Election Hacking and Security

Kensington Public Library
Kensington, CA

Philip B. Stark

13 January 2020

University of California, Berkeley

Many collaborators including (most recently) Andrew Appel, Josh Benaloh, Matt Bernhard, Rich DeMillo, Steve Evans, Alex Halderman, Mark Lindeman, Kellie Ottoboni, Ron Rivest, Peter Ryan, 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:

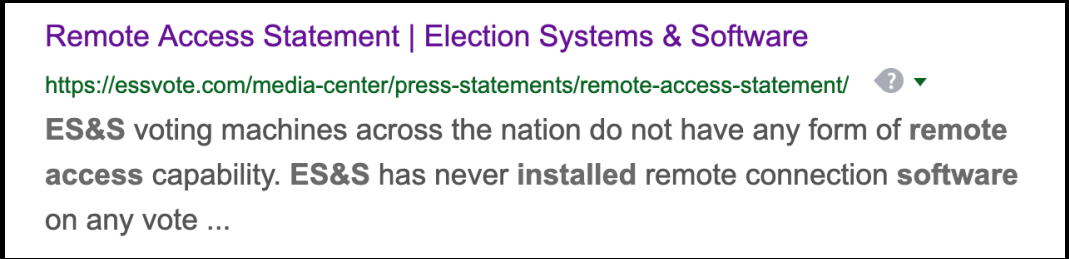
- Physical security
- Not connected to the Internet
- Tested before election day
- Too decentralized

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


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

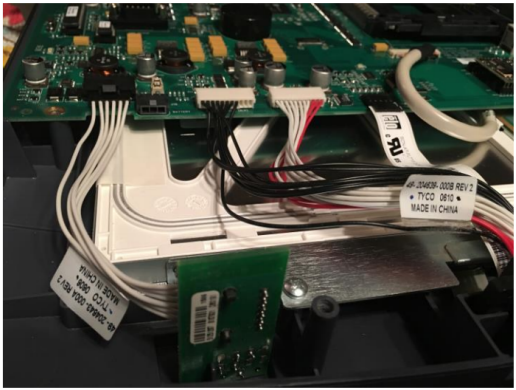
September 2017

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
- 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.

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

How the paper is marked, curated, tabulated, and 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.

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

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: 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

- If there's a trustworthy 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 doesn't alter correct outcomes).

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

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

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, ...

Risk-Limiting Audits

- Endorsed by NASEM, PCEA, ASA, LWV, CC, VV, ...
- Large chance of requiring a full hand count, if that would show the outcome is wrong. (Full hand count of trustworthy paper corrects wrong outcomes.)

Risk-Limiting Audits

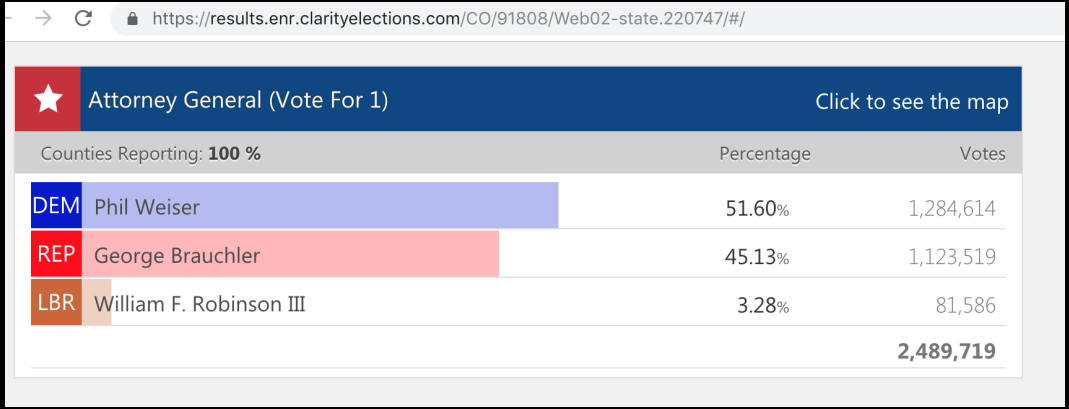
- Endorsed by NASEM, PCEA, ASA, LWV, CC, VV, ...
- Large chance of requiring a full hand count, if that would show the outcome is wrong. (Full hand count of trustworthy paper corrects wrong outcomes.)
- Most efficient options: **ballot-polling** and **ballot-level comparison**

- 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

- ~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


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

RLA pseudo-algorithm

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

RLA pseudo-algorithm

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

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

RLA pseudo-algorithm

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

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

Chance RLA won't correct wrong outcome is less than pre-selected **risk limit**.

"Wrong" means full handcount of *trustworthy* paper would find different winner(s)

Sampling ballots: requirements

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


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

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