Evidence-Based Elections

Securing the Election Infrastructure: Challenges and Opportunities
IEEE International Conference on Collaboration and Internet Computing

---

Philip B. Stark

15 December 2022

University of California, Berkeley

Half of Republicans say Biden won because of a 'rigged' election: Reuters/Ipsos poll

By Chris Kahn

3 MIN READ

(Reuters) - About half of all Republicans believe President Donald Trump "rightfully won" the U.S. election but that it was stolen from him by widespread voter fraud that favored Democratic President-elect Joe Biden, according to a new Reuters/Ipsos opinion poll.

The Nov. 13-17 opinion poll showed that Trump's open defiance of Biden's victory in both the popular vote and Electoral College appears to be affecting the public's confidence in American democracy, especially among Republicans.

Hand-marked paper ballots, kept physically secure, are key

- US elections neither *tamper evident* nor *resilient*.
- Need systems/procedures that can provide *affirmative* evidence that the reported winners really won.
- *Every* electronic system is vulnerable to bugs, configuration errors, & hacking.
- Security properties of paper
  - tangible/accountable
  - tamper evident
  - human readable
  - large alteration/substitution attacks require physical access & many accomplices
  - not all paper records are trustworthy

Election Law Journal: Rules, Politics, and Policy, VOL. 19, NO. 3 | Original Research Articles

normal

Ballot-Marking Devices Cannot Ensure the Will of the Voters

Andrew W. Appel, Richard A. DeMillo, and Philip B. Stark

Published Online: 17 Sep 2020 | https://doi.org/10.1089/elj.2019.0619

Tools Share

Abstract

The complexity of U.S. elections usually requires computers to count ballots—but computers can be hacked, so election integrity requires a voting system in which paper ballots can be recounted by hand. However, paper ballots provide no assurance unless they accurately record the votes as expressed by the voters.

Voters can express their intent by indelibly hand-marking ballots or using computers called ballot-marking devices (BMDs). Voters can make mistakes in expressing their intent in either technology, but only BMDs are also subject to hacking, bugs, and misconfiguration of the software that prints the marked ballots. Most voters do not review BMD-printed ballots, and those who do often fail to notice when the printed vote is not what they expressed on the touchscreen. Furthermore, there is no action a voter can take to demonstrate to election officials that a BMD altered their expressed votes, nor is there a corrective action that election officials can take if notified by voters—there is no way to deter, contain, or correct computer hacking in BMDs. These are the essential security flaws of BMDs.

Risk-limiting audits can ensure that the votes recorded on paper ballots are tabulated correctly, but no audit can ensure that the votes on paper are the ones expressed by the voter on a touchscreen: Elections conducted on current BMDs cannot be confirmed by audits. We identify two properties of voting systems, *contestability* and *defensibility*, necessary for audits to confirm election outcomes. No available BMD certified by the Election Assistance Commission is contestable or defensible.

They may look and look, yet not see: BMDs cannot be tested adequately

Philip B. Stark, Ran Xie

Bugs, misconfiguration, and malware can cause ballot-marking devices (BMDs) to print incorrect votes. Several approaches to testing BMDs have been proposed. In logic and accuracy testing (LAT) and parallel or live testing, auditors input known test votes into the BMD and check the printout. Passive testing monitors the rate of "spoiled" BMD printout, on the theory that if BMDs malfunction, the rate will increase noticeably. We show that these approaches cannot reliably detect outcome-altering problems, because: (i) The number of possible interactions with BMDs is enormous, so testing interactions uniformly at random is hopeless. (ii) To probe the space of interactions intelligently requires an accurate model of voter behavior, but because the space of interactions is so large, building an accurate model requires observing a huge number of voters in every jurisdiction in every election—more voters than there are in most jurisdictions. (iii) Even with a perfect model of voter behavior, the number of tests needed exceeds the number of voters in most jurisdictions. (iv) An attacker can target interactions that are expensive to test, e.g., because they involve voting slowly; or interactions for which tampering is less likely to be noticed, e.g., because the voter uses the audio interface. (v) Whether BMDs misbehave or not, the distribution of spoiled ballots is unknown and varies by election and possibly by ballot style: historical data do not help much. Hence, there is no way to calibrate a threshold for passive testing, e.g., to guarantee at least a 95% chance of noticing that 5% of the votes were altered, with at most a 5% false alarm rate. (vi) Even if the distribution of spoiled ballots were known to be Poisson, the vast majority of jurisdictions do not have enough voters for passive testing to have a large chance of detecting problems but only a small chance of false alarms.

- Hand-marked paper ballots are a record of what the voter did.
- Machine-marked paper ballots are a record of what the machine did.
- Few voters check BMD printout; fewer notice errors.
- Voters who notice problems have no evidence to convince others: open security loop.
- Even if EO is convinced of problems, no way to determine correct outcome.

Evidence-Based Elections

P.B. Stark and D.A. Wagner

***Abstract*—We propose an alternative to current requirements for certifying voting equipment and conducting elections. We argue that elections should be structured to provide convincing affirmative evidence that the reported outcomes actually reflect how people voted. This can be accomplished with a combination of software-independent voting systems, compliance audits, and risk-limiting audits. Together, these yield a resilient canvass framework: a fault-tolerant approach to conducting elections that gives strong evidence that the reported outcome is correct or reports that the evidence is not convincing. We argue that, if evidence-based elections are adopted, certification and testing of voting equipment can be relaxed, saving money and time and reducing barriers to innovation in voting systems—and election integrity will benefit. We conclude that there should be more regulation of the evidence trail and less regulation of equipment, and that compliance audits and risk-limiting audits should be required.**

***Keywords*-elections, software-independent voting system, risk-limiting audit, resilient canvass framework EDICS SEC-INTE, APP-CRIM, APP-INTE, APP-OTHE.**

I. Introduction

IDEALLY, what should an election do? Certainly, an election should find out who won, but we believe it also should produce convincing evidence that it found the real winners—or report that it cannot. This is not automatic; it requires thoughtful design of voting equipment, carefully planned and implemented voting and vote counting processes, and rigorous post-election auditing.

While approximately 75% of US voters currently vote on equipment that produces a voter-verifiable paper record of the vote, about 25% vote on paperless electronic voting machines that do not produce such a record [1].

Because paperless electronic voting machines rely upon complex software and hardware, and because there is no feasible way to ensure that the voting software is free of bugs or that the hardware is executing the proper software, there is no guarantee that electronic voting machines record the voter's votes accurately. And, because paperless voting machines preserve only an electronic record of the vote that cannot be directly observed by voters, there is no way to produce convincing evidence that the electronic record accurately reflects the voters' intent. Internet voting shares the shortcomings of paperless electronic voting machines, and has additional vulnerabilities.

Numerous failures of electronic voting equipment have been documented. Paperless voting machines in Carteret County, North Carolina irretrievably lost 4,400 votes; other machines in Mecklenburg, North Carolina recorded 3,955 more votes than the number of people who voted; in Bernalillo County, New Mexico, machines recorded 2,700 more votes than voters; in Mahoning County, Ohio, some machines reported a negative total vote count; and in Fairfax, Virginia, county officials found that for every hundred or so votes cast for one candidate, the electronic voting machines subtracted one vote for her [2]. In short, when elections are conducted on paperless voting

Evidence-Based Elections: Create a Meaningful Paper Trail, Then Audit

Andrew W. Appel* & Philip B. Stark**

Cite as: 4 Geo. L. Tech. Rev. 523 (2020)

Table of Contents

Evidence-Based elections: trustworthy paper + risk-limiting audits

RLA: any procedure w/ a known maximum chance of not correcting the reported outcome if it's wrong & never changes correct outcomes.

Evidence-Based elections: trustworthy paper + risk-limiting audits

RLA: any procedure w/ a known maximum chance of not correcting the reported outcome if it's wrong & never changes correct outcomes.

Risk limit: max chance of *not* correcting reported outcome if it's wrong, no matter why it's wrong.

Evidence-Based elections: trustworthy paper + risk-limiting audits

RLA: any procedure w/ a known maximum chance of not correcting the reported outcome if it's wrong & never changes correct outcomes.

Risk limit: max chance of *not* correcting reported outcome if it's wrong, no matter why it's wrong.

RLA corrects wrong outcomes via a full hand count of trustworthy paper trail.

Evidence-Based elections: trustworthy paper + risk-limiting audits

RLA: any procedure w/ a known maximum chance of not correcting the reported outcome if it's wrong & never changes correct outcomes.

Risk limit: max chance of *not* correcting reported outcome if it's wrong, no matter why it's wrong.

RLA corrects wrong outcomes via a full hand count of trustworthy paper trail.

Can't limit risk w/o trustworthy vote records.

Evidence-Based elections: trustworthy paper + risk-limiting audits

RLA: any procedure w/ a known maximum chance of not correcting the reported outcome if it's wrong & never changes correct outcomes.

Risk limit: max chance of *not* correcting reported outcome if it's wrong, no matter why it's wrong.

RLA corrects wrong outcomes via a full hand count of trustworthy paper trail.

Can't limit risk w/o trustworthy vote records.

Establishing whether paper trail is trustworthy involves other processes incl. canvass, ballot accounting, pollbook/participation reconciliation, eligibility verification, secure chain of custody, etc.

The National Academies of SCIENCES ENGINEERING MEDICINE

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

Risk-Limiting Audits

- Endorsed by NASEM, PCEA, ASA, LWV, CC, VV, ...
- ~60 pilot audits in AK, CA, CO, GA, IN, KS, MI, MT, NJ, OH, OR, PA, RI, WA, WY, VA, DK.
- CA counties: Alameda, El Dorado, Humboldt, Inyo, Madera, Marin, Merced, Monterey, Napa, Orange, San Francisco, San Luis Obispo, Santa Clara, Santa Cruz, Stanislaus, Ventura, Yolo.
- Routine statewide in CO since 2017. Statewide audits in AK, KS, WY in 2020.
- Laws (of varying quality) in CA, CO, CT, GA, NV, NJ, OH, OR, RI, TX, VA, WA

Wrinkles

- ~20% of U.S. voters don't vote on paper
- jurisdictions adopting universal-use BMDs: paper trail untrustworthy
- inadequate chain of custody & canvass (physical ballot accounting, pollbook & participation reconciliation, eligibility verification, . . .)
- missing ballots; imperfect manifests (Bañuelos & Stark 2012)
- producing CVRs linked to ballots while preserving vote anonymity (SOBA, VAULT, Non(c)esuch); redacted CVRs
- preserve vote anonymity but provide public evidence the audit didn't stop too soon

- auditing some contests doesn't ensure any other contest results are correct: need to look at every contest.
- laws & industry of "Cargo-cult RLAs" that go through some of the motions of an RLA but don't actually limit the risk that wrong outcomes will be certified, generally b/c paper trail is untrustworthy (how it's created and/or curated): distraction from bigger problems. Viz, GA in 2020 & 2022.
- applying RLA procedures to untrustworthy paper is like building the penthouse of a skyscraper before the foundation
- even some experts are confused about the difference between *fault detection* and *affirmative evidence*

Evidence-Based Elections: 3 C's

- Voters *CREATE* complete, durable, verified, trustworthy audit trail.
- LEO *CARES FOR* the audit trail adequately to ensure it remains complete and accurate.
- Verifiable audit *CHECKS* reported results against the paper & *CORRECTS* outcome if wrong

Appropriate uses of technology in Elections

Use only in ways that malfunctions can be detected reliably and corrected.


411412
411413
411418
421224
421422
421222
421225
421226
511221
521225
561341