Risk-Limiting Audits and Evidence-Based Elections

Joint Berkeley/Davis Statistics Colloquium
Sheltered in Place

Philip B. Stark

21 April 2020

University of California, Berkeley

Many collaborators including (most recently) Andrew Appel, Josh Benaloh, Matt Bernhard, Michelle Blom, Andrew Conway, Rich DeMillo, Steve Evans, Amanda Glazer, Alex Halderman, Mark Lindeman, Kellie Ottoboni, Ron Rivest, Peter Ryan, Jake Spertus, Peter Stuckey, Vanessa Teague, Poorvi Vora

https://www.youtube.com/embed/cruh2p_Wh_4

Video Channels

The Washington Post
Democracy Dies in Darkness

WASHINGTON POST LIVE > WASHINGTON POST LIVE · October 6, 2016

EAC Commissioner: It would take an army to hack into our voting system

The Recorded Future Blog

Russian-Speaking Hacker Selling Access to the US Election Assistance Commission

Posted in Cyber Threat Intelligence by Andrei Barysevich on December 15, 2016

Arguments that US elections can't be hacked:

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

Arguments that US elections can't be hacked:

- Physical security
  - "sleepovers," unattended equipment in warehouses, school gyms, ...
  - locks use minibar keys
  - bad/no seal protocols, easily defeated seals
  - no routine scrutiny of custody logs, 2-person custody rules, ...
- Not connected to the Internet
- Tested before election day
- Too decentralized

Arguments that US elections can't be hacked:

- Physical security
- Not connected to the Internet
  - remote desktop software
  - wifi, bluetooth, cellular modems, ... https://tinyurl.com/r8cseun
  - removable media used to configure equipment & transport results
    - Zip drives
    - USB drives. Stuxnet, anyone?
  - parts from foreign manufacturers, including China; Chinese pop songs in flash
- Tested before election day
- Too decentralized

The New York Times

Russia Targeted Election Systems in All 50 States, Report Finds

A voter casting his ballot in the midterm elections last year in Medina, N.D. Hilary Swift for The New York Times

By David E. Sanger and Catie Edmondson

July 25, 2019

716

WASHINGTON — The Senate Intelligence Committee concluded Thursday that election systems in all 50 states were targeted by Russia in 2016, an

Remote Access Statement | Election Systems & Software

https://essvote.com/media-center/press-statements/remote-access-statement/

ES&S voting machines across the nation do not have any form of **remote access** capability. **ES&S** has never **installed** remote connection **software** on any vote ...

Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States

Remote-access software and modems on election equipment 'is the worst decision for security short of leaving ballot boxes on a Moscow street corner.'

By **Kim Zetter**

Jul 17 2018, 5:00am Share Tweet Snap

IMAGE: SHUTTERSTOCK

The nation's top voting machine maker has admitted in a letter to a federal lawmaker that the company installed remote-access software on election-management systems it sold over a period of six years, raising questions about the security of those systems and the integrity of elections that were conducted with them.

In a letter sent to Sen. Ron Wyden (D-OR) in April and obtained recently by Motherboard, Election Systems and Software acknowledged that it had "provided pcAnywhere remote connection software ... to a small number of customers between 2000 and 2006," which was installed on the election-management system ES&S sold them.

Voting Machine Hacking Village

Report on Cyber Vulnerabilities in

U.S. Election Equipment, Databases, and Infrastructure

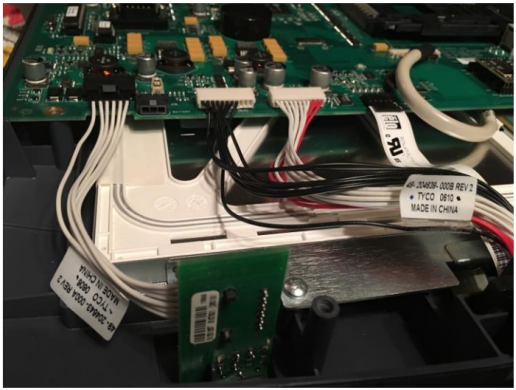
September 2017

Co-authored by:
Matt Blaze, University of Pennsylvania
Jake Braun, University of Chicago & Cambridge Global Advisors
Harri Hursti, Nordic Innovation Labs
Joseph Lorenzo Hall, Center for Democracy & Technology
Margaret MacAlpine, Nordic Innovation Labs
Jeff Moss, DEFCON

The results were sobering. **By the end of the conference, every piece of equipment in the Voting Village was effectively breached in some manner. Participants with little prior knowledge and only limited tools and resources were quite capable of undermining the confidentiality, integrity, and availability of these systems**, including:

- The first voting machine to fall – an AVS WinVote model – was hacked and taken control of remotely in a matter of minutes, using a vulnerability from 2003, meaning that for the entire time this machine was used from 2003-2014 it could be completely controlled remotely, allowing changing votes, observing who voters voted for, and shutting down the system or otherwise incapacitating it.
- That same machine was found to have an unchangeable, universal default password – found with a simple Google search – of "admin" and "abcde."
- An "electronic poll book", the Diebold ExpressPoll 5000, used to check in voters at the polls, was found to have been improperly decommissioned with live voter file data still on the system; this data

Moreover, a closer physical examination of the machines found, as expected, multiple cases of foreign-manufactured internal parts (including hardware developed in China), highlighting the serious possibility of supply chain vulnerabilities. This discovery means that a hacker's point-of-entry into an entire make or model of voting machine could happen well before that voting machine rolls off the production line. With an ability to infiltrate voting infrastructure at any point in the supply chain process, then the ability to synchronize and inflict large-scale damage becomes a real possibility. Also, as expected, many of these systems had extensive use of binary software for subcomponents that could completely control the behavior of the system and information flow, highlighting the need for greater use of trusted computing elements to limit the effect of malicious software. In other words, a nation-state actor with resources, expertise and motive – like Russia – could exploit these supply chain security flaws to plant malware into the parts of every machine, and indeed could breach vast segments of U.S. election infrastructure remotely, all at once.



DEF CON 27 Voting Village Report!

Posted 9.26.19

The DEF CON Voting Village has released its findings from DEF CON 27!

This is the third year we've hosted the Voting Village, and this year we were able to give attendees access to over 100 machines, all of which are currently certified for use in at least one US jurisdiction. The units tested included direct-recording electronic (DRE) voting machines, electronic poll books, Ballot Marking Devices (BMDs), Optical scanners and Hybrid systems.

The hackers at DEF CON once again compromised every single machine over the 2.5 day event, many of them with trivial attacks that require no sophistication or special knowledge on the part of the attacker. In too many cases

Arguments that US elections can't be hacked:

- Physical security
- Not connected to the Internet
- Tested before election day
  - Dieselgate, anyone?
  - Northampton, PA
  - Los Angeles, CA VSAP
- Too decentralized

Expensive, Glitchy Voting Machines Expose 2020 Hacking Risks

Paper ballots may be safer and cheaper, but local officials swoon at digital equipment.

By Kartikay Mehrotra and Margaret Newkirk
November 8, 2019, 12:30 PM PST

A man casts his ballot at polling station in New Jersey in 2016. *Photographer: Eduardo Munoz Alvarez/AFP via Getty Images*

The first sign something was wrong with Northampton County, Pennsylvania's state-of-the-art voting system came on Election Day when a voter called the local Democratic Party chairman to say a touchscreen in her precinct was acting "finicky." As she scrolled down the ballot, the tick-marks next to candidates she'd selected kept disappearing.

(Bloomberg) -- The first sign something was wrong with Northampton County, Pennsylvania's state-of-the-art voting system came on Election Day when a voter called the local Democratic Party chairman to say a touchscreen in her precinct was acting "finicky." As she scrolled down the ballot, the tick-marks next to candidates she'd selected kept disappearing.

Her experience Nov. 5 was no isolated glitch. Over the course of the day, the new election machinery, bought over the objections of cybersecurity experts, continued to malfunction. Built by Election Systems & Software, the ExpressVote XL was designed to marry touchscreen technology with a paper-trail for post-election audits. Instead, it created such chaos that poll workers had to crack open the machines, remove the ballot records and use scanners summoned from across state lines to conduct a recount that lasted until 5 a.m.

In one case, it turned out a candidate that the XL showed getting just 15 votes had won by about 1,000. Neither Northampton nor ES&S know what went wrong.

In Philadelphia, a three-person election commission discounted cybersecurity warnings and, in February, selected ExpressVote XL from ES&S after a massive lobbying effort. It has a 32-inch touchscreen at a cost of $29 million, or $27.59 per voter, not including roughly $3.8 million over 10 years in fees.

But the decision raised suspicions. State Auditor General Eugene DePasquale noted that the request for proposals appeared to favor equipment of the XL's type and size. An investigation by City Controller Rebecca Rhynhart later found that ES&S had courted the tiny commission for six years, spending almost half a million dollars lobbying it. The company paid a $2.9 million penalty—the highest in Philadelphia history—for failing to disclose lobbying on bid documents, according to the city controller's office.

2020 ELECTIONS

Los Angeles County's risky voting experiment

The nation's most populous county is debuting new voting technology that has drawn scrutiny.

By KIM ZETTER
03/03/2020 04:30 AM EST

In November 2018, potential voters wait in long lines to register and vote at the Los Angeles County Registrar's office. | Mark J. Terrill, File/AP Photo

Los Angeles County spent nine years working on a government-designed and -owned voting system with the goal of setting a new standard for security, reliability and transparency.

Instead, millions of county voters on Super Tuesday will cast ballots on a system in which numerous security flaws were found. This has prompted some election integrity experts to call for barring the system from elections until they're fully resolved. The issues include multiple digital and physical vulnerabilities, some of them identified in a recent assessment by California's secretary of state and others identified by outside computer security

nty-voting...

Arguments that US elections can't be hacked:

- Physical security
- Not connected to the Internet
- Tested before election day
- Too decentralized
  - market concentrated: few vendors/models in use
  - vendors & EAC have been hacked
  - demonstration viruses that propagate across voting equipment
  - "mom & pop" contractors program thousands of machines, no IT security
  - changing presidential race requires changing votes in only a few counties
  - small number of contractors for election reporting
  - many weak links

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 all paper is trustworthy: How paper is marked, curated, tabulated, & audited are crucial.

Mother Jones

Smart, Fear

POLITICS ENVIRONMENT CRIME AND JUSTICE FOOD MEDIA INVESTIGATIONS PHO

POLITICS JANUARY 8, 2020

A New Voting System Promises Reliable Paper Records. Security Experts Warn It Can't Be Trusted.

A just-released study says over ninety percent of errors introduced by ballot marking devices go undetected.

AJ VICENS
Reporter
Bio | Follow

FREEDOM TO TINKER
research and expert commentary on digital technologies in public life

Serious design flaw in ESS ExpressVote touchscreen: "permission to cheat"

SEPTEMBER 14, 2018 BY ANDREW APPEL

Kansas, Delaware, and New Jersey are in the process of purchasing voting machines with a serious design flaw, and they should reconsider while there is still time!

Over the past 15 years, almost all the states have moved away from paperless touchscreen voting systems (DREs) to optical-scan paper ballots. They've done so because if a paperless touchscreen is hacked to give fraudulent results, there's no way to know and no way to correct; but if an optical scanner were hacked to give fraudulent results, the fraud could be detected by a random audit *of the paper ballots that the voters actually marked*, and corrected by a recount of those paper ballots.

Accepted for publication in *Election Law Journal*

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

Andrew W. Appel[†]
Princeton University

Richard A. DeMillo[†]
Georgia Tech

Philip B. Stark[†]
Univ. of California, Berkeley

February 14, 2020

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 device (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.

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
- *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?**

Evidence-Based Elections (Stark & Wagner, 2012)

Election officials should provide convincing public evidence that reported outcomes are correct.

Evidence-Based Elections (Stark & Wagner, 2012)

Election officials should provide convincing public evidence that reported outcomes are correct.

Absent such evidence, there should be a new election.

Risk-Limiting Audits (RLAs, Stark, 2008)

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

A risk-limiting audit has a known minimum chance of correcting the reported outcome if the reported outcome is wrong (& doesn't alter correct outcomes).

A risk-limiting audit has a known minimum chance of correcting the reported outcome if the reported outcome is wrong (& doesn't alter correct outcomes).

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

A risk-limiting audit has a known minimum chance of correcting the reported outcome if the reported outcome is wrong (& doesn't alter correct outcomes).

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

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

A risk-limiting audit has a known minimum chance of correcting the reported outcome if the reported outcome is wrong (& doesn't alter correct outcomes).

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

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

Establishing whether paper trail is trustworthy involves other processes, generically, *compliance audits*

RLA pseudo-algorithm

```
while (!(full handcount) && !(strong evidence outcome is correct)) {
    examine more ballots
}
```

RLA pseudo-algorithm

```
while (!(full handcount) && !(strong evidence outcome is correct)) {
    examine more ballots
}

if (full handcount) {
    handcount result is final
}
```

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, ...

Role of math/stat

- Get evidence about the population of cast ballots from a random sample.
- Guarantee a large chance of correcting wrong outcomes; minimize work if the outcome is correct.
- When can you stop inspecting ballots?
  - When there's strong evidence that a full hand count is pointless

- Null hypothesis: reported outcome is wrong.
- Significance level (Type I error rate) is “risk”
- Frame the hypothesis quantitatively: necessary and sufficient conditions

b_i is ith ballot card, N cards in all.

$$1_{\text{candidate}}(b_i) \equiv \begin{cases} 1, & \text{ballot } i \text{ has a mark for candidate} \\ 0, & \text{otherwise.} \end{cases}$$

$$A_{\text{Alice,Bob}}(b_i) \equiv \frac{1_{\text{Alice}}(b_i) - 1_{\text{Bob}}(b_i) + 1}{2} \geq 0.$$

mark for Alice but not Bob, $A_{\text{Alice,Bob}}(b_i) = 1$.

mark for Bob but not Alice, $A_{\text{Alice,Bob}}(b_i) = 0$.

marks for both (overvote) or neither (undervote) or doesn't contain contest, $A_{\text{Alice,Bob}}(b_i) = 1/2$.

$$\bar{A}^b_{\mathrm{Alice,Bob}} \equiv \frac{1}{N} \sum_{i=1}^{N} A_{\mathrm{Alice,Bob}}(b_i).$$

Mean of a finite nonnegative list of N numbers.

Alice won iff $\bar{A}^b_{\mathrm{Alice,Bob}} > 1/2$.

Plurality & Approval Voting

$K \geq 1$ winners, $C > K$ candidates in all.

Candidates $\{w_k\}_{k=1}^{K}$ are reported winners.

Candidates $\{\ell_j\}_{j=1}^{C-K}$ reported losers.

Plurality & Approval Voting

$K \geq 1$ winners, $C > K$ candidates in all.

Candidates $\{w_k\}_{k=1}^{K}$ are reported winners.

Candidates $\{\ell_j\}_{j=1}^{C-K}$ reported losers.

Outcome correct iff

$$\bar{A}^{b}_{\mathrm{w_k},\ell_\mathrm{j}} > 1/2, \quad \text{for all } 1 \leq k \leq K, \;\; 1 \leq j \leq C-K$$

$K(C-K)$ inequalities.

Plurality & Approval Voting

$K \geq 1$ winners, $C > K$ candidates in all.

Candidates $\{w_k\}_{k=1}^{K}$ are reported winners.

Candidates $\{\ell_j\}_{j=1}^{C-K}$ reported losers.

Outcome correct iff

$$\bar{A}^{b}_{\mathrm{w_k},\ell_\mathrm{j}} > 1/2, \quad \text{for all } 1 \leq k \leq K, \;\; 1 \leq j \leq C - K$$

$K(C - K)$ inequalities.

Same approach works for D'Hondt & other proportional representation schemes. (Stark & Teague 2015)

Super-majority

$f \in (1/2, 1]$.

Alice won iff

$$(\text{votes for Alice}) > f \times ((\text{valid votes for Alice}) + (\text{valid votes for everyone else}))$$

Set

$$A(b_i) \equiv \begin{cases} \frac{1}{2f}, & b_i \text{ has a mark for Alice and no one else} \\ 0, & b_i \text{ has a mark for exactly one candidate, not Alice} \\ \frac{1}{2}, & \text{otherwise.} \end{cases}$$

Alice won iff

$$\bar{A}^b > 1/2.$$

Borda count, STAR-Voting, & other additive weighted schemes

Winner is the candidate who gets most "points" in total.

$s_{\text{Alice}}(b_i)$: Alice's score on ballot i.

$s_{\text{cand}}(b_i)$: another candidate's score on ballot i.

s^+: upper bound on the score any candidate can get on a ballot.

Alice beat the other candidate iff Alice's total score is bigger than theirs:

$$A_{\text{Alice,c}}(b_i) \equiv \frac{s_{\text{Alice}}(b_i) - s_{\text{c}}(b_i) + s^+}{2s^+}.$$

Alice won iff $\bar{A}^b_{\text{Alice,c}} > 1/2$ for every other candidate c.

Ranked-Choice Voting, Instant-Runoff Voting (RCV/IRV)

2 types of assertions together give sufficient (not necessary) conditions (Blom et al. 2018):

1. Candidate i has more first-place ranks than candidate j has total mentions.
2. After a set of candidates E have been eliminated from consideration, candidate i is ranked higher than candidate j on more ballots than *vice versa*.

Both can be written $\bar{A}^b > 1/2$.

Finite set of such assertions implies reported outcome is right.

More than one set suffices; can optimize expected workload.

Auditing assertions

Test *complementary null hypothesis* $\bar{A}^b \leq 1/2$ sequentially.

- Audit until either all complementary null hypotheses about a contest are rejected at significance level α or until all ballots have been tabulated by hand.
- Yields a RLA of the contest in question at risk limit α.
- No multiplicity adjustment needed.

Sequential testing originated w/ Wald (1945; military secret before).

Key object: martingale.

Sequence of rvs $\{Z_j\}$ s.t.

- $\mathbb{E}|Z_j| < \infty$
- $\mathbb{E}(Z_{j+1}|Z_1, \ldots, Z_j) = Z_j$

Kolmogorov's inequality

If $\{Z_j\}$ is a nonnegative martingale, then for any $p > 0$ and all $J \in \{1, \ldots, N\}$,

$$\Pr\left(\max_{1 \le j \le J} Z_j(t) > 1/p\right) \le p\, \mathbb{E}|Z_J|.$$

Markov's inequality applied to optionally stopped martingales.

Wald's SPRT

For $j = 1, 2, \ldots$, let P_{j0} be the probability of $X_1, \ldots, X_j$ under H_0; P_{j1} be the probability of $X_1, \ldots, X_j$ under H_1.

$$Z_j = \frac{P_{j1}}{P_{j0}}, \quad j = 1, 2, \ldots$$

is a nonnegative martingale if H_0 is true.

$1/Z_j$ is a valid P-value for H_0 at step j.

Ballot-polling audits

Sample sequentially w/o replacement from a finite population of N non-negative items, $\{x_1, \ldots, x_N\}$, with $x_j \geq 0$, $\forall j$.

Total is $N\bar{x} \geq 0$. Value of the jth item drawn is X_j.

If $\bar{x} = t$, $\mathbb{E}X_1 = t$, so $\mathbb{E}(X_1/t) = 1$.

Given $X_1, \ldots, X_n$, the total of the remaining $N - n$ items is $Nt - \sum_{j=1}^{n} X_j$, so the mean of the remaining items is

$$\frac{Nt - \sum_{j=1}^{n} X_j}{N - n} = \frac{t - \frac{1}{N}\sum_{j=1}^{n} X_j}{1 - n/N}.$$

Define

$$Y_1(t) \equiv \begin{cases} X_1/t, & Nt > 0, \\ 1, & Nt = 0, \end{cases}$$

and for $1 \leq n \leq N-1$,

$$Y_{n+1}(t) \equiv \begin{cases} X_{n+1} \frac{1-\frac{n}{N}}{t-\frac{1}{N}\sum_{j=1}^{n} X_j}, & \sum_{j=1}^{n} X_j < Nt, \\ 1, & \sum_{j=1}^{n} X_j \geq Nt. \end{cases}$$

Then $\mathbb{E}(Y_{n+1}(t)|Y_1, \ldots Y_n) = 1$.

Let $Z_n(t) \equiv \prod_{j=1}^{n} Y_j(t)$.

$\mathbb{E}|Z_k| \leq \max_j x_j < \infty$ and

$$\mathbb{E}\left(Z_{n+1}(t)|Z_1(t), \ldots Z_n(t)\right) = \mathbb{E}\left(Y_{n+1}(t)Z_n(t)|Z_1(t), \ldots Z_n(t)\right) = Z_n(t).$$

Thus

$$(Z_1(t), Z_2(t), \ \ldots, Z_N(t))$$

is a non-negative closed martingale.

Thus a P-value for the hypothesis $\bar{x} = t$ for data $X_1, \ldots X_J$ is $\left(\max_{1 \leq j \leq J} Z_j(t)\right)^{-1} \wedge 1$.

Kaplan's martingale (KMART)
Let $S_j \equiv \sum_{k=1}^{j} X_k$, $\tilde{S}_j \equiv S_j/N$, and $\tilde{j} \equiv 1 - (j-1)/N$. Define

$$Y_n \equiv \int_0^1 \prod_{j=1}^{n} \left(\gamma \left[X_j \frac{\tilde{j}}{t - \tilde{S}_{j-1}} - 1 \right] + 1 \right) d\gamma.$$

Polynomial in γ of degree at most n, with constant term 1.

Under the null, $(Y_j)_{j=1}^{N}$ is a non-negative closed martingale with expected value 1.

Ballot-comparison audits

Use cast vote records (CVRs): system's interpretation of each ballot.

Like checking an expense report.

b_i is ith ballot, c_i is cast-vote record for ith ballot.

A an assorter.

overstatement error for ith ballot is

$$\omega_i \equiv A(c_i) - A(b_i) \leq A(c_i) \leq u,$$

where u is an upper bound on the value A assigns to any ballot card or CVR.

$v \equiv 2\bar{A}^c - 1$, *reported assorter margin*.

$B(b_i, c) \equiv (1 - \omega_i/u)/(2 - v/u) > 0$, $i = 1, \ldots, N$.

B assigns non-negative numbers to ballots.

Reported outcome correct iff

$$\bar{B} > 1/2.$$

Stratified sampling

Cast ballots are partitioned into $S \geq 2$ *strata*.

Stratum s contains N_s cast ballots.

Let $\bar{A}_s^b$ denote the mean of the assorter applied to just the ballot cards in stratum s. Then

$$\bar{A}^b = \frac{1}{N} \sum_{s=1}^{S} N_s \bar{A}_s^b = \sum_{s=1}^{S} \frac{N_s}{N} \bar{A}_s^b.$$

Can reject the hypothesis $\bar{A}^b \leq 1/2$ if we can reject the hypothesis

$$\bigcap_{s \in S} \left\{ \frac{N_s}{N} \bar{A}_s^b \leq \beta_s \right\}$$

for all $(\beta_s)_{s=1}^S$ s.t. $\sum_{s=1}^S \beta_s \leq 1/2$.

Union-Intersection Test

Fisher's Combining Function

$\{P_s(\beta_s)\}_{s=1}^S$ are independent random variables.

If $\bigcap_{s\in S}\left\{\frac{N_s}{N}\bar{A}_s^b \le \beta_s\right\}$, distribution of

$$-2\sum_{s=1}^{S} \ln P_s(\beta_s)$$

is dominated by chi-square distribution with $2S$ degrees of freedom.

Low-dimensional optimization problem to maximize P-value over $(\beta_s)_{s=1}^S$.

Sample design

- individual ballots?
- clusters of ballots?
- stratify? (logistics, equipment capabilities, . . .)
- sampling probabilities?
- with replacement? without replacement? Bernoulli?
- fully sequential? batch-oriented?

Statistics > Applications

[Submitted on 15 Dec 2018]

Bernoulli Ballot Polling: A Manifest Improvement for Risk-Limiting Audits

Kellie Ottoboni, Matthew Bernhard, J. Alex Halderman, Ronald L. Rivest, Philip B. Stark

We present a method and software for ballot-polling risk-limiting audits (RLAs) based on Bernoulli sampling: ballots are included in the sample with probability p, independently. Bernoulli sampling has several advantages: (1) it does not require a ballot manifest; (2) it can be conducted independently at different locations, rather than requiring a central authority to select the sample from the whole population of cast ballots or requiring stratified sampling; (3) it can start in polling places on election night, before margins are known. If the reported margins for the 2016 U.S. Presidential election are correct, a Bernoulli ballot-polling audit with a risk limit of 5% and a sampling rate of $p_0 = 1\%$ would have had at least a 99% probability of confirming the outcome in 42 states. (The other states were more likely to have needed to examine additional ballots.) Logistical and security advantages that auditing in the polling place affords may outweigh the cost of examining more ballots than some other methods might require.

Comments: Accepted for Voting'19 workshop

Bayesian election audits

Limit the *upset probability*, the posterior probability that the reported outcome is wrong, given the sample, for a particular prior distribution on outcomes

Bayesian election audits

Limit the *upset probability*, the posterior probability that the reported outcome is wrong, given the sample, for a particular prior distribution on outcomes

Typically use Dirichlet-multinomial prior.

"Non-partisan" priors invariant under permutations of the candidate names.

A Bayesian Method for Auditing Elections

Ronald L. Rivest
Computer Science and Artificial Intelligence Lab,
MIT, Cambridge, MA 02139
rivest@mit.edu

Emily Shen
Computer Science and Artificial Intelligence Lab,
MIT, Cambridge, MA 02139
eshen@csail.mit.edu

Abstract

We propose an approach to post-election auditing based on Bayesian principles, and give experimental evidence for its efficiency and effectiveness. We call such an audit a "Bayes audit". It aims to control the probability of miscertification (certifying a wrong election outcome). The miscertification probability is computed using a Bayesian model based on information gathered by the audit so far.

A Bayes audit is a single-ballot audit method applicable to any voting system (e.g. plurality, approval, IRV, Borda, Schulze, etc.) as long as the number of ballot types is not too large. The method requires only the ability to randomly sample single ballots and the ability to compute the election outcome for a profile of ballots. A Bayes audit does not require the computation of a "margin of victory" in order to get started.

1 Introduction

This section provides a quick introduction to post-election audits and our notation. Section 2 then presents our proposed Bayes audit procedure. Section 3 gives the results of our initial experiments using this method on simulated and real election data. Section 4 considers some extensions and variations of the basic method, and Sections 5 and 6 discuss and summarize what we have learned about the Bayes audit. Appendix A provides some additional technical details on efficient implementation methods.

1.1 Post-election audits

Informally, the purpose of a post-election audit is to check that the reported election outcome is correct, by auditing enough randomly chosen ballots.

Absolute certainty isn't required of an audit (the only

Bayes/Frequentist duality

Risk of an audit for a set of cast votes and a reported outcome:

- probability of not correcting outcome if reported outcome is wrong for that set of votes
- 0 if reported outcome is correct for that set of votes

Bayes/Frequentist duality

Risk of an audit for a set of cast votes and a reported outcome:

- probability of not correcting outcome if reported outcome is wrong for that set of votes
- 0 if reported outcome is correct for that set of votes
- RLAs control *maximum* risk.
- Bayesian audits (Rivest & Shen) control *weighted average* of the risk. The prior determines the weights in the average.
- For 2-candidate plurality contest w/ no invalid votes, least-favorable prior has point mass $1/2$ at tie, remaining $1/2$ mass arbitrary over winning outcomes (Vora, 2018).

Wrinkles

- ~20% of U.S. voters don't vote on paper
- ballot-marking devices make the paper trail hackable
- inadequate rules for chain of custody, ballot accounting, ...
- transparent high-quality randomness
  - public ceremony of die rolls, published crypto-quality PRNG
- missing ballots; imperfect manifests
  - "Manifest Phantoms to Evil Zombies"
- ability to produce CVRs linked to ballots
- redacted CVRs
- preserving privacy while ensuring the public can confirm audit didn't stop too soon

Open-source software

- auditTools
- ballotPollTools
- SUITE
- SHANGRLA
- Arlo

Evidence-Based Elections: 3 C's

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

Evidence-Based Elections: 3 C's

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

Evidence-Based Elections: 3 C's

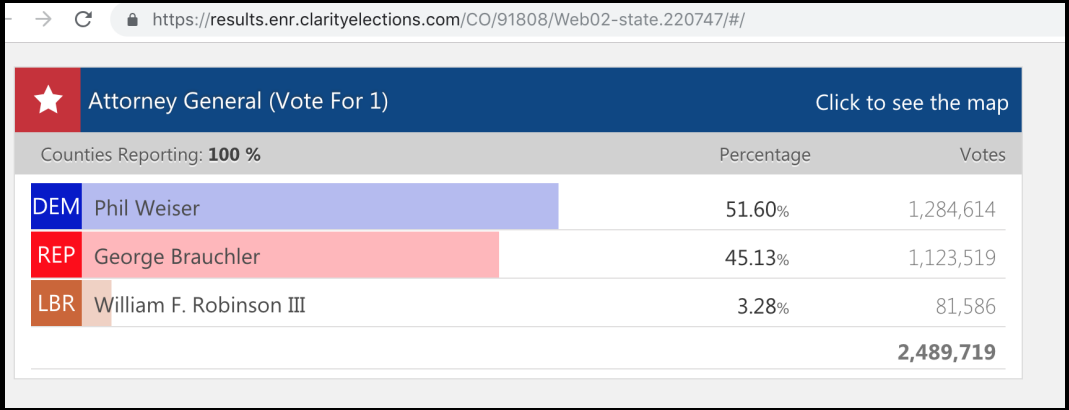
- Voters *CREATE* complete, durable, verified audit trail.
- LEO *CARES FOR* the audit trail adequately to ensure it remains complete and accurate.
- Verifiable audit *CHECKS* reported results against the paper

- 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** ($<0.5\%$)

Risk-Limiting Audits

- ~60 pilot audits in AK, CA, CO, GA, IN, 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 Cruz, Stanislaus, Ventura, Yolo.
- Routine statewide in CO since 2017. AK did statewide audit in 2020; WY auditing today.
- Laws in CA, CO, RI, VA, WA


https://results.enr.clarityelections.com/CO/91808/Web02-state.220747/#/
Attorney General (Vote For 1)
Click to see the map
Counties Reporting: 100 %
Percentage
Votes
DEM
Phil Weiser
51.60%
1,284,614
REP
George Brauchler
45.13%
1,123,519
LBR
William F. Robinson III
3.28%
81,586
2,489,719

Voting and COVID-19

Per Curiam

SUPREME COURT OF THE UNITED STATES

No. 19A1016

REPUBLICAN NATIONAL COMMITTEE, ET AL. *v.*
DEMOCRATIC NATIONAL COMMITTEE, ET AL.

ON APPLICATION FOR STAY

[April 6, 2020]

PER CURIAM.

The application for stay presented to JUSTICE KAVANAUGH and by him referred to the Court is granted. The District Court's order granting a preliminary injunction is stayed to the extent it requires the State to count absentee ballots postmarked after April 7, 2020.

Wisconsin has decided to proceed with the elections scheduled for Tuesday, April 7. The wisdom of that decision is not the question before the Court. The question before the Court is a narrow, technical question about the absentee ballot process. In this Court, all agree that the deadline for the municipal clerks to receive absentee ballots has been extended from Tuesday, April 7, to Monday, April 13. That extension, which is not challenged in this Court, has afforded Wisconsin voters several extra days in which to mail their absentee ballots. The sole question before the Court is whether absentee ballots now must be mailed and postmarked by election day, Tuesday, April 7, as state law would necessarily require, or instead may be mailed and postmarked after election day, so long as they are received

CBS NEWS

NEWS CORONAVIRUS SHOWS LIVE

At least 7 COVID-19 cases tied to in-person voting in Wisconsin

BY ADAM BREWSTER
APRIL 21, 2020 / 4:36 PM / CBS NEWS

- In-person voting involves congregating & touching common objects (esp. BMDs & DREs, but also pens, doorknobs), but S. Korea did great job recently

Coronavirus: South Korea holds parliamentary elections despite COVID-19 pandemic

South Korea's mass testing, tracing and quarantine measures meant authorities believed it was safe for the ballot to go ahead.

Tom Cheshire
Asia correspondent @chesh

Wednesday 15 April 2020 08:47, UK

COVID-19 CORONAVIRUS SOUTH KOREA

About 44 million people are eligible to vote

- Online voting does not require contact, but
  - No way to secure online voting
  - Demonstration hacks by Halderman et al.

MIT News

Browse or Search

MIT researchers identify security vulnerabilities in voting app

Mobile voting application could allow hackers to alter individual votes and may pose privacy issues for users.

Abby Abazorius | MIT News Office
February 13, 2020

Press Inquiries

In recent years, there has been a growing interest in using internet and mobile technology to increase access to the voting process. At the same time, computer security experts caution that paper ballots are the only secure means of voting.

Now, MIT researchers are raising another concern: They say they have uncovered security vulnerabilities in a mobile voting application that was used during the 2018 midterm elections in West Virginia. Their security analysis of the application, called Voatz, pinpoints a number of weaknesses, including the opportunity for hackers to alter, stop, or expose how an individual user has voted. Additionally, the researchers found that Voatz's

PRESS MENTIONS

MIT researchers have identified security flaws in a mobile voting application that allowed some overseas and military citizens to vote remotely, reports Lydia Emmanouilid for PRI's *The World*. "When things a opaque — when you can't verify, whe you can't see what the code is doing says graduate student Michael Specter, "there is no way of vetting that it's doing the right thing."

"PR

3/30/2020
03:45 PM

HackerOne Drops Mobile Voting App Vendor Voatz

Bug bounty platform provider cited "Voatz's pattern of interactions with the research community" in its decision to halt the app vendor's vuln disclosure program on HackerOne.

Dark Reading Staff
Quick Hits

Mobile voting application vendor Voatz has been dismissed from HackerOne's bug bounty program platform, according to a report on CyberScoop.

Voatz — whose mobile voting app used in limited elections in a handful of states, including West Virginia and Colorado — has been under intense scrutiny over security concerns, and recently published studies by MIT and Trail of Bits uncovered significant security weaknesses in the app.

While security experts long have dismissed mobile voting as inherently risky, proponents of mobile-voting have maintained that the apps and process are more secure and private, for example, than the standard practice of sending PDF-based ballots via unencrypted email to military personnel overseas.

Voatz recently had updated its bug bounty policy on HackerOne to say that it could not "guarantee safe harbor" for researchers who discover flaws in its software under the program, CyberScoop said in its report.

FREE SPEECH FOR PEOPLE .ORG

April 20, 2020

The Honorable Ellen F. Rosenblum
Office of the Attorney General
Commerce Building
158 12th St. NE
Salem, OR 97301

Dear Attorney General Rosenblum,

We write to you to urge you to initiate an investigation into the voting system vendor Voatz for advancing potential false claims and deceptive marketing practices while promoting its mobile voting application in Oregon that may violate the Unlawful Trade Practices Act, Or. Rev. Stat. § 646.607; fraudulent misrepresentation; or any other violation of state law.[1]

Voatz is Boston-based startup company that is developing and aggressively marketing an internet-based voting system that enables voters to cast a ballot from application loaded on to their mobile phones. In 2019, Jackson and Umatilla counties contracted to have Voatz offer its internet voting system to voters eligible under the Uniformed and Overseas Citizen Absentee Voting Act (UOCAVA) for Oregon's 2020 general elections.

Voatz's campaign to promote its voting system in Oregon has included bogus claims of "military grade security,"[2] public statements asserting that votes cast on its platform could not be deleted or altered,[3] and published materials[4] and presentations[5] promising that Voatz's system was robustly vetted and secure.[6] Though many computer security

- VBM does not require congregating . . .
  - Klobuchar & Wyden introduced bill requiring everyone to get VBM ballot . . .
  - Serious logistical and security problems:
    - printing & mailing: 3rd parties need more equipment
    - ballots lost in the mail in either direction
    - USPS might be dead
    - potential for DOS attacks
    - ballot harvesting, coercion, vote-selling
    - authentication, signature verification (if any)
    - weaponized to disenfranchise minority voters, e.g., GA
    - need to inform voters of (non) receipt, notify them of problems & allow time to "cure"

PBS NEWS HOUR

menu

By Kate Brumback, Associated Press

Leave a comment

Share

Georgia's rejection of mail ballots over mismatched signatures halted by judge

Politics Oct 24, 2018 3:28 PM EDT

ATLANTA — Georgia election officials must stop rejecting absentee ballots and absentee ballot applications because of a mismatched signature without first giving voters a chance to fix the problem, a federal judge ruled Wednesday.

U.S. District Judge Leigh May ordered the secretary of state's office to instruct county election officials to stop the practice for the November midterm elections. She outlined a procedure to allow voters to resolve alleged signature discrepancies.

May's order comes in response to two lawsuits filed earlier this month allege that election officials are improperly rejecting absentee ballots. The lawsuits said the rejections without first letting voters challenge the determination violated voters' constitutional rights.

Stanford Law School
Law and Policy Lab

Policy Practicum: Every Vote Counts (Law 806Z)

Signature Verification and Mail Ballots: Guaranteeing Access While Preserving Integrity

April 15, 2020

RESEARCH TEAM

Roxana ARJON
BA Public Policy '22

Ali Haley Phillips BLOOMGARDEN
MA Education Policy '20

Benjamin C HATTEM
JD '20 BA '20

Garrett Jens JENSEN
MPP/MA Education '20

Zahavah LEVINE
Distinguished Career Institute Fellow 2019-20

Mike NORTON, Ph.D.
JD '21

Megha Nanaki PARWANI
BA Philosophy/Political Science '21

Emily POSTMAN
JD '21

Ashwin RAMASWAMI
BS Computer Science '21

Grace RYBAK
JD '21

Emily WILSON
BA History '20

ELECTIONS

North Carolina GOP Operative Faces New Felony Charges That Allege Ballot Fraud

July 30, 2019 · 10:29 PM ET

RICHARD GONZALES

Prosecutors in North Carolina filed new felony charges against a Republican political operative accused of ballot tampering in a congressional election in 2018.

GOP operative Leslie McCrae Dowless was arrested in February 2017 and charged with illegal ballot handling and obstruction of justice. New charges were filed Tuesday.

Wake City-County Bureau of Identification via AP

Leslie McCrae Dowless was charged Tuesday with two counts of felony obstruction of justice, perjury, solicitation to commit perjury, conspiracy to obstruct justice and illegal possession of absentee ballots, according to a statement by Wake County District Attorney Lorrin Freeman.

The charges relate to the tainted 9th congressional district election last year in which Republican Mark Harris led in the unofficial vote tally by a margin of about 900 votes over Democrat Dan McCready. But the election results were overturned by the state after an investigation into an absentee ballot operation on Harris' behalf suggested that Dowless had improperly collected and possibly tampered with ballots.

The Washington Post
Democracy Dies in Darkness

White House rejects bailout for U.S. Postal Service battered by coronavirus

The pandemic has pushed USPS to the brink, but Trump and Mnuchin shot down emergency aid

A U.S. Postal Service carrier wears a mask and gloves while making deliveries in Washington, D.C., on April 1. (Erik S Lesser/EPA-EFE/Shutterstock)

By **Jacob Bogage**

April 11, 2020 at 8:41 a.m. PDT

Through rain, sleet, hail, and even a pandemic, mail carriers serve every address in the United States, but the coronavirus crisis is shaking the foundation of the U.S. Postal Service in new and dire ways.

Recommendations for November 2020

- expand vote by mail and early voting
- reduce use of DREs & BMDs (not secure; vector for coronavirus)
- secure/monitored kiosks to pick up blank ballots (BOD?) & cast voted ballots
- ballot tracking; provide adequate notice & opportunity to cure defects
- increase transparency: public video monitoring, etc.
- rigorous ballot accounting & compliance audits including eligibility
- risk-limiting audits for statewide contests

Recommendations for Statistics instruction

- finite sample exact/conservative nonparametric inference
- sampling designs
- sequential tests
- martingale methods
- methods for combining P-values, including Fisher's method
- testing by maximizing P-values over nuisance parameters
- pseudo-random number generation


411412
411413
411418
421224
421422
411221
421222
421225
421226
511221
521225
561341
511211