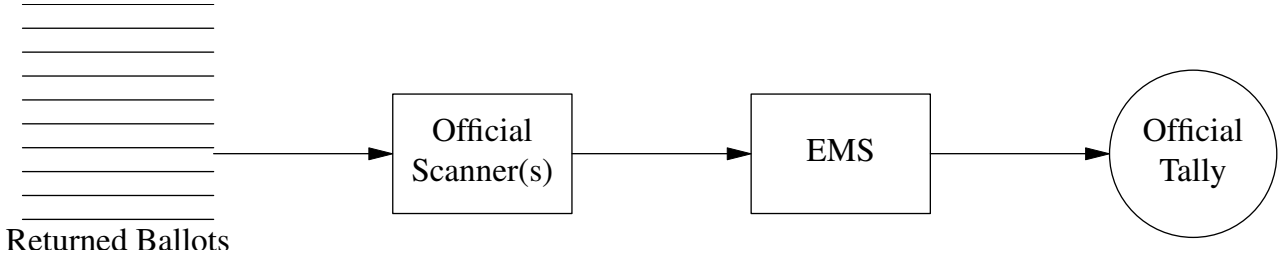
Understanding the Security Properties of Ballot-Based Verification Techniques

Eric Rescorla
ekr@rtfm.com

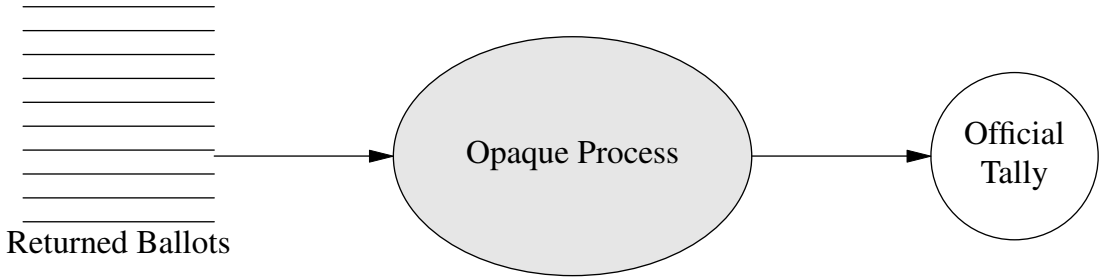
WARNING

This talk contains no research content.

Two views of vote tabulation



The insider's view



The outsider's view

What are we trying to verify?

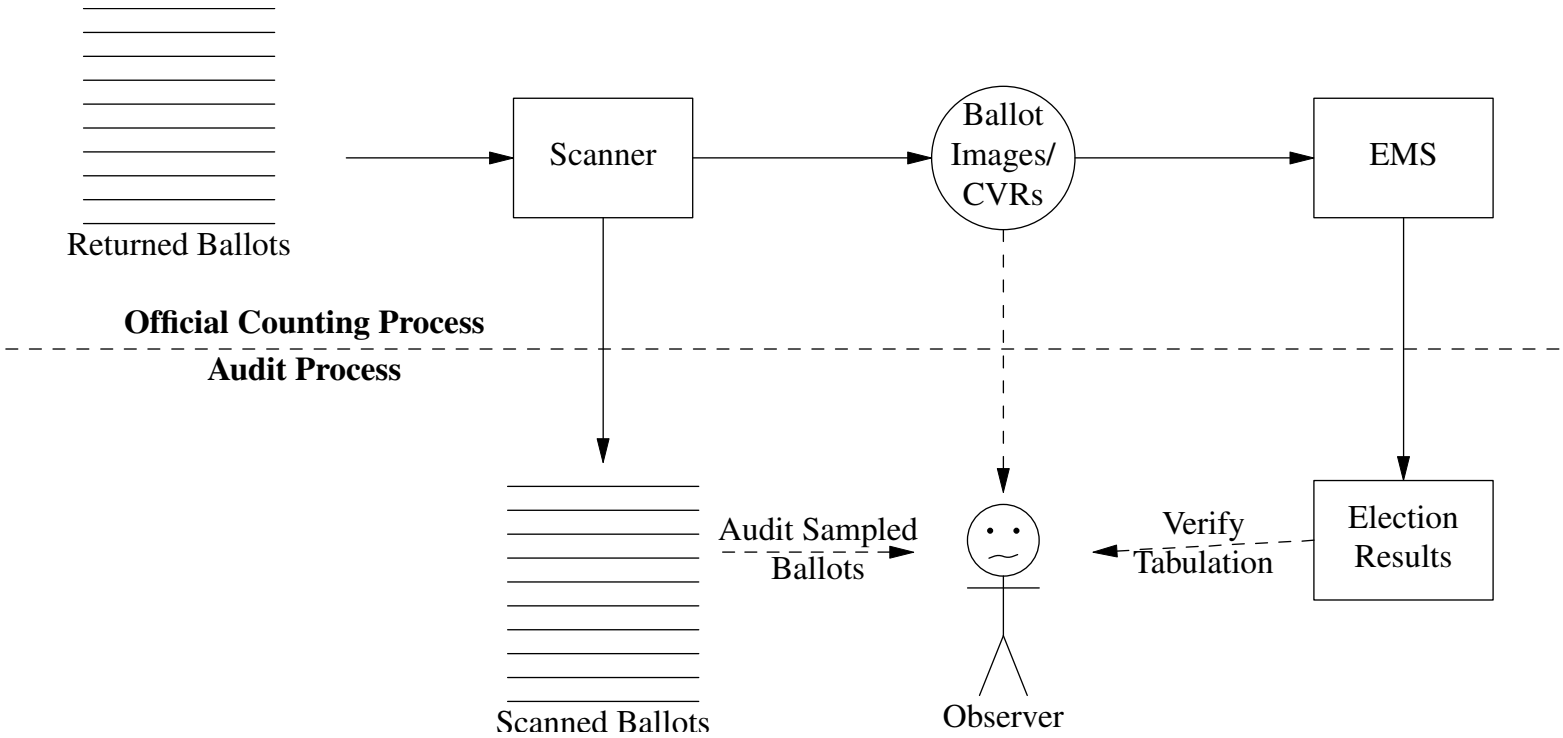
- ~~The votes were correctly counted~~
- ~~The right candidate won~~
- ~~The stack of votes in front of us was correctly counted~~
- ~~A recount of this stack of votes wouldn't change the winner~~
- Third party verifiability: A third party with no special access can verify that a recount of this stack* of votes wouldn't change the winner

* Alert: we are sweeping the topic of ballot chain of custody under the rug.

Why ballot-based audits?

- Statistical power of an audit depends on the number of samples
  - Very little dependency on the size of each sample
  - (Assuming attacker is intelligent)
- Traditional precinct-based audits are not very efficient
- Auditing individual ballots is far more efficient
- Independently proposed several times [CHF07, Nef03, Joh04]

Ballot-Based Auditing Workflow [CHF07]



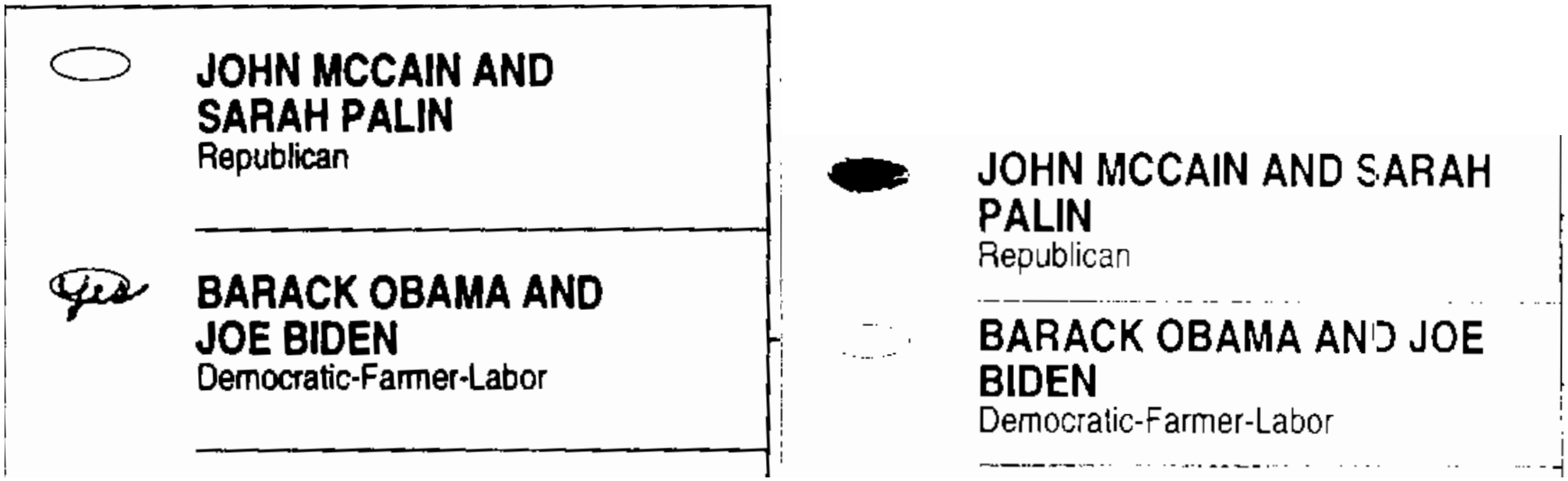
Adapted from [SRW09]

Problems with Ballot-Based Auditing

- Finding individual ballots is hard
  - Possibilities: serial numbers on ballots, hand-indexing, paper counters, weight...
- We need to publish the contents of each ballot (CVR or image)
  - Accessible to any third party
  - The ballots are anonymous but all contents are published
  - This allows coercion and vote buying
    - Easiest if we publish images
    - Pattern voting

What about ballot images?

- Trivial to encode information

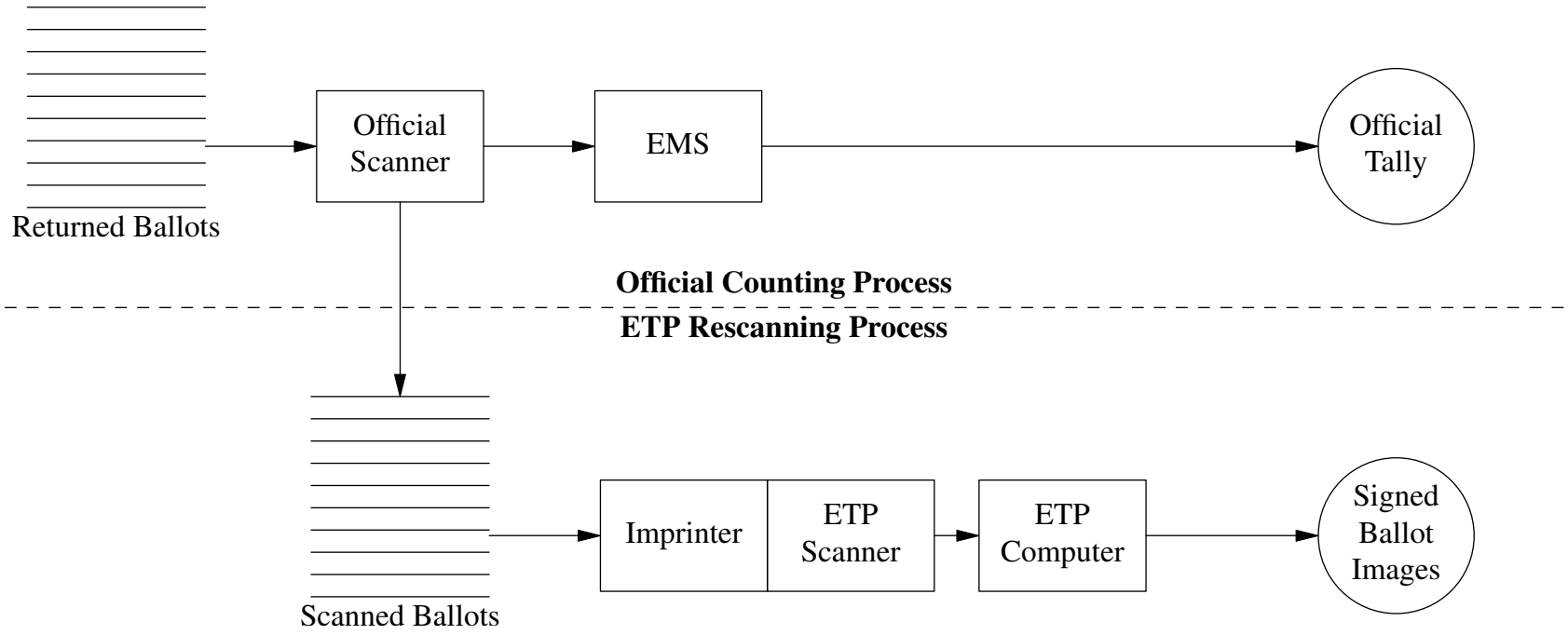


- Even valid marks can encode information
  - Incompletely/overfilled
- Could digitally sanitize
  - You've just turned ballots into CVRs

The Math of Pattern Voting

- Basic idea: encode voter identity in downticket races
  - Assume results are reported by precinct
    - Just need to identify voter within precincts
  - Need to encode no more than 1000-10,000 distinct identities (10-14 bits)
- Each contest lets us encode minimum 1-2 bits
  - Alice, Bob, undervote, overvote(?)
  - 10 contests is enough to encode 60,000–1,000,000 identies

Humboldt Election Transparency Project Workflow



Advantages of ETP Style Approaches

- Fast detection of scanner/EMS errors
  - Requires minimal manual intervention
  - It already has found errors: Deck 0 bug
  - Independent check on compromise of EMS (or scanner) by outsiders
- Backup for physical control of ballots
  - Only applies post-scanning
  - And requires tight control of images or signing key

Does the ETP offer third party verifiability?

- Third parties can independently count the scanned ballots
  - With BallotBrowser or their own software
- This only detects some errors
  - Third parties cannot verify the ETP scanner software
  - What if it substitutes fake ballot images?
  - This cannot be detected by re-processing those images
- Checking the images requires random sampling
  - ... At the same level as a ballot-based audit
- Easiest to think of ETP checking the tabulation

Why digital signatures don't help

- Signatures are applied by the ETP scanning computer [Tra08]
- Third parties can download ballot images
  - And verify that they weren't tampered in transit
- But this doesn't help if the ETP scanner is compromised
  - You're getting fake ballot images that weren't tampered in transit
- Signatures are sort of overkill here
  - Could just publish a message digest in a non-tamperable form (e.g., local paper)

Summary

- Ballot-based auditing systems have far higher statistical power
  - But worse privacy properties (vote buying and coercion)
- Finding the right physical ballot is a challenge
- ETP provides good detection of scanner/EMS error
  - And some kinds of outsider attack
- ... But requires a separate audit for third-party verifiability

References

[CHF07] Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Machine-assisted election auditing. USENIX/ACCURATE Electronic Voting Technology Workshop 2007, August 2007. http://www.usenix.org/events/evt07/tech/full_papers/calandrino/calandrino.pdf.

[Joh04] Kenneth C. Johnson. Election certification by statistical audit of voter-verified paper ballots, October 2004. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=640943.

[Nef03] C. Andrew Neff. Election confidence—a comparison of methodologies and their relative effectiveness at achieving it (revision 6), December 2003. http://web.archive.org/web/20060117190359/http://www.votehere.net/papers/ElectionConfidence.pdf.

[SRW09] Cynthia Sturton, Eric Rescorla, and David Wagner. Weight, Weight, Don't Tell Me: Using Scales to Select Ballots for Auditing. In Joseph Lorenzo Hall, David Jefferson, and Tal Moran, editors, Proceedings of EVT/WOTE 2009. USENIX/ACCURATE/IAVoSS, August 2009. To appear.

[Tra08] Mitch Trachtenberg. Can't Digital Images Be Faked. http://democracycounts.blogspot.com/2008/07/cant-digital-images-be-faked.html, August 2008.