RLAs and my Beefs with BMDs

NVRTF 3rd National Election Integrity Conference
The Coming 2020 Election Crisis: In Paper We Trust
Berkeley, CA

Philip B. Stark

5 October 2019

University of California, Berkeley

Can't have a trustworthy voting system without paper.

Can't have a trustworthy voting system without paper.

Paper isn't enough: how the paper is marked, curated, tabulated, and audited are crucial.

Can't have a trustworthy voting system without paper.

Paper isn't enough: how the paper is marked, curated, tabulated, and audited are crucial.

- Images of ballots are not trustworthy.
- BMD output is not trustworthy.
- No feasible amount of testing can tell whether BMD misbehavior altered election outcomes.

Did the reported winner really win?

- Procedure-based vs. evidence-based elections
  - sterile scalpel v. patient's condition

Did the reported winner really win?

- Procedure-based vs. evidence-based elections
  - sterile scalpel v. patient's condition
- Check equipment? Or check outcomes?

Did the reported winner really win?

- Procedure-based vs. evidence-based elections
  - sterile scalpel v. patient's condition
- Check equipment? Or check outcomes?
- Whom must we trust, and for what?

Why audit?

- *Any* way of counting votes can make mistakes
- *Every* electronic system is vulnerable to bugs, configuration errors, & hacking
- **Did error/bugs/hacking cause losing candidate(s) to appear to win?**

Security properties of paper

- tangible/accountable
- tamper evident
- human readable
- large alteration/substitution attacks generally require many accomplices

Security properties of paper

- tangible/accountable
- tamper evident
- human readable
- large alteration/substitution attacks generally require many accomplices

Not electronic systems nor electronic data, including images.

Image audits

- Digital images of ballots are not a trustworthy record of voter intent.
- Hashes don't help
- Auditing contests against images, then auditing images against paper, requires looking at **more** paper ballots to get the same assurance.
- Examples of hacks that alter images "in flight."
- Examples of scanner firmware altering images.
- No way to tell whether there's one image per ballot, nor whether images are accurate.
- Wastes resources that could be used to check something more meaningful

Auditing outcomes against paper

- If there's a reliable, voter-verified paper trail, can check whether reported winner really won.
- If you permit a small "risk" of not correcting the reported outcome if it is wrong, generally don't need to look at many ballots if outcome is right.

A risk-limiting audit has a known chance of correcting the reported outcome if the reported outcome is wrong (and won't change a correct reported outcome).

A risk-limiting audit has a known chance of correcting the reported outcome if the reported outcome is wrong (and won't change a correct reported outcome).

Risk limit: largest possible chance of *not* correcting reported outcome, if reported outcome is wrong.

A risk-limiting audit has a known chance of correcting the reported outcome if the reported outcome is wrong (and won't change a correct reported outcome).

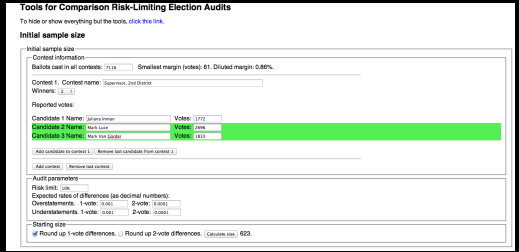
Risk limit: largest possible chance of *not* correcting reported outcome, if reported outcome is wrong.

Worst-case calculation: does not assume anything about how or why the errors occurred.

- Audit enough to have strong evidence reported winner really won.

- Audit enough to have strong evidence reported winner really won.
- "Spoonful of soup": small sample often enough (depends on margin)

- Audit enough to have strong evidence reported winner really won.
- "Spoonful of soup": small sample often enough (depends on margin)
- Should be routine, no matter how big the margin


Tools for Comparison Risk-Limiting Election Audits
To hide or show everything but the tools, click this link.
Initial sample size
Initial sample size
Contest information
Ballots cast in all contests: 7116
Smallest margin (votes): 61. Diluted margin: 0.86%.
Contest 1. Contest name: Supervisor, 2nd District
Winners: 2 ...1
Reported votes:
Candidate 1 Name: Juliana Inman
Votes: 1773
Candidate 2 Name: Mark Luce
Votes: 2898
Candidate 3 Name: Mark Van Gorder
Votes: 1833
Add candidate to contest 1.
Remove last candidate from contest 1.
Add contest.
Remove last contest
Audit parameters
Risk limit: 10%
Expected rates of differences (as decimal numbers):
Overstatements. 1-vote: 0.001
2-vote: 0.0001
Understatements. 1-vote: 0.005
2-vote: 0.0001
Starting size
Round up 1-vote differences.
Round up 2-vote differences.
Calculate size
623.

Requirements

- Voter-verified paper trail
  - Any jurisdiction with paper can do an RLA
  - Need to ensure the paper trail is trustworthy
  - Some equipment makes it *easier*, but replacing equipment isn't necessary

Requirements

- Voter-verified paper trail
  - Any jurisdiction with paper can do an RLA
  - Need to ensure the paper trail is trustworthy
  - Some equipment makes it *easier*, but replacing equipment isn't necessary
- "Ballot manifest": description of how ballots are stored
  - Should be routine
  - "It's the day after the election. Do you know where your ballots are?"

Requirements

- Voter-verified paper trail
  - Any jurisdiction with paper can do an RLA
  - Need to ensure the paper trail is trustworthy
  - Some equipment makes it *easier*, but replacing equipment isn't necessary
- "Ballot manifest": description of how ballots are stored
  - Should be routine
  - "It's the day after the election. Do you know where your ballots are?"
- Manually inspect randomly selected paper ballots
  - individual ballots, batches, unstratified, stratified, w/ or w/o replacement
  - polling audits: just need ballots
  - comparison audits: also need to export data & check totals

Requirements

- Voter-verified paper trail
  - Any jurisdiction with paper can do an RLA
  - Need to ensure the paper trail is trustworthy
  - Some equipment makes it *easier*, but replacing equipment isn't necessary
- "Ballot manifest": description of how ballots are stored
  - Should be routine
  - "It's the day after the election. Do you know where your ballots are?"
- Manually inspect randomly selected paper ballots
  - individual ballots, batches, unstratified, stratified, w/ or w/o replacement
  - polling audits: just need ballots
  - comparison audits: also need to export data & check totals
- Routine in CO and soon RI; pilots in 9 states and Denmark
- laws in CA, OR, NV, VA

BMDs

- “electronic pen”

BMDs

- “electronic pen”
- can present ballots in many languages, “accessible” interface

BMDs

- “electronic pen”
- can present ballots in many languages, “accessible” interface
- what if they malfunction or are misconfigured or hacked?

- research so far:
  - few voters check BMD printout
  - checks too brief to help
  - voters can't remember selections or even contests

- if astute voter catches error:
  - might get a fresh ballot
  - has no evidence to prove malfunction, only claim
  - presumption will be voter error, not machine error
  - fresh ballot doesn't ensure correct outcome overall
  - even a small rate of uncorrected BMD problems can change outcomes

- if astute voter catches error:
  - might get a fresh ballot
  - has no evidence to prove malfunction, only claim
  - presumption will be voter error, not machine error
  - fresh ballot doesn't ensure correct outcome overall
  - even a small rate of uncorrected BMD problems can change outcomes
- if pollworker convinced, what recourse is there?
  - new election? (no way to find correct outcome)
  - "wolf!"

BMDs need to be designed to allow disputes to be resolved

- If voter observes malfunction, should be able to prove it to others*

BMDs need to be designed to allow disputes to be resolved

- If voter observes malfunction, should be able to prove it to others*
- If LEO has evidence that the outcome is still correct, should be able to prove it to public*

(*Without compromising the anonymity of votes.)

- BMD printout might not match what voters indicated to the BMD.
- RLA of elections conducted on BMDs may confirm the wrong winner.
- "Parallel testing" requires unworkable sample sizes (& labor, training, equipment, infrastructure).

- BMD printout might not match what voters indicated to the BMD.
- RLA of elections conducted on BMDs may confirm the wrong winner.
- "Parallel testing" requires unworkable sample sizes (& labor, training, equipment, infrastructure).

Current BMDs can be hacked undetectably and alter outcomes: not *software independent*.

Useful ideas for election integrity and security

- (Strong) software independence

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections
- End-to-end verifiability

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections
- End-to-end verifiability
- Contestability

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections
- End-to-end verifiability
- Contestability
- Defensibility

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections
- End-to-end verifiability
- Contestability
- Defensibility

5 Cs

- *Create* durable, trustworthy record of voter intent
  - ideally, hand-marked paper ballots + BMDs for voters who benefit from them
- *Care* for the paper record
  - verifiable chain of custody, 2-person custody rules, ballot accounting, good seal protocols, etc.
- *Compliance* audit: establish whether paper trail is trustworthy
  - ballot accounting including VRDB, pollbooks, etc.; check chain of custody logs, video, etc.; eligibility
- *Check* reported outcome against the paper by auditing
- *Correct* the reported outcome if it is wrong

Rant on Voting Systems

- Current best voting system: optically scanned hand-marked paper ballots, with BMDs for accessibility
  - It can generate the strongest evidence that the reported winner(s) really won, while being as accessible as current technology permits.
- Current commercial BMDs are terrible.
  - Testing in PA has shown that voters with disabilities cannot independently cast votes using current BMDs.
  - VSAP might be better; I don't have an opinion yet.
  - We need better options for accessibility
- Some BMD designs are much worse than others: all-in-one, etc.

- Voters make mistakes hand-marking ballots. But those are *their* mistakes.
- Making voters an essential part of the security of the voting system is a really bad idea
  - Voters aren't good at it
  - BMDs make voters responsible for system security, but don't give the voters evidence they can use to prove that the system misbehaved.
  - If election officials believe voters who report malfunctions, only recourse is to hold a new election: there's no way to figure out who really won.
- Systems that rely on BMDs are not strongly software independent; arguably, they are not even software independent.

- Deploying BMDs for all voters is a bad idea for many reasons, including cost, security, and vulnerability to failures that halt voting.
- The way elections are run in the US, outcome-altering BMD malfunctions have little or no chance of being caught. Because hacking, misconfiguration, or malfunction could cause BMD printout not to reflect voter intent, election integrity is maximized by minimizing the use of BMDs.
- Parallel "live" testing of BMDs can't offer much
  - the amount of testing needed to have a good chance of detecting outcome-altering problems would leave no time for voting
  - Would require new infrastructure, extra machines, more staff, and more training.
  - If parallel testing uncovers a problem, only recourse is a new election.

- BMD printout does not need to have barcodes or QR codes, and such codes add vulnerabilities (e.g., hacking through QR codes or embedding identifying information) and compound moral hazard for election officials (tempting them to base recounts and audits on the QR codes instead of on the human-readable printing).
- The alternative to QR codes isn't OCR, it's pattern recognition, which is a much easier problem (there are only so many candidate names on a ballot).
- BMD printout should be difficult to distinguish from a hand-marked ballot, to protect the anonymity of votes. That means BMD printout should be a full-face ballot, not a summary, and should not have barcodes. Marks indicating selections should be printed to look like they were handmade.

- There should be air-gapped stations that provide an accessible way for voters to check whether the human-readable printing on the ballot accurately reflects their intentions.
  - Voters should be permitted to bring their own accessible technology to read their marked ballots.
- Every voter should be urged to double-check before casting the ballot.
- Ballot design is critical, both for BMDs and for hand-marked paper ballots. It's easy to design a ballot that makes it hard to vote accurately.

“The cyber”

- Voting machines should not have wireless networking, including WiFi, Bluetooth, and cellular modems.
- Voting systems should not have remote desktop software.
- Voting systems should not be connected to the internet, even through a firewall.
- Appropriate cybersecurity hygiene should be used for any removable storage devices (flash drives, USB memory, etc.) involved in moving data to or from voting systems and voting machines.

The law

- None of this matters if there are not good laws for audits and recounts. In particular, audits and recounts should require manually inspecting *paper ballots* and ascertaining voter intent from the human-readable print on the ballots (not, for instance, using digital images of ballots or using QR codes on paper ballots).
- Digital images of ballots are an inherently untrustworthy record of voter intent, whether the images are hashed or not. Examining images cannot confirm outcomes.
- Every contest should receive some auditing. Most or all contests should be subject to a RLA with a reasonable risk limit. A RLA is the lowest reasonable standard for accuracy: was the tally accurate enough to determine (with high confidence) who won? Higher standards might be desirable, but we should be willing to audit enough to have strong evidence that the reported winners really got the most votes.

Physical security

- Audits and recounts don't help unless the paper trail is trustworthy.
- Need much stronger laws around ballot security, accountability, and chain of custody.
- We need routine "compliance audits" to establish whether the paper trail is trustworthy.