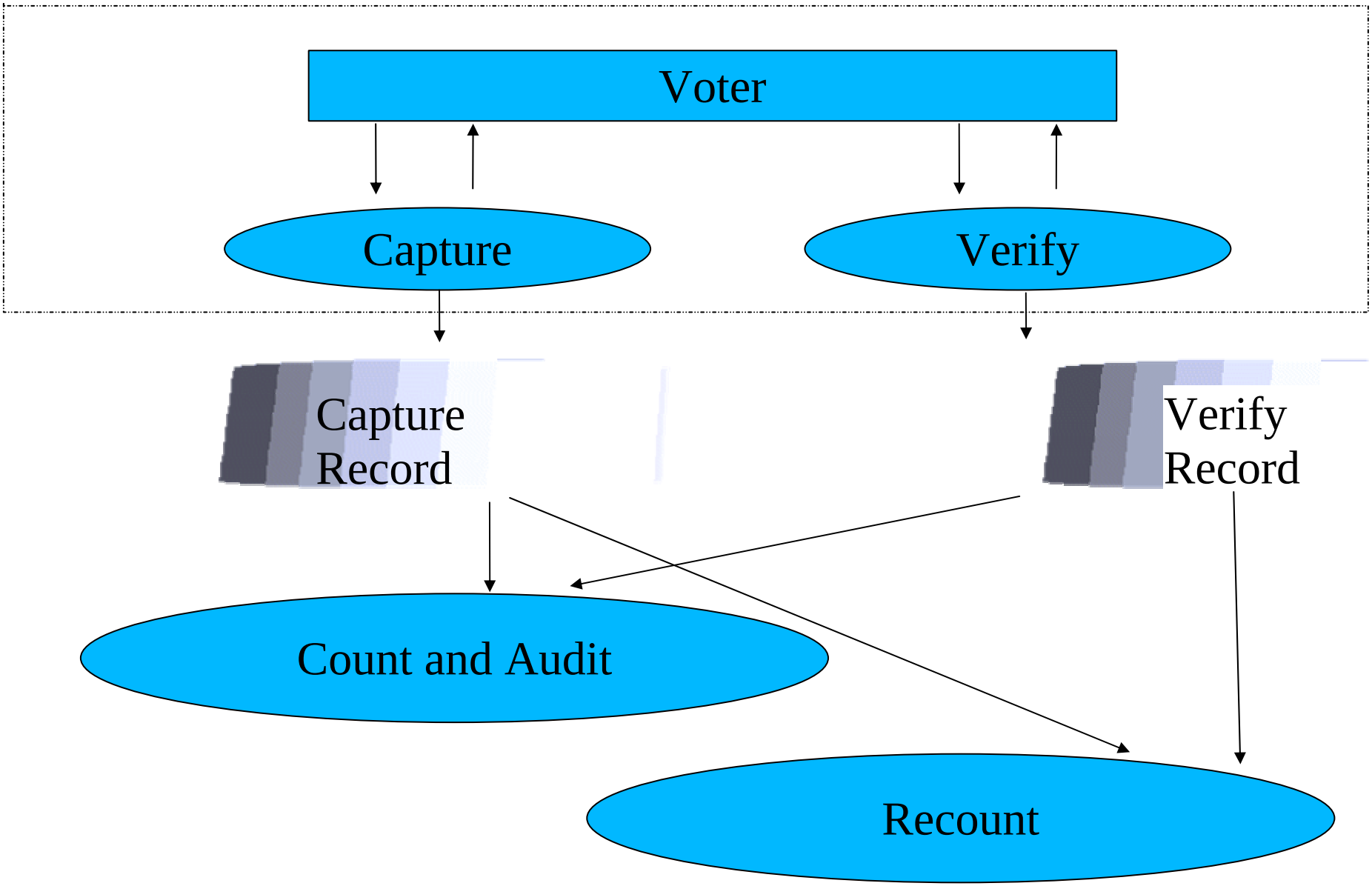
A Very Simple Model of Voting



Interaction Between Voter and System

- Errors and fraud in this interaction hard to catch
  - Not observable
  - Can't be redone without redoing election
  - Privacy of voter imposes limits on auditing
- Voter verification step gets voter to verify his own choices
  - HAVA requires this step [sec. 301(a)(1)(A)(i)]
  - Our security framework: *Use this step to provide independent evidence of voter choices*

A Dual-Verification Voting System



Our Security Framework: Dual-Verification Systems

- Produce two or more records of independent validity from interaction with voter
  - Capture
  - Verify
- Each record gives independent evidence of voter's choices
- Examples: VVPAT, frog protocol from MIT/Caltech report, DRE+camera, DRE+external screen, etc.

Apply to all electronic voting systems in future stds

The Resolutions

- Resolution 12-05: Introduces DV / IV distinction
  - Voter has to get a chance to verify choices
  - DV = voter verifies choices directly
  - IV = voter verifies choices with computer
- Resolution 21-05: Multiple representations
  - Some voting systems produce multiple records of independent validity
  - Examples: VVPAT, Frog Protocol
  - How to reconcile disagreements between records?

DV Systems in Our Framework

- Definition
  - Let voter verify record with own senses (paper)
  - Paper + electronic used in first count
  - Examples: VVPAT of various flavors
- Requirements/Concerns
  - Verify human-readable == scanned-in electronic
  - Error and reliability rates
  - Privacy problems with unshuffled paper
  - Blind / alternative-language voters

IV Systems in Our Framework

- Definition (*Much wider range of systems)*
  - Voter verifies representation of votes via computer equipment (separate for two processes)
  - Examples: Frog protocol, camera+DRE, cryptographic schemes, etc.
- Requirements/Concerns
  - Meaningful independence of processes (Different vendors, OS, HW source, coding tools?)
  - Cryptographic schemes different from all others

DV/IV Roundup

- Distinction less clear than appears at first
  - Most paper systems convert to electronic records for first count—is that DV?
  - Cryptographic schemes provide receipt for later verification (without revealing vote)--is that IV?
- Neither DV nor IV inherently more secure
  - IV better for voter privacy
  - DV harder to fix election in widespread attack
  - Specific attack and attacker resources determine which is better in given situation

Dealing with Multiple Records

- Dual verification architectures don't have a “fundamental representation”
  - Both records have independent validity
  - Always check against each other in normal counting process (full count, auditing/sampling processes)
- Goal: Disagreements Rare and Meaningful
  - Reliability requirement on records (VVPAT problems!)
  - Zero misreads (okay to fail to read, never okay to accidentally misread A as B)
  - Remove ambiguity about damage vs fraud

Important Points on Mult. Repr.

- Neither record can always dominate in disputes
- Records must be reconciled in normal count
  - Full count of all records—easy if electronic
  - Statistical sampling techniques—more complicated, but possible
  - Special DV concern: human readable vs scanned in electronic record
- Records must be kept under separate control
  - No use of same crypto keys, physical custody, same locks/seals, etc.

Conclusions

- Broad Security Framework: Dual Verification
  - Plan: new voting systems shall be Dual Verification
- Addressing DV/IV Within Framework
- Addressing Multiple Representations Within Framework
- Lots of interesting cans of worms:
  - Cryptographic schemes
  - Accomodating disabilities and languages in DV
  - Independent vendor source requirements for IV

A Dual-Verification Voting System