Evidence-Based Elections: The Role of Risk-Limiting Audits

Election Integrity in the Networked Information Era Georgetown Law Washington, DC

Philip B. Stark 7 February 2020

University of California, Berkeley

- Physical security
- Not connected to the Internet
- Tested before election day
- Too decentralized

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

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

How the paper is marked, curated, tabulated, and audited are crucial.

Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters

28 Pages · Posted: 21 May 2019 · Last revised: 4 Jan 2020

Andrew Appel Princeton University

Richard DeMillo Georgia Institute of Technology

Philip Stark University of California, Berkeley

Date Written: April 21, 2019

Abstract

Computers, including all modern voting systems, can be hacked and misprogrammed. The scale and complexity of U.S. elections may require the use of computers to count ballots, but election integrity requires a paper-ballot voting system in which, regardless of how they are initially counted, ballots can be re- counted by hand to check whether election outcomes have been altered by buggy or hacked software. Furthermore, secure voting systems must be able to recover from any errors that might have occurred.

However, paper ballots provide no assurance unless they accurately record the vote as the voter expresses it.

Did the reported winner really win?

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

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

• Voters *CREATE* complete, durable, voter-verified audit trail.

- Voters *CREATE* complete, durable, voter-verified audit trail.
- LEO CARES FOR the audit trail adequately to ensure it remains demonstrably trustworthy.

- Voters *CREATE* complete, durable, voter-verified audit trail.
- LEO CARES FOR the audit trail adequately to ensure it remains demonstrably trustworthy.
- Verifiable, rigorous audit CHECKS reported results against the trustworthy paper trail.

- Can catch & correct wrong outcomes by manually tabulating the trustworthy paper trail.
- 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.

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

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

Wrong means accurate handcount of *trustworthy* paper trail would find different winner(s).

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

Wrong means accurate handcount of *trustworthy* paper trail would find different winner(s).

Trustworthy means a full hand count would show the will of the (eligible) voters who voted.

No way to limit the risk if there is not a trustworthy paper trail.

RLA corrects the outcome by conducting a full hand count.

No way to limit the risk if there is not a trustworthy paper trail.

- RLA corrects the outcome by conducting a full hand count.
- If paper trail is not trustworthy, full hand count might show the wrong winner(s).

No way to limit the risk if there is not a trustworthy paper trail.

- RLA corrects the outcome by conducting a full hand count.
- If paper trail is not trustworthy, full hand count might show the wrong winner(s).
- BMD printout is not trustworthy: hackable, not voter-verified.

• Keep looking at more ballots until there's strong evidence that a full handcount would confirm the results.

- Keep looking at more ballots until there's strong evidence that a full handcount would confirm the results.
- If the audit becomes a full handcount, the results of the handcount replace the reported result.

The National Academies of



Home



Elections should be conducted with human-readable paper ballots. Paper ballots form a body of evidence that is not subject to manipulation by faulty software or hardware and that can be used to audit and verify the results of an election. Human-readable paper ballots may be marked by hand or by machine (using a ballot-marking device), and they may be counted by hand or by machine (using an optical scanner), the report says. Voters should have an opportunity to review and confirm their selections before depositing the ballot for tabulation. Voting machines that do not provide the capacity for independent auditing – i.e., machines that do not produce a printout of a voter's selections that can be verified by the voter and used in audits – should be removed from service as soon as possible.

States should mandate a specific type of audit known as a "risk-limiting" audit prior to the certification of election results. By examining a statistically appropriate random sample of paper ballots, risk-limiting audits can determine with a high level of confidence whether a reported election outcome reflects a correct tabulation Endorsed by NASEM, PCEA, ASA, LWV, VV, CC, ...

- Endorsed by NASEM, PCEA, ASA, LWV, VV, CC,
- Most efficient RLA options: ballot-polling and ballot-level comparison

- Like an exit poll, but of ballots, not voters.
- Large-enough majority for the reported winner in a large-enough random sample is strong evidence reported winner really won.
- Arithmetic simple: can check w/ pencil & paper.
- Requires paper ballots, but no special requirements on voting machines.

 If reported outcome is right, the number of ballots an RLA inspects before stopping is typically very small (unless the margin is microscopic).

- If reported outcome is right, the number of ballots an RLA inspects before stopping is typically very small (unless the margin is microscopic).
- Tablespoon of soup suffices.

- 255 state-level pres. races, 1992–2012, 10% risk limit
 - BPA expected to examine fewer than 308 ballots for half.

- 255 state-level pres. races, 1992–2012, 10% risk limit
 - BPA expected to examine fewer than 308 ballots for half.
- 2016 presidential election, 5% risk limit
 - BPA expected to examine ~700k ballots nationally (<0.5%)

- ~50 pilot audits in CA, CO, GA, IN, MI, NJ, OH, OR, PA, RI, WA, VA, DK.
- CA counties: Alameda, El Dorado, Humboldt, Inyo, Madera, Marin, Merced, Monterey, Napa, San Luis Obispo, Santa Cruz, Stanislaus, Ventura, Yolo
- AL, MO pilots planned.
- Laws in CO, RI, VA, WA; CA has pilot laws

- ballots (25% of US voters don't have)
- ballot manifest
- good, transparent, verifiable source of randomness
 - 20 public rolls of translucent 10-sided dice



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

- End-to-end verifiability
- Contestability
- Defensibility