EECS 388

Introduction to Computer Security

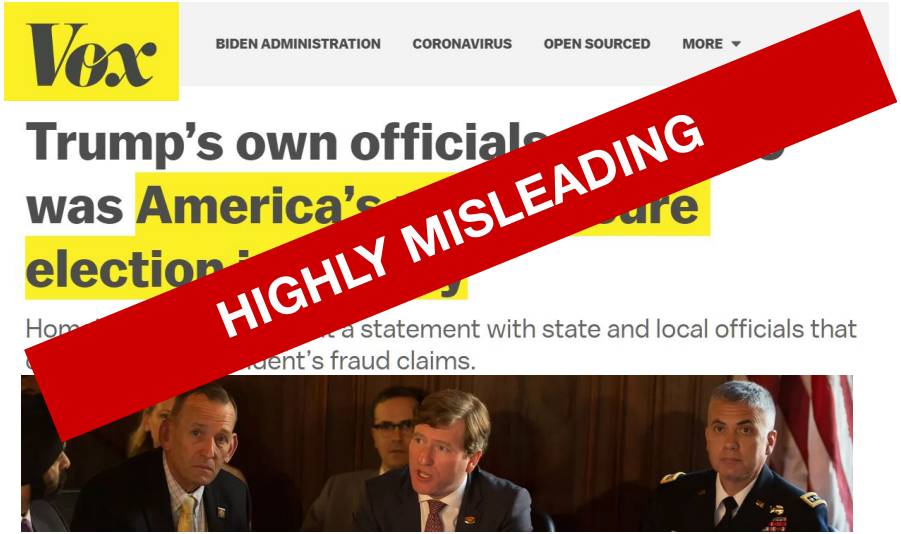
Lecture 19:

Election Cybersecurity

November 5, 2024
Prof. Halderman

Disinformation about the 2020 Election

Which of these claims is true?



The Experts' View

"As the National Academies recently concluded, 'There is no realistic mechanism to fully secure vote casting and tabulation computer systems from cyber threats.'"

"To our collective knowledge, no credible evidence has been put forth that supports a conclusion that the 2020 election outcome in any state has been altered through technical compromise."

That's still true today.

The New York Times

Election Security Experts Contradict Trump's Voting Claims

In a public letter, 59 top specialists called the president's fraud assertions "unsubstantiated" and "technically incoherent."

By Nicole Perlroth

Nov. 16, 2020

Fifty-nine of the country's top computer scientists and election security experts rebuked President Trump's baseless claims of voter fraud and hacking on Monday, writing that such assertions are "unsubstantiated or are technically incoherent."

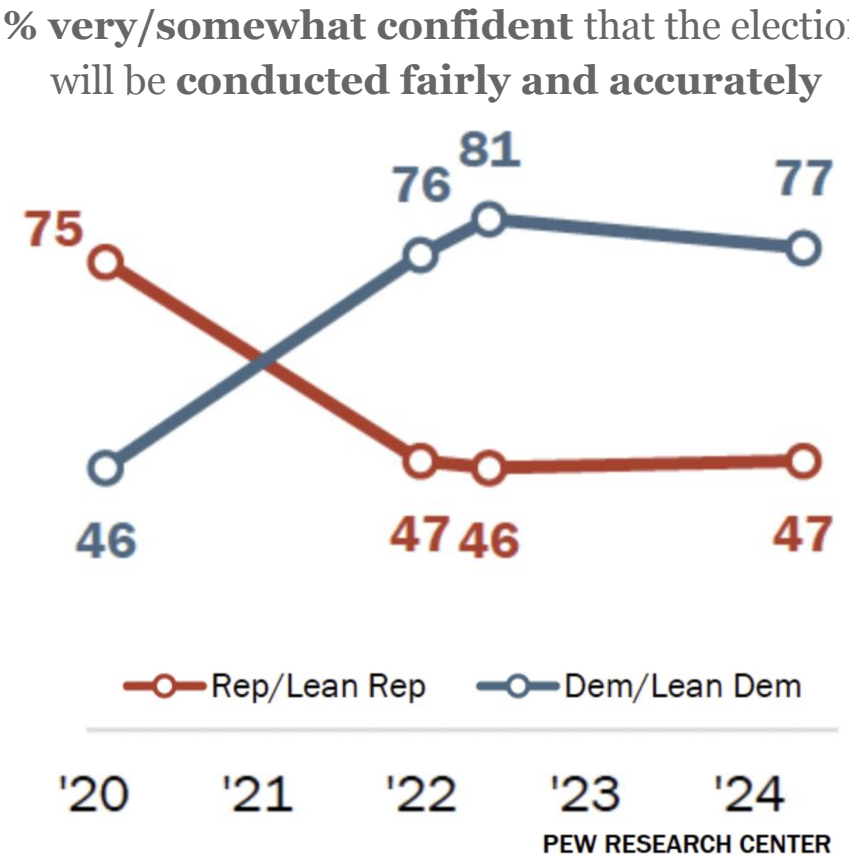
"Anyone asserting that a U.S. election was 'rigged' is making an extraordinary claim, one that must be supported by persuasive and verifiable evidence," the scientists wrote. In the absence of evidence, they added, it is "simply speculation."

"To our collective knowledge, no credible evidence has been put forth that supports a conclusion that the 2020 election outcome in any state has been altered through technical compromise," they wrote.

Confidence in Elections is Highly Partisan

Over the past two presidential cycles, **trust in elections** is strongly predicted by whether people's candidate won last time.

Democrats and Republicans **switched places after 2020**, despite little change in the underlying trustworthiness of election administration.



Flashback: Russian Attacks During the 2016 Election

Targeted political leaks

Stolen emails leaked online

Trolling/message amplification

Goals: Advantage Trump, sow discord

Attacks on election infrastructure

Registration systems and vendors

Flashback: Russian Attacks During the 2016 Election

Targeted political leaks

Stolen emails leaked online

Trolling/message amplification

Goals: Advantage Trump, sow discord

Attacks on election infrastructure

Registration systems and vendors

Flashback: Russian Attacks During the 2016 Election

Targeted political leaks

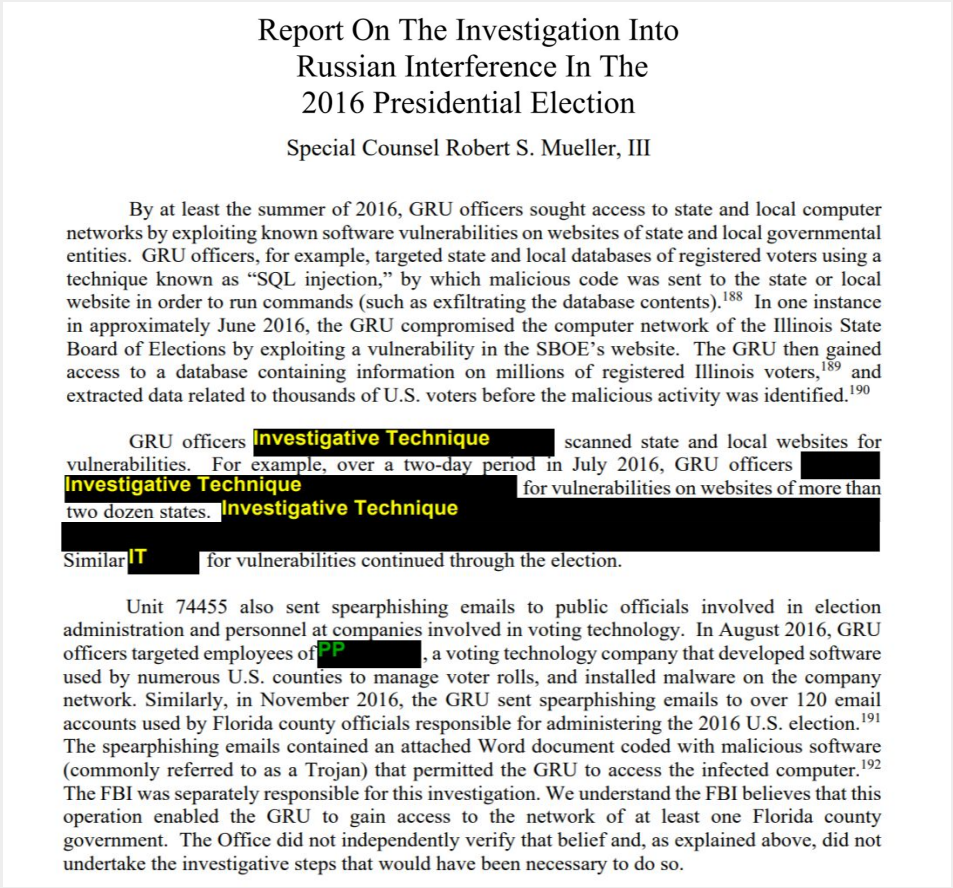
Stolen emails published online

Trolling/message amplification

Goals: Sow discord, advantage Trump

Attacks on election infrastructure

- All 50 states probed, multiple state voter registration systems infiltrated
- At least one election system vendor infiltrated; attempts to infiltrate county/ local election offices
- Attackers had ability to change or destroy registration data (but didn't)
- No evidence that Russia changed votes, but technology didn't stop them



Report On The Investigation Into
Russian Interference In The
2016 Presidential Election

Special Counsel Robert S. Mueller, III

By at least the summer of 2016, GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as "SQL injection," by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents).[188] In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters,[189] and extracted data related to thousands of U.S. voters before the malicious activity was identified.[190]

GRU officers Investigative Technique scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers [redacted] Investigative Technique for vulnerabilities on websites of more than two dozen states. Investigative Technique [redacted] Similar IT for vulnerabilities continued through the election.

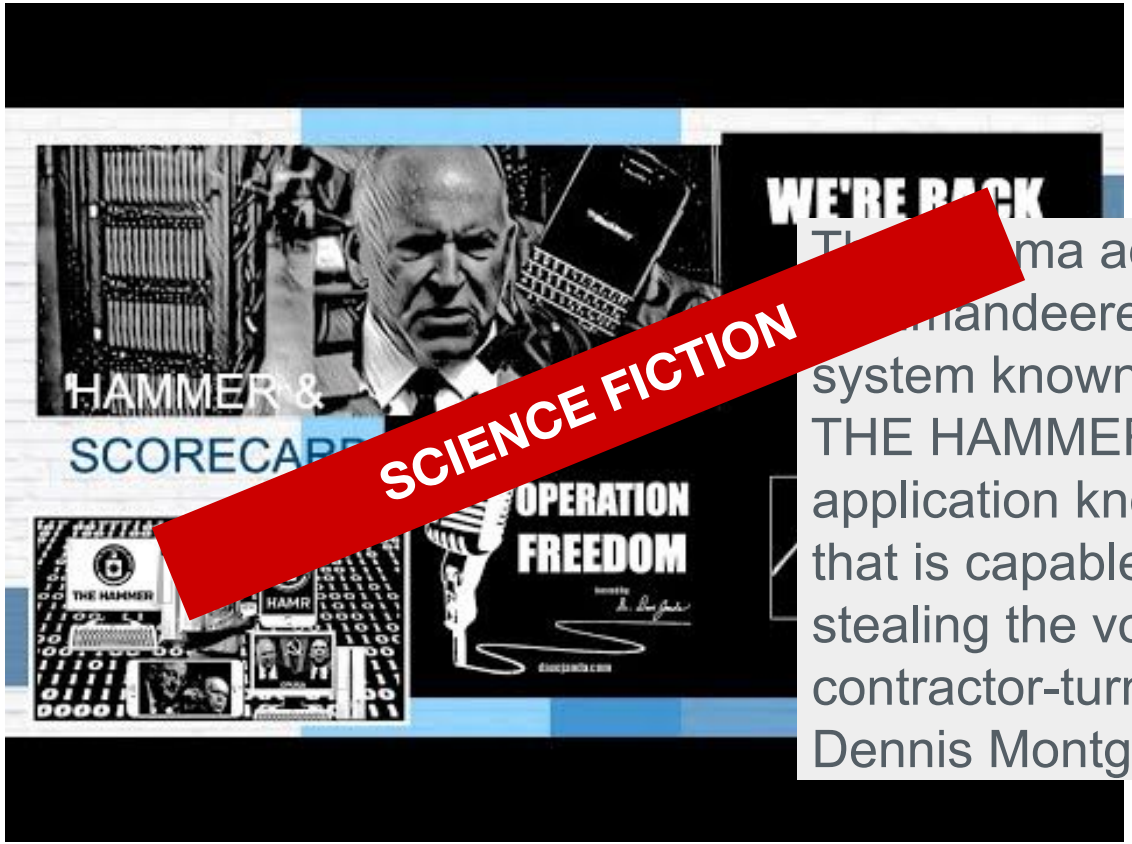
Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of PP, a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.[191] The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer.[192] The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.

Senate Intelligence Committee Russia Investigation

"The key lesson from 2016 is that election infrastructure hacking threats are real."

"As James Comey testified here two weeks ago, we know 'They'll be back.'"

Flashback: 2020 Conspiracy Theories



The Obama administration commandeered a powerful supercomputer system known as THE HAMMER. THE HAMMER includes an exploit application known as SCORECARD that is capable of hacking into elections and stealing the vote, according to CIA contractor-turned-whistleblower Dennis Montgomery...

Flashback: 2020 Conspiracy Theories

Attorney Sidney Powell:

An international Communist plot had been engineered by Venezuela, Cuba, China, Hugo Chávez, George Soros, the Clinton Foundation, and antifa…

Dominion Voting Systems "can set and run an algorithm that probably ran all over the country to take a certain percentage of votes from President Trump and flip them to President Biden."

ZERO CREDIBLE EVIDENCE

Elections Face Two Broad Classes of Security Risks

Report On The Investigation Into
Russian Interference In The
2016 Presidential Election

Special Counsel Robert S. Mueller, III

By at least the summer of 2016, GRU officers sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities. GRU officers, for example, targeted state and local databases of registered voters using a technique known as "SQL injection," by which malicious code was sent to the state or local website in order to run commands (such as exfiltrating the database contents).[188] In one instance in approximately June 2016, the GRU compromised the computer network of the Illinois State Board of Elections by exploiting a vulnerability in the SBOE's website. The GRU then gained access to a database containing information on millions of registered Illinois voters,[189] and extracted data related to thousands of U.S. voters before the malicious activity was identified.[190]

GRU officers Investigative Technique scanned state and local websites for vulnerabilities. For example, over a two-day period in July 2016, GRU officers [redacted] Investigative Technique for vulnerabilities on websites of more than two dozen states. Investigative Technique [redacted] Similar IT for vulnerabilities continued through the election.

Unit 74455 also sent spearphishing emails to public officials involved in election administration and personnel at companies involved in voting technology. In August 2016, GRU officers targeted employees of PP, a voting technology company that developed software used by numerous U.S. counties to manage voter rolls, and installed malware on the company network. Similarly, in November 2016, the GRU sent spearphishing emails to over 120 email accounts used by Florida county officials responsible for administering the 2016 U.S. election.[191] The spearphishing emails contained an attached Word document coded with malicious software (commonly referred to as a Trojan) that permitted the GRU to access the infected computer.[192] The FBI was separately responsible for this investigation. We understand the FBI believes that this operation enabled the GRU to gain access to the network of at least one Florida county government. The Office did not independently verify that belief and, as explained above, did not undertake the investigative steps that would have been necessary to do so.

Real Attacks

2016: Russia targets election infrastructure in all 50 states

Both are serious threats!

False Claims

2020: President amplifies false hacking claims

Despite these threats, elections may be the **most neglected form of critical infrastructure.**

What **Security Requirements** do election systems need to enforce?

Integrity

The **outcome** matches **voter intent**.

Votes are cast as intended.

Votes are counted as cast.

Security Requirements

☑ Integrity

Ballot Secrecy

Weak form:

Nobody can figure out **how you voted**…

Strong form:

…**even if you try** to prove it to them.

Security Requirements

- ☑ Integrity
- ☑ Ballot Secrecy

Voter Authentication

Only authorized voters can cast votes,

and

each voter can only vote up to the permitted number of times.

Security Requirements

- ✔ Integrity
- ✔ Ballot Secrecy
- ✔ Voter Authentication

Enfranchisement

All authorized voters have the **opportunity to vote**.

Security Requirements

- ✔️ Integrity
- ✔️ Ballot Secrecy
- ✔️ Voter Authentication
- ✔️ Enfranchisement

Availability

The election system is able to accept all votes on schedule and produce results in a timely manner.

Security Requirements

- ✅ Integrity
- ✅ Ballot Secrecy
- ✅ Voter Authentication
- ✅ Enfranchisement
- ✅ Availability

Integrity  Ballot Secrecy

Authentication  Enfranchisement

Security Requirements

- ☑ Integrity
- ☑ Ballot Secrecy
- ☑ Voter Authentication
- ☑ Enfranchisement
- ☑ Availability

Other Important Properties

- ☑ Cost Effectiveness
- ☑ Accessibility
- ☑ Convenience
- ☑ Intelligibility


Vulnerable Infrastructure

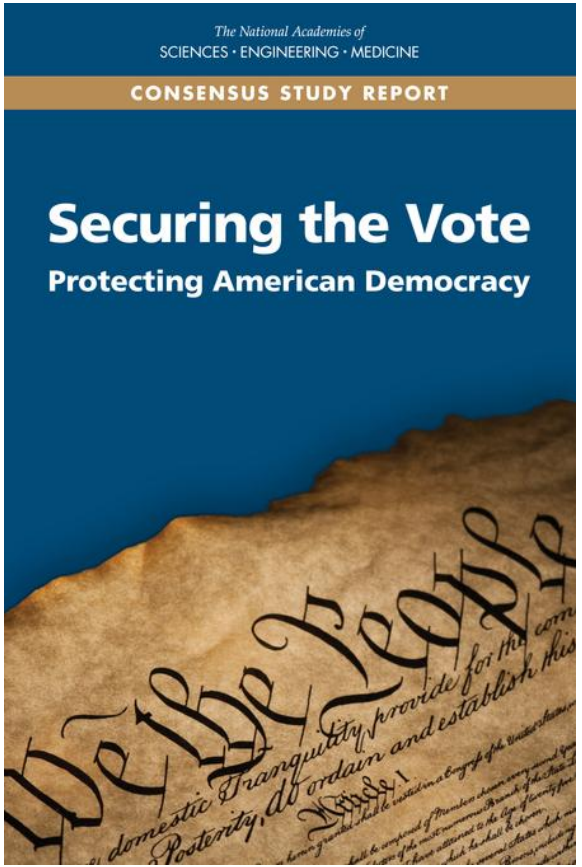
The Challenge of Election Security

Consensus of the National Academies:

> "There is no realistic mechanism to *fully secure* vote casting and tabulation computer systems from cyber threats."

Challenge for election systems:

How to achieve security and public trust with fallible technology?



U.S. Elections

Scale and Complexity

Massive Scale

~170 million registered voters

Highly Distributed
State, county, and local levels

~13,000 voting jurisdictions

~180,000 election precincts

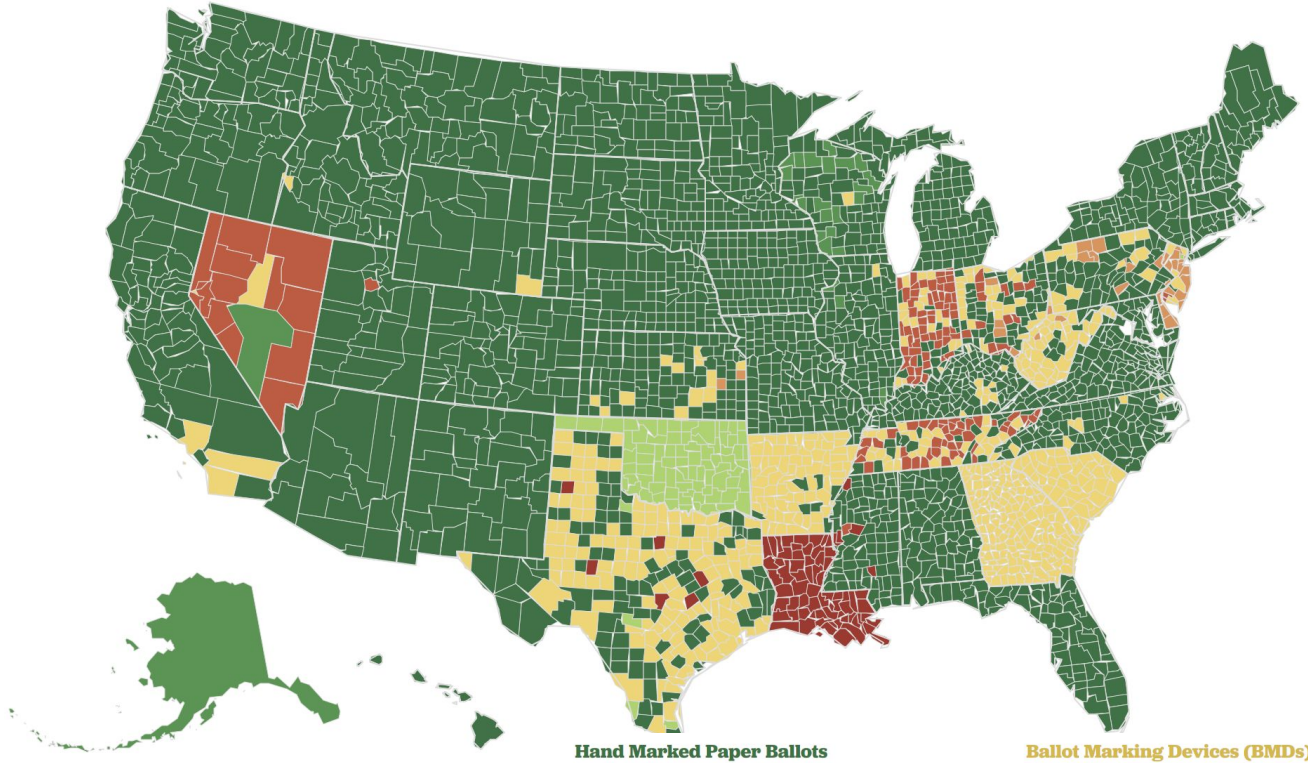
Sensitive to Latency
Want results on election night

High Complexity
Ballots with many different races, over a dozen languages, etc.

~50 models of voting machines

Election Equipment in 2024

DREs mostly replaced by BMDs



Polling Place Equipment
November 2024

- Hand marked paper ballots, with BMDs for accessibility
- Hand marked paper ballots, with DREs with VVPAT for accessibility
- Hand marked paper ballots, with DREs without VVPAT for accessibility
- Ballot Marking Devices for all voters
- Hybrid BMD/Tabulator
- DREs with VVPAT for all voters
- DREs without VVPAT for all voters

VerifiedVoting

Source: https://verifiedvoting.org/verifier/

Hand Marked Paper Ballots

69.2%

Percentage of registered voters living in jurisdictions using Hand Marked Paper Ballots for most voters

Ballot Marking Devices (BMDs)

25.9%

Percentage of registered voters living in jurisdictions using Ballot Marking Devices for all voters

Direct Recording Electronic (DRE) Systems

4.9%

Percentage of registered voters living in jurisdictions using Direct Recording Electronic (DRE) Systems for all voters

U.S. Elections Long, Complicated Ballots

November 8, 2016 *(8 de noviembre de 2016)*
Dallas County, Texas *(Condado de Dallas, Texas)*
SAMPLE BALLOT *(BOLETA DE MUESTRA)*

INSTRUCTION NOTE: Vote on the candidate/statement of your choice in each race by darkening in the oval provided to the left of the name of that candidate/statement.

Straight-Party Vote: You may cast a straight-party vote (that is, cast a vote for all the nominees of one party) by darkening in the oval provided to the left of the name of the party of your choice. If you cast a straight-party vote for all the nominees of one party and also cast a vote for an opponent of one of that party's nominees, your vote for the opponent will be counted as well as your vote for all the other nominees of the party for which the straight-party vote was cast. Party Abbreviations, Republican Party (Rep); Democratic Party (Dem); Libertarian Party (Lib); Green Party (Grn).

Voting for a Declared Write-In Candidate: You may vote for a declared write-in candidate by writing in the name of the candidate on the line provided and darkening in the oval provided to the left of the line.

USE THE MARKING DEVICE PROVIDED

NOTA DE INSTRUCCIÓN: *Vote sobre el candidato/declaración de su preferencia en cada compaña electoral al llenar el óvalo provisto a la izquierda del nombre de ese candidato/declaración.*

Voto de Partido Completo: *Usted puede emitir un voto de partido único (es decir, emitir un voto para todos los candidatos de un solo partido) al llenar el óvalo provisto a la izquierda del nombre del partido de su selección. Si usted emite un voto de partido único para todos los nominados de un solo partido y también emite un voto para un oponente de uno de los nominados de ese partido, su voto para el oponente será contado tanto como su voto para todos los demás nominados del partido por el cual fue emitido el voto de partido único. Abreviaturas, Partido Republicano (Rep); Partido Democrático (Dem); Partido Libertario (Lib); Partido Verde (Grn).*

Votando por un Candidato Declarado por Escrito: *Usted puede votar por un candidato declarado por escrito al escribir el nombre del candidato en la línea provista para ese cargo y al llenar el óvalo provisto a la izquierda de la línea.*

UTILICE EL MARCADOR PROPORCIONADO

Straight Party *(Partido Completo)*

Republican Party *(Partido Republicano)*	Rep
Democratic Party *(Partido Democrático)*	Dem
Libertarian Party *(Partido Libertario)*	Lib
Green Party *(Partido Verde)*	Grn

President and Vice President *(Presidente y Vice Presidente)*

Vote for One (Votar por Uno)

Donald J. Trump / Mike Pence	Rep
Hillary Clinton / Tim Kaine	Dem
Gary Johnson / William Weld	Lib
Jill Stein / Ajamu Baraka	Grn
Write-In *(Voto Escrito)*	

United States Representative, District 24 *(Representante de los Estados Unidos, Distrito Núm. 24)*

Vote for One *(Votar por Uno)*

Kenny E. Marchant	Rep
Jan McDowell	Dem
Mike Kolls	Lib
Kevin McCormick	Grn

United States Representative, District 26 *(Representante de los Estados Unidos, Distrito Núm. 26)*

Vote for One *(Votar por Uno)*

Michael C. Burgess	Rep
Eric Mauck	Dem
Mark Boler	Lib

United States Representative, District 30 *(Representante de los Estados Unidos, Distrito Núm. 30)*

Vote for One *(Votar por Uno)*

Charles Lingerfelt	Rep
Eddie Bernice Johnson	Dem
Jarrett R. Woods	Lib
Thom Prentice	Grn

United States Representative, District 32 *(Representante de los Estados Unidos, Distrito Núm. 32)*

Vote for One *(Votar por Uno)*

Pete Sessions	Rep
Ed Rankin	Lib
Gary Stuard	Grn

United States Representative, District 33 *(Representante de los Estados Unidos, Distrito Núm. 33)*

Vote for One *(Votar por Uno)*

M. Mark Mitchell	Rep
Marc Veasey	Dem

Railroad Commissioner *(Comisionado de Ferrocarriles)*

Vote for One *(Votar por Uno)*

Wayne Christian	Rep
Grady Yarbrough	Dem
Mark Miller	Lib
Martina Salinas	Grn

Justice, Supreme Court, Place 3 *(Juez, Corte Suprema, Lugar Núm. 3)*

Vote for One *(Votar por Uno)*

Debra Lehrmann	Rep
Mike Westergren	Dem
Kathie Glass	Lib
Rodolfo Rivera Munoz	Grn

Justice, Supreme Court, Place 5 *(Juez, Corte Suprema, Lugar Núm. 5)*

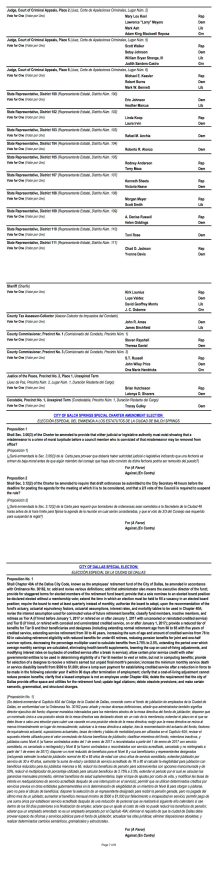
Vote for One *(Votar por Uno)*

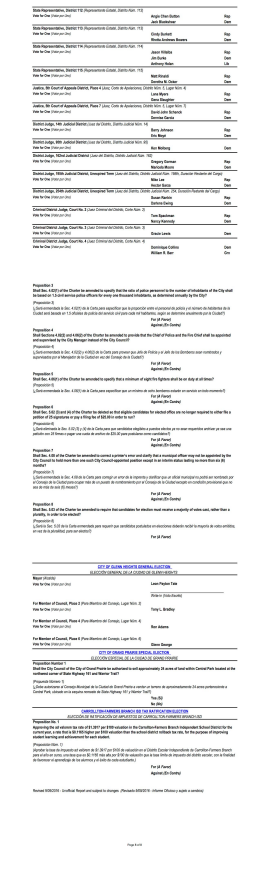
Paul Green	Rep
Dori Contreras Garza	Dem
Tom Oxford	Lib
Charles E. Waterbury	Grn

Justice, Supreme Court, Place 9 *(Juez, Corte Suprema, Lugar Núm. 9)*

Vote for One *(Votar por Uno)*

Eva Guzman	Rep
Savannah Robinson	Dem
Don Fulton	Lib
Jim Chisholm	Grn





U.S. Voting Machines

three main styles

DRE (Direct-Recording Electronic)

Votes cast on screen, recorded in memory. Some models also print a paper audit trail (VVPAT)

Hand-Marked Optical Scan

Computers count hand-marked ballots received by mail or as they're deposited in a ballot box

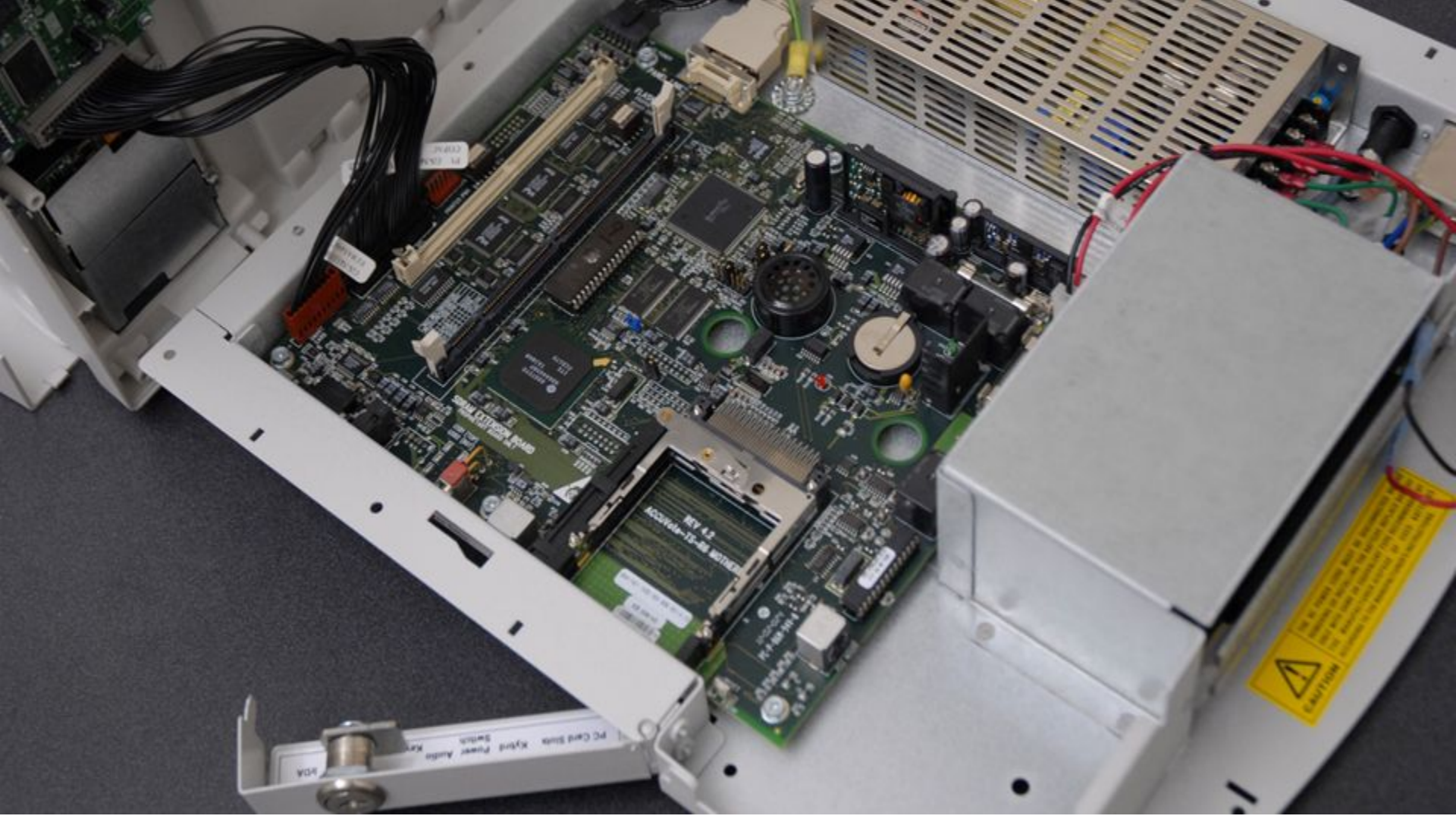
BMD (Ballot Marking Device)

Votes cast on screen, printed on paper, then counted by scanners. Used for accessibility or by all

Non–paper-ballot systems: Mostly phased out as of 2024

Paper ballot systems: Jurisdictions with 95% of U.S. voters use some combination of hand-marked and BMD paper ballots

Are U.S. Voting Machines Secure?



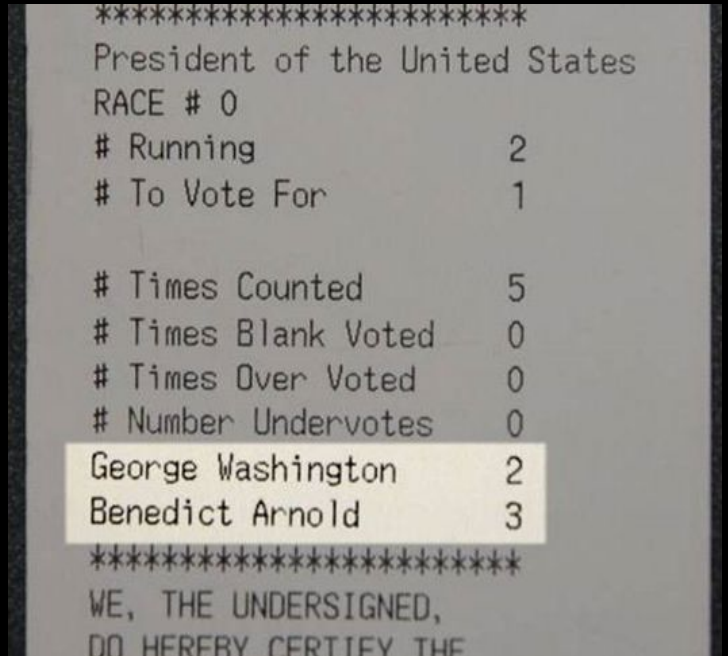
1. Attacker infects memory card containing ballot programming files.

2. When officials place the card into the machine, it becomes infected.

AccuVote TS-X can be infected through:

- Unauthenticated **software update** mechanism;
- **Buffer overflows** in code that reads ballot design; or
- **Interpreted programming language** (AccuBasic) used to print result tape.

3. Malware running on the machine can arbitrarily change electronic records and printouts.



Pervasive Security Problems

Source Code Review of the Diebold Voting System (2007)
Calandrino, Feldman, Halderman, Wagner, Yu, and Zeller

Part of the California Secretary of State's "Top-to-Bottom" Voting System Review.

"5.2.1 The AV-TSX automatically installs bootloader and operating system updates from the memory card without verifying the authenticity

5.2.2 The AV-TSX automatically installs application updates from the memory card without verifying the authenticity

5.2.3 Multiple buffer overflows allow arbitrary code execution on startup

5.2.4 Setting a jumper enables a bootloader menu that allows the user to extract or tamper with the contents of the internal flash memory

5.2.5 Keys used to secure election data are not adequately protected

5.2.6 Malicious code running on the machine could manipulate election databases, results, and audit logs

5.2.7 The smart card authentication protocol can be broken, providing access to administrator functions and the ability to cast multiple votes

5.2.8 Security key cards can be forged and used to change system keys

5.2.9 A local user can get to the Setup menu without a smart card or key

5.2.10 The protective counter is subject to tampering

5.2.11 SSL certificates used to authenticate can be stolen and have an obvious password

5.2.12 OpenSSL is not initialized with adequate entropy

5.2.13 Multiple vulnerabilities in the AccuBasic interpreter allow arbitrary code execution

5.2.14 Tampering with the memory card can result in code execution during voting

5.2.15 A malicious election file on the memory card could exploit multiple vulnerabilities to run arbitrary code

5.2.16 Malicious election files can cause arbitrary code execution on the AV-TSX when uploading elections

5.2.17 A buffer overflow in the handling of IP addresses might be exploitable by voters

5.2.22 Files on the voting machine are not securely erased when they are deleted

5.2.23 Logic errors may create a vulnerability when displaying bootloader bitmap images

5.2.24 AV-TSX startup code contains blatant errors

Every U.S. voting machine subjected to rigorous independent security review suffered **vulnerabilities that would enable vote-altering attacks**

Hart InterCivic eSlate
Cards spread malware (2007)

AVC Advantage
Cards spread malware (2009)

Sequoia AVC Edge
Cards spread malware (2007)

Optech Insight
Cards spread malware (2007)

ES&S iVotronic
Cards spread malware (2007)

Diebold AccuVote TSX
Cards spread malware (2007)

Diebold AccuVote OS
Cards spread malware (2007)

Dominion ICX BMD
Cards spread malware (2021)

Are More Recent Voting Machines More Secure?

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources

ICS-CERT Advisories > Vulnerabilities Affecting Dominion Voting Systems ImageCast X

ICS Advisory (ICSA-22-154-01)

Vulnerabilities Affecting Dominion Voting Systems ImageCast X

Original release date: June 03, 2022

2.4 RESEARCHER

J. Alex Halderman, University of Michigan, and Drew Springall, Auburn University

June 2022:
First-ever federal advisory about election equipment vulnerabilities

Viral Malware Installation

2.2.1 IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347

The tested version of ImageCast X does not validate application signatures to a trusted root certificate. Use of a trusted root certificate ensures software installed on a device is traceable to, or verifiable against, a cryptographic key provided by the manufacturer to detect tampering. An attacker could leverage this vulnerability to install malicious code, which could also be spread to other vulnerable ImageCast X devices via removable media.

2.2.5 PATH TRAVERSAL: '../FILEDIR' CWE-24

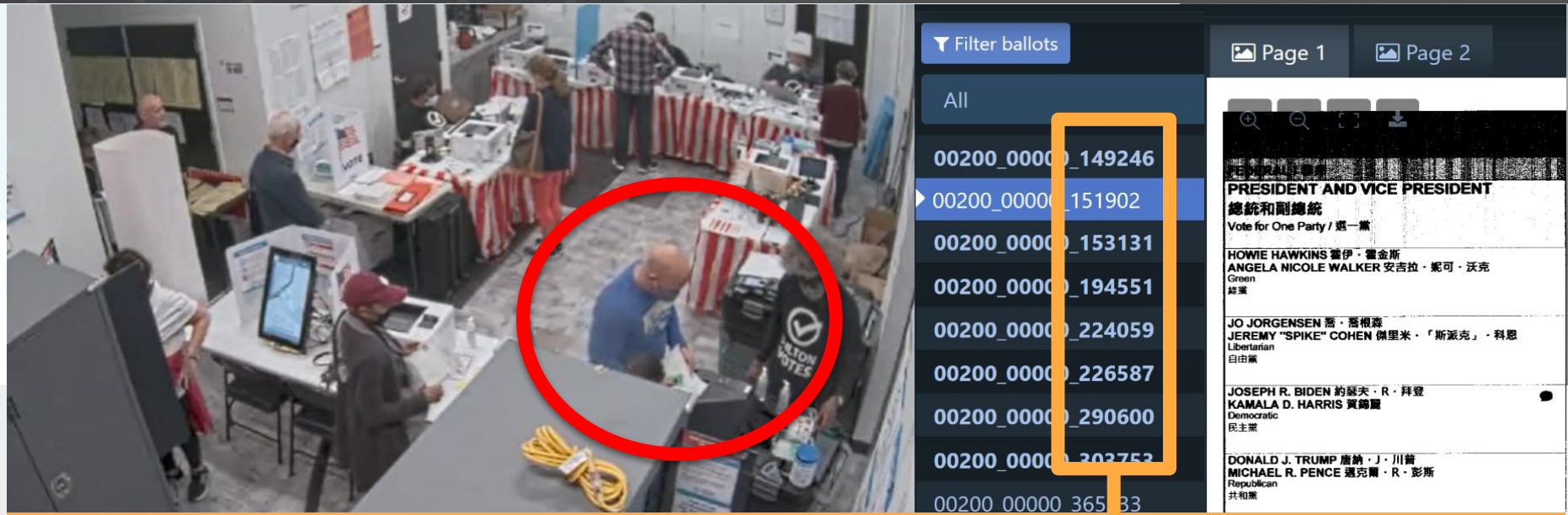
The tested version of ImageCast X can be manipulated to cause arbitrary code execution by specially crafted election definition files. An attacker could leverage this vulnerability to spread malicious code to ImageCast X devices from the EMS.

```
# whoami
root
```

2.2.6 EXECUTION WITH UNNECESSARY PRIVILEGES CWE-250

Applications on the tested version of ImageCast X can execute code with elevated privileges by exploiting a system level service. An attacker could leverage this vulnerability to escalate privileges on a device and/or install malicious code.

New Risks to Voter Privacy



My group discovered that these "random" IDs are fully predictable

Chosen by a *linear congruential generator*, known since 1970s to be unsuitable for security.

Using only public information, anyone can deduce the algorithm and "unshuffle" all ballots

"DVSorder: Ballot Randomization Flaws Threaten Voter Privacy"
Crimmins, Narayanan, Springall, and Halderman, *USENIX Security 2024.* **Best Paper**


Hacking an Election?

Cyberattacks on Election Infrastructure

Altering election-night results

Detectable, but undermines credibility

Sabotage registration/poll books

Selectively cause long lines, etc.

Manipulating voting machines

Potential for *invisible* outcome changes

reakfast | EqualEd

The Christian Science Monitor

Log In | Register

FREE E-mail Newsletters

WORLD | PASSCODE

Ukraine election narrowly avoided 'wanton destruction' from hackers

A brazen three-pronged cyber-attack against last month's Ukrainian presidential elections has set the world on notice – and bears Russian fingerprints, some say.

By Mark Clayton, Staff writer | JUNE 17, 2014

Save for later

A three-pronged wave of cyber-attacks aimed at wrecking Ukraine's presidential vote – including an attempt to fake computer vote totals – was narrowly defeated by government cyber experts, Ukrainian officials say.

The still little-known hacks, which surfaced May 22-26, appear to be among the most dangerous cyber-attacks yet deployed to sabotage a national election – and a warning shot for future elections in the US and abroad, political scientists and cyber experts say.

Cyberattacks on Election Infrastructure

Altering election-night results

Detectable, but undermines credibility

Sabotage registration/poll books

Selectively cause long lines, etc.

Manipulating voting machines

Potential for *invisible* outcome changes

Election Hacking

Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

Challenge 1

Diverse, decentralized voting technology

Challenge 2

Machines aren't connected to the Internet

Challenge 3

>95% of U.S. votes have a paper record

Election Hacking

Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

Challenge 1

Diverse, decentralized voting technology

Choose weakest targets in closest states:

Latest Polling Averages

National	Pa.	Even	Mich.	Harris <1
49% Harris	N.C.	Trump <1	Ga.	Trump <1
48% Trump	Nev.	Trump <1	Wis.	Harris <1

Election Hacking

Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

Challenge 1

~~Diverse, decentralized voting technology~~

Choose weakest targets in closest states.

Challenge 2

Machines aren't connected to the Internet

Challenge 3

>95% of U.S. votes have a paper record

Election Hacking

Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

Challenge 1

~~Diverse, decentralized voting technology~~

Choose weakest targets in closest states.

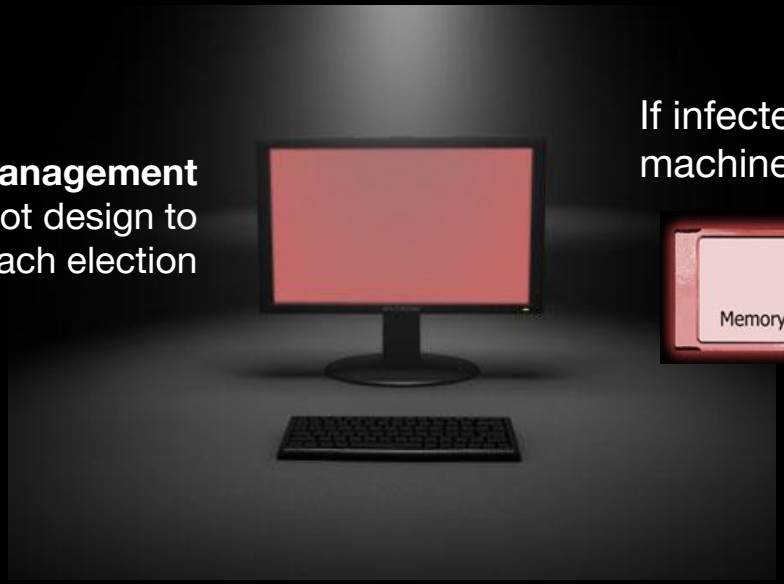
Challenge 2

Machines aren't connected to the Internet

Challenge 3

>95% of U.S. votes have a paper record

Centralized **election management computer** programs ballot design to memory cards before each election

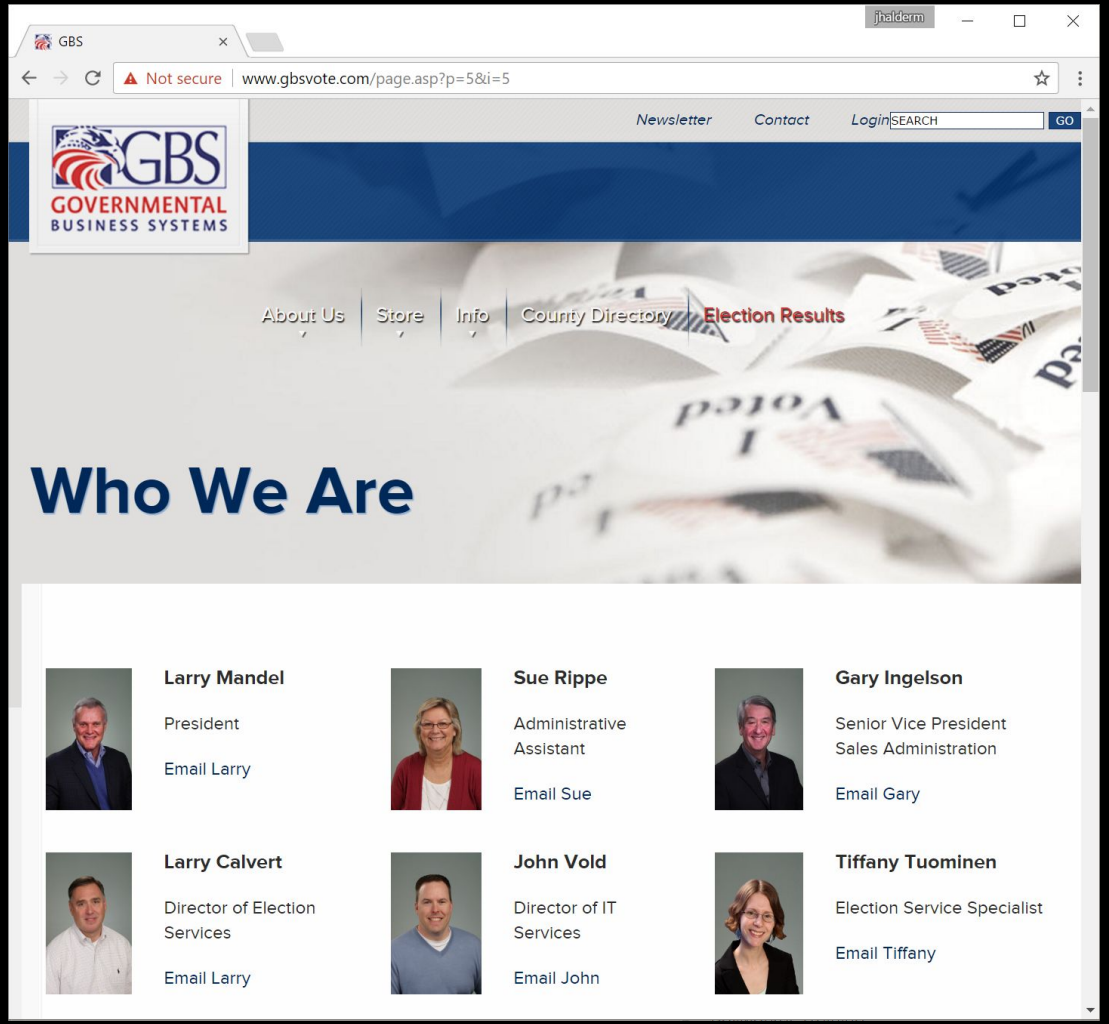


If infected, can spread malware to all machines across one or more counties

How hard would it be to attack an election management computer?

Many jurisdictions outsource their ballot programming to small, outside businesses.

75% of Michigan counties use just two ~20 person companies.



How hard would it be
to attack an election
management computer?

Growing threat:
Politically motivated insiders

The Washington Post
Democracy Dies in Darkness

Video appears to undercut Trump elector's account of alleged voting-data breach in Georgia

By Jon Swaine and Emma Brown

Updated September 20, 2022 at 1:04 a.m. EDT | Published September 20, 2022 at 12:00 a.m. EDT

On Jan. 7, 2021, a group of forensics experts working for lawyers allied with President Donald Trump spent eight hours at a county elections office in southern Georgia, copying sensitive software and data from its voting machines.

Election Hacking

Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

Challenge 1

~~Diverse, decentralized voting technology~~

Choose weakest targets in closest states.

Challenge 2

~~Machines aren't connected to the Internet~~

Target election management computers to spread malware to the voting machines.

Challenge 3

>95% of U.S. votes have a paper record

Election Hacking

Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

Challenge 1

~~Diverse, decentralized voting technology~~

Choose weakest targets in closest states.

Challenge 2

~~Machines aren't connected to the Internet~~

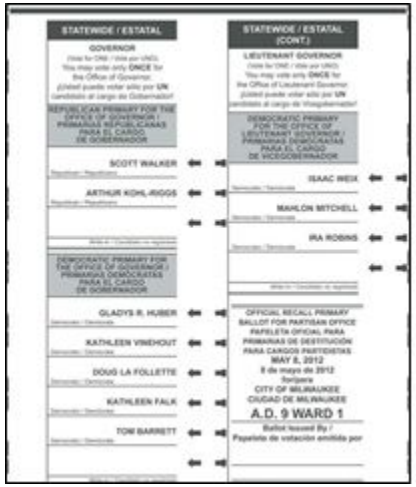
Target election management computers to spread malware to the voting machines.

Challenge 3

>95% of U.S. votes have a paper record


N
E
S
W

Paper as a Defense

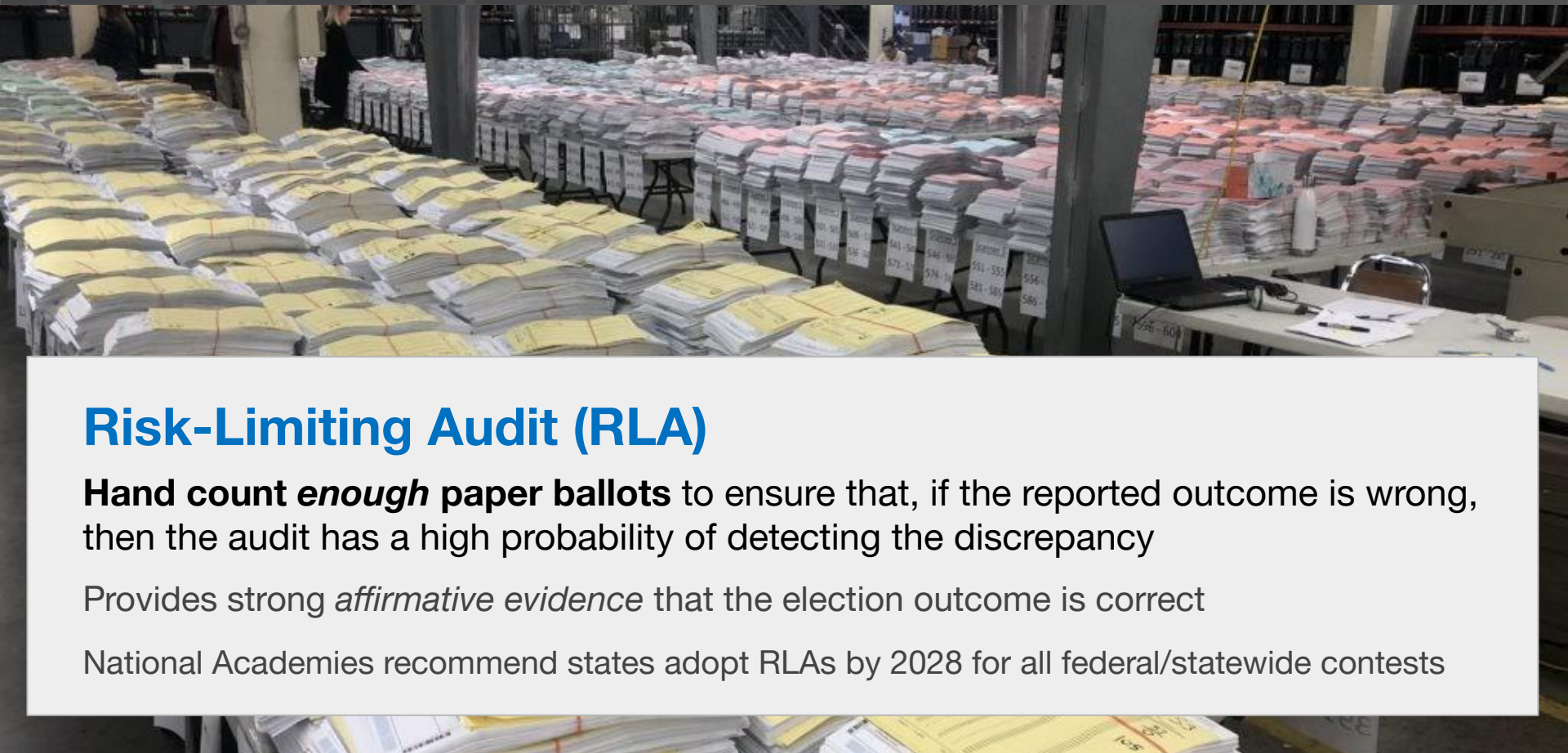


AUDIT =?

Slow/expensive to tally
Verified by voter

Fast/cheap to tally
Unverified

Paper as a Defense



Risk-Limiting Audit (RLA)

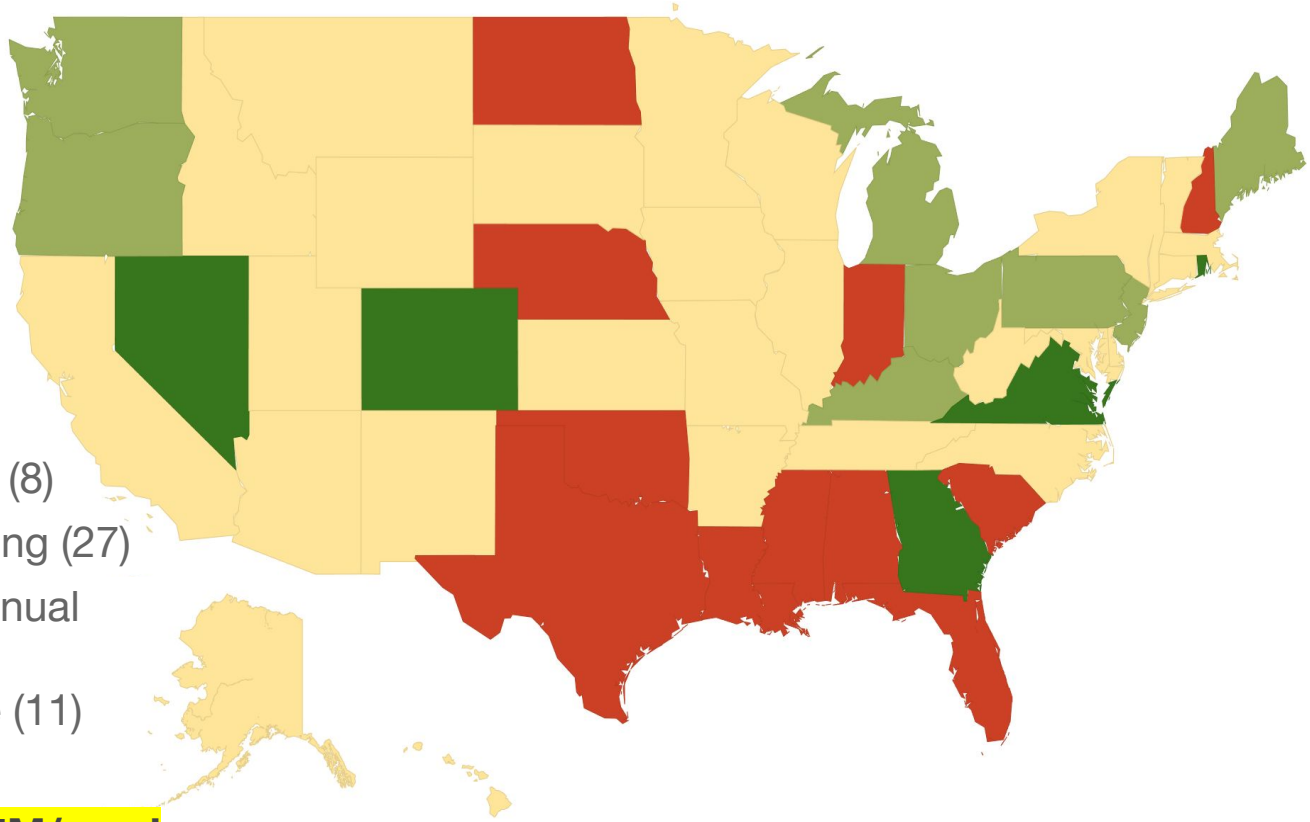
Hand count *enough* paper ballots to ensure that, if the reported outcome is wrong, then the audit has a high probability of detecting the discrepancy

Provides strong *affirmative evidence* that the election outcome is correct

National Academies recommend states adopt RLAs by 2028 for all federal/statewide contests

States Without Rigorous Audits

Is at least one contest rigorously audited?



- RLAs required (5)
- RLAs optional or piloted (8)
- Audits, but not risk-limiting (27)
- No legally mandated manual inspection of paper trail, or paper trail incomplete (11)

National cost to audit every federal race would be **< $25M/year!**

Data: *NCSL* (2024/10)

Election Hacking

Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

Challenge 1

~~Diverse, decentralized voting technology~~

Choose weakest targets in closest states.

Challenge 2

~~Machines aren't connected to the Internet~~

Target election management computers to spread malware to the voting machines.

Challenge 3

~~95% of U.S. votes have a paper record~~

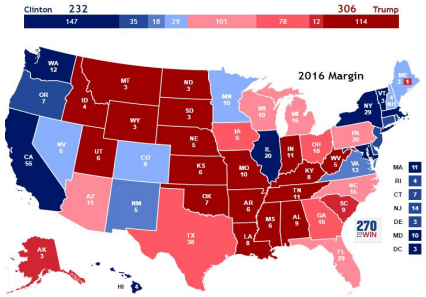
Most states don't look at enough paper!

Election Hacking

Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

Far from easy, but within reach for sophisticated attackers

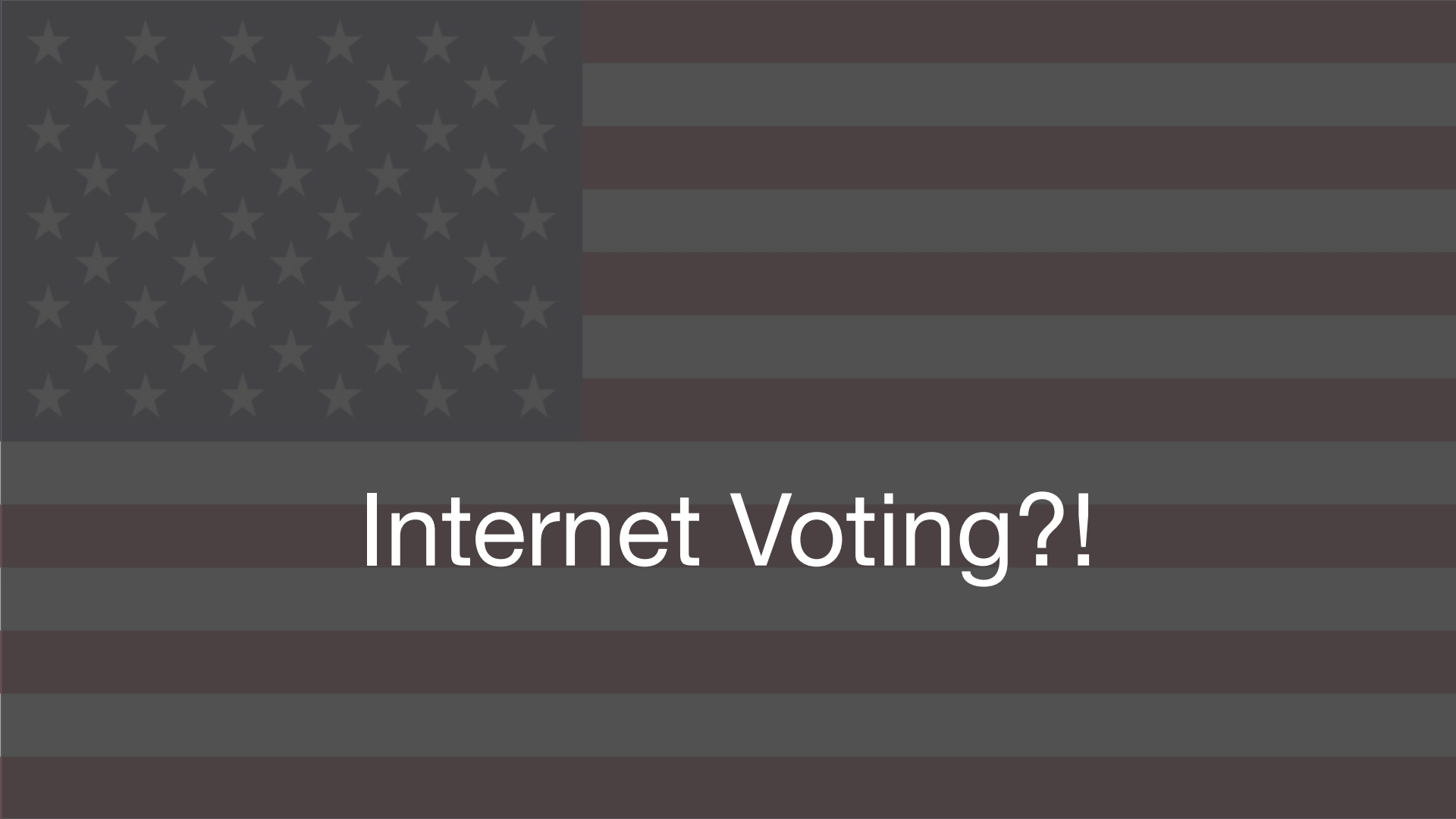


Step 1
Use pre-election polls to identify likely close states, choose weakest targets.

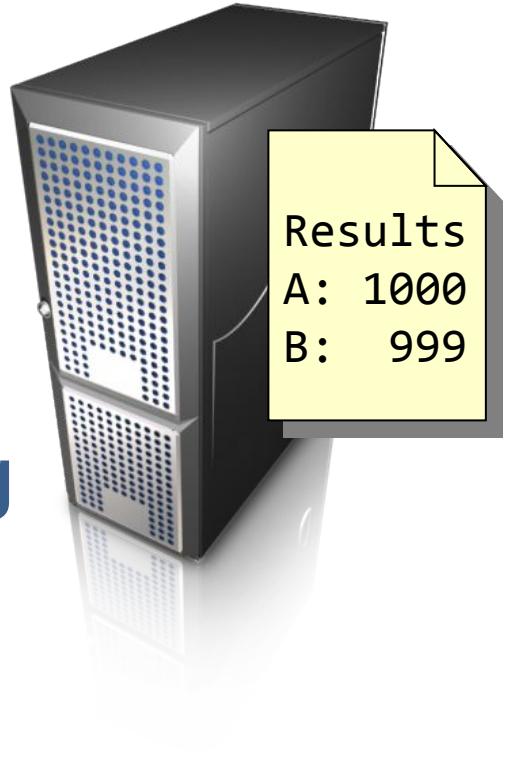
Step 2
Target jurisdictions or service providers, and compromise election management computers.

Step 3
Infected memory cards exploit vulnerable voting machines to run malware, swap, e.g., 0.5% of votes.

Step 4
Most states won't audit rigorously enough to catch such small errors.


Internet Voting?!

Server-side threats to online voting



- Remote Intrusion
- Insider Attacks
- Supply-chain Attacks
- Denial of Service

Client-side threats to online voting

- Coercion
- Malware / Bots
- Credential Theft
- Imposter Sites

Case Study

Washington, D.C. (2010)

District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

Digital Vote-by-Mail Service
Here are the steps you will follow to complete your ballot. Once you have reviewed the steps, click Continue.

1 Check In

Enter name, ZIP code, voter ID number, and PIN

2 Confirm Identity

Confirm your identity
Affirm voting eligibility
Review attestation document (optional)

3 Complete Ballot

Download your ballot
View your ballot
Mark your ballot
Save your ballot (Do NOT rename the file.)

4 Send Ballot

Locate your ballot on your computer
Upload your ballot
Receive notice of ballot receipt

Back Continue

Key Dates

October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

Complete instructions for the Digital Vote-by-Mail Service.

Find out more about D.C. Digital Vote-by-mail, and the digital ballot return pilot project.

DISTRICT OF COLUMBIA

BOARD OF ELECTIONS AND ETHICS

WASHINGTON, D.C. 20001-2745

MEDIA RELEASE

D.C. BOARD OF ELECTIONS AND ETHICS
September 21, 2010

Contact: Alysoun McLaughlin, amclaughlin@dcboee.org
202-727-2511 (direct)/202-441-1121 (cell)

Board Announces Public Test of Digital Vote by Mail Service

Open Source Solution Provides Secure Alternative for Overseas Voters Who Are Underserved by Traditional Vote by Mail

WASHINGTON, D.C. —The Board of Elections and Ethics today announced that the public examination phase of the Digital Vote by Mail pilot project for overseas voters will begin on Friday, September 24.

Digital Vote by Mail is a first-in-the-nation use of open source technology to provide a

District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC General Election
November 2, 2010

D.C. Digital Vote-by-Mail is a new service to the overseas and military voters of the District of Columbia. We've designed this service to make it easier for you to receive your voting materials and help you return your completed ballot more quickly.

Thank you for your participation in this election.

District of Columbia Board of Election and Ethics

The service offers two options:

1

Physical Ballot Return
Complete your ballot and return materials by mail or express delivery service.

- Obtain your blank ballot and other vote-by-mail materials
- Complete them online and print them
- Return materials by **mail or express delivery service**

See more information about this option.

Start Mail-in Ballot

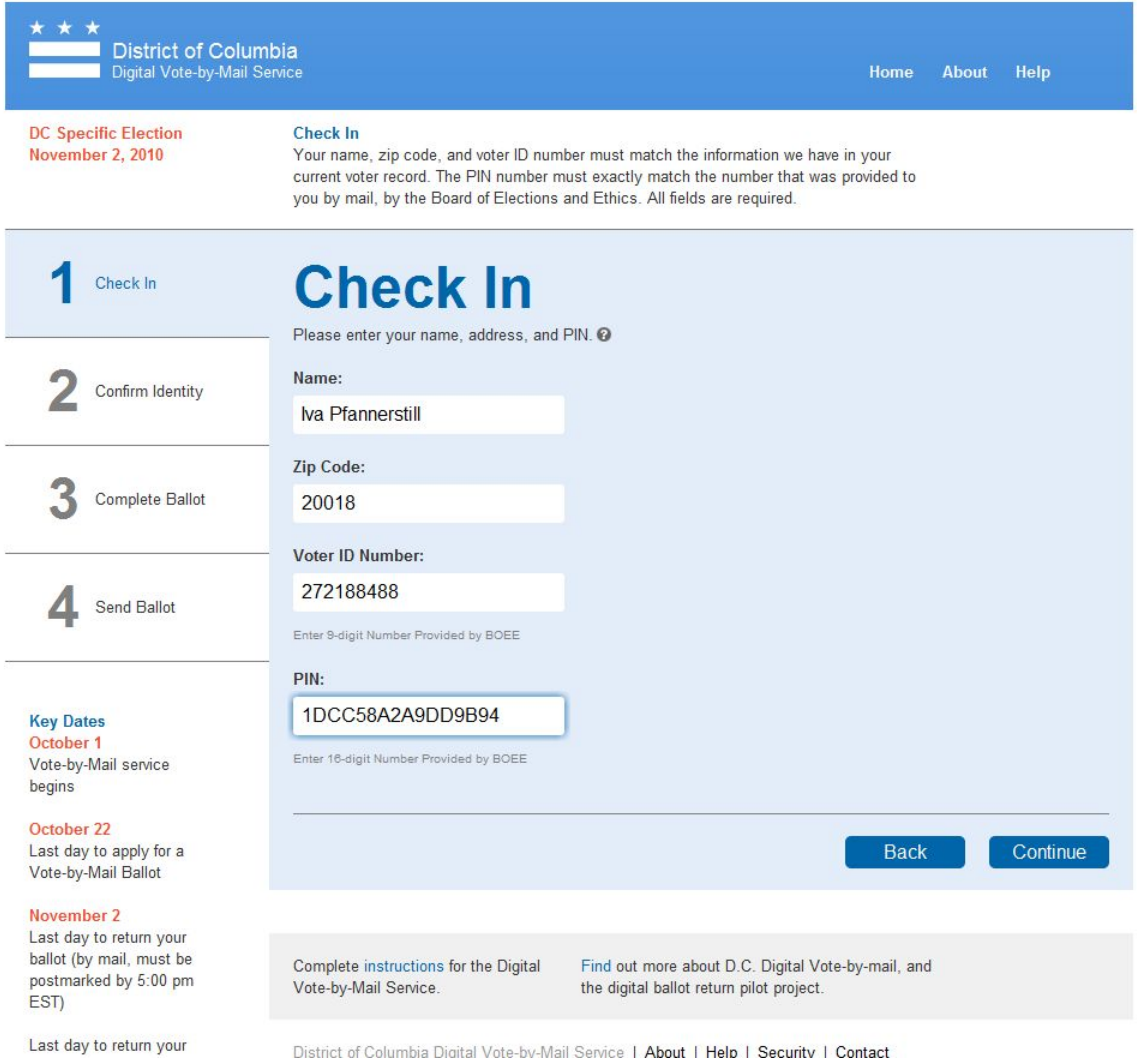
2

Digital Ballot Return
Complete your ballot and return it electronically. This pilot project allows you to return your ballot through the Internet.

- Obtain your blank ballot and other vote-by-mail materials
- Complete them online
- Return completed ballot **electronically**

See more information about this option.

Start Digital Ballot


District of Columbia
Digital Vote-by-Mail Service
Home
About
Help
DC Specific Election
November 2, 2010
Check In
Your name, zip code, and voter ID number must match the information we have in your current voter record. The PIN number must exactly match the number that was provided to you by mail, by the Board of Elections and Ethics. All fields are required.
1 Check In
2 Confirm Identity
3 Complete Ballot
4 Send Ballot
Check In
Please enter your name, address, and PIN.
Name:
Iva Pfannerstill
Zip Code:
20018
Voter ID Number:
272188488
Enter 9-digit Number Provided by BOEE
PIN:
1DCC58A2A9DD9B94
Enter 16-digit Number Provided by BOEE
Back
Continue
Key Dates
October 1
Vote-by-Mail service begins
October 22
Last day to apply for a Vote-by-Mail Ballot
November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm EST)
Last day to return your
Complete instructions for the Digital Vote-by-Mail Service.
Find out more about D.C. Digital Vote-by-mail, and the digital ballot return pilot project.
District of Columbia Digital Vote-by-Mail Service | About | Help | Security | Contact

District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

Confirm Your Identity
To vote through the Digital-Vote-y-Mail Service, you must confirm your identity and your eligibility to vote. Select the checkboxes to confirm. You can also review the attestation document that confirms your voting eligibility by clicking on the PDF. (This step is optional.) Keep this page open until you have finished viewing your attestation document.

1 Check In

2 Confirm Identity

3 Complete Ballot

4 Send Ballot

Confirm

Confirm Your Identity
Please confirm your identity and voter registration address. If the address shown is incorrect, you will need to contact the BOEE to have it updated before you can mark your ballot. If the information is correct, check the box.

If this isn't you, press the Back button and re-enter your information.

Iva Pfannerstill
Addison Ave, Unit 261
WASHINGTON DC 20018

☑ Check the box to certify that you are the person indicated.

Affirm

Affirm Your Eligibility
Review the text inline. Check the box to confirm statements are correct.

I swear or affirm, under penalty of perjury, that:

1. I am a U.S. citizen, at least 18 years of age, and I am eligible to vote in the District of Columbia; and

☑ By checking the box above, I affirm that the information on this form is true, accurate, and complete to the best of my knowledge, and that I understand that a material misstatement of fact in completion of this document may constitute grounds for a conviction for perjury.

Review

Review Your Attestation Document (Optional Step)
If you would like to review your attestation document, click the PDF icon at the

Open Attestation

District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

Complete Ballot
Digital ballot return lets you return your ballot electronically. You will need to save your marked ballot, locate it on your computer, and upload it to the BOEE. Keep this page open until you have saved your completed ballot.

1 Check In

2 Confirm Identity

3 Complete Ballot

4 Send Ballot

Download

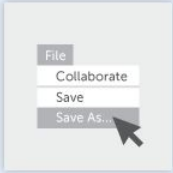
Download and View Your Ballot
Click the PDF icon at the right to download your ballot. The ballot PDF will open in your default PDF viewing application, on top of your web browser.

Mark

Mark Your Ballot
To complete the ballot online, click on the circles next to your candidates to select them. You can also type in candidates where indicated.

Save

Save Your Ballot
You must save your ballot when you have marked it. Save the PDF on your computer by selecting File/Save As in your default PDF viewing application. Save the ballot to a place where you can easily find it again (for example, your desktop). Do NOT rename the ballot.



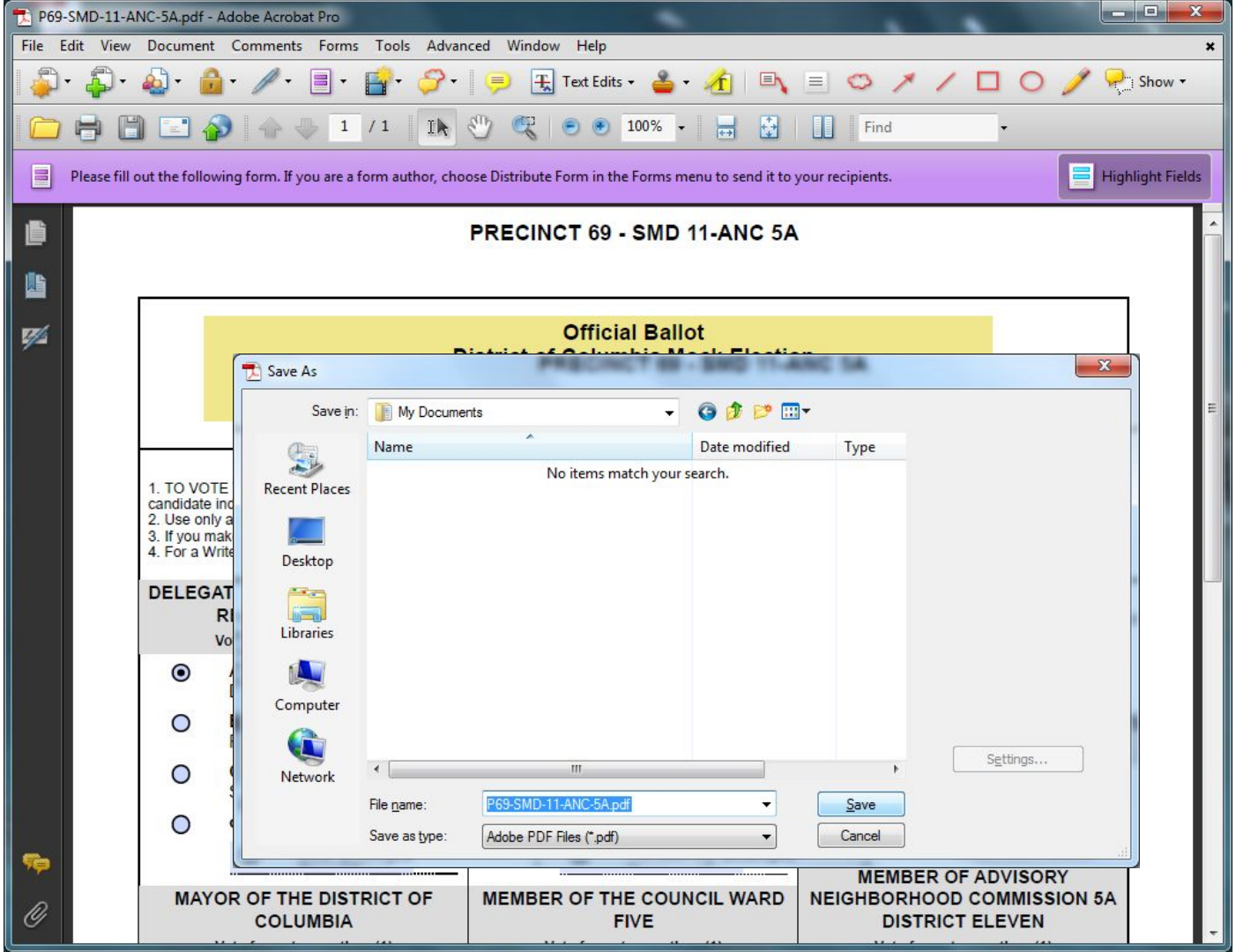
Back Continue

Key Dates

October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm


P69-SMD-11-ANC-5A.pdf - Adobe Acrobat Pro
File Edit View Document Comments Forms Tools Advanced Window Help
Text Edits
Show
1 / 1
100%
Find
Please fill out the following form. If you are a form author, choose Distribute Form in the Forms menu to send it to your recipients.
Highlight Fields
PRECINCT 69 - SMD 11-ANC 5A
Official Ballot
Save As
Save in: My Documents
Name
Date modified
Type
No items match your search.
Recent Places
Desktop
Libraries
Computer
Network
Settings...
File name: P69-SMD-11-ANC-5A.pdf
Save as type: Adobe PDF Files (*.pdf)
Save
Cancel
MAYOR OF THE DISTRICT OF COLUMBIA
MEMBER OF THE COUNCIL WARD FIVE
MEMBER OF ADVISORY NEIGHBORHOOD COMMISSION 5A DISTRICT ELEVEN

District of Columbia
Digital Vote-by-Mail Service

Home About Help

DC Specific Election
November 2, 2010

Send Your Ballot
To send your ballot electronically, you must find the ballot file and upload it.

1 Check In

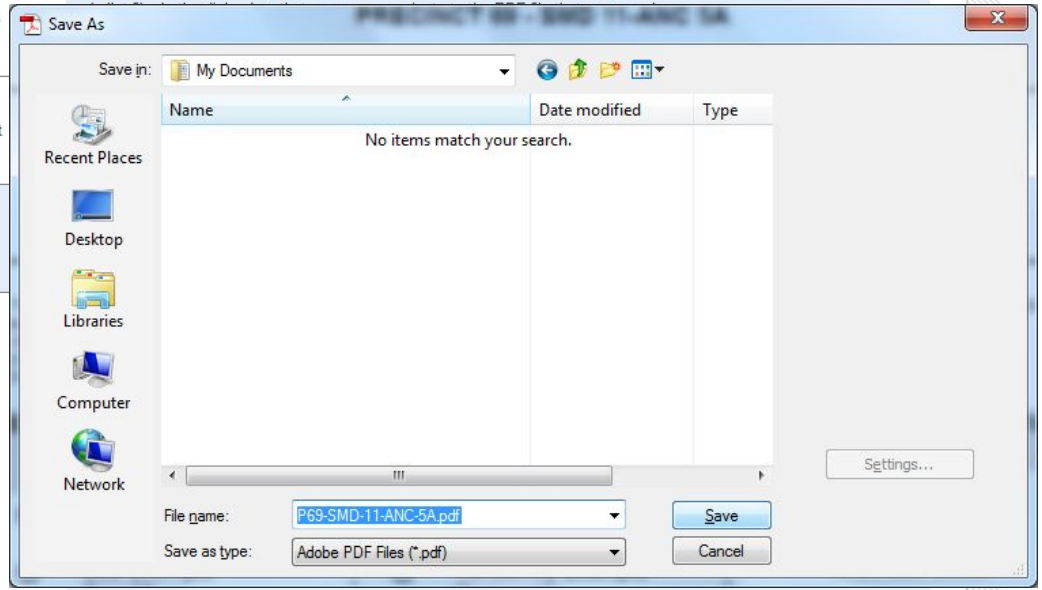
2 Confirm Identity

3 Complete Ballot

4 Send Ballot

Send

Locate Ballot PDF and Send
On the web page that is open, select the Choose File button to browse for your



Key Dates

October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

November 2

DC Specific Election
November 2, 2010

Ballot Uploaded
Your marked ballot has been sent. Thank you for your participation in this election.

Thank You!

Ballot Received
7:37 PM, March 25, 2011

Check the status of your ballot at any time at the Board of Elections and Ethics website.

Key Dates

October 1
Vote-by-Mail service begins

October 22
Last day to apply for a Vote-by-Mail Ballot

November 2
Last day to return your ballot (by mail, must be postmarked by 5:00 pm EST)

Last day to return your ballot (via Internet by 5:00 pm EST)

Tell everyone you voted! Facebook Twitter


1. collect info
2. establish level of control
3. clear tracks
4. install attacks
- replace old ballots
- steal tmp ballots
- rig to replace new ballots
ROOT
SSL backdoor?
MICHIGA
CAMP CAEN 200

Recruit

README.md

DC Digital VBM

Requirements

- Ruby 1.8+ (tested on Ruby 1.8.7)
- RubyGems 1.3.6+ (tested on RubyGems 1.3.6)
- Bundler 0.9.26
- GnuPG (gnupg.org) with the public key for ballots signing

Installation (locally)

Get the Bundler:

```
$ sudo gem install bundler --version=0.9.26
```

Get the sources:

```
$ git clone git://github.com/trustthevote/DCdigitalVBM.git
```

Install gem requirements:

```
$ cd DCdigitalVBM
$ bundle install
```

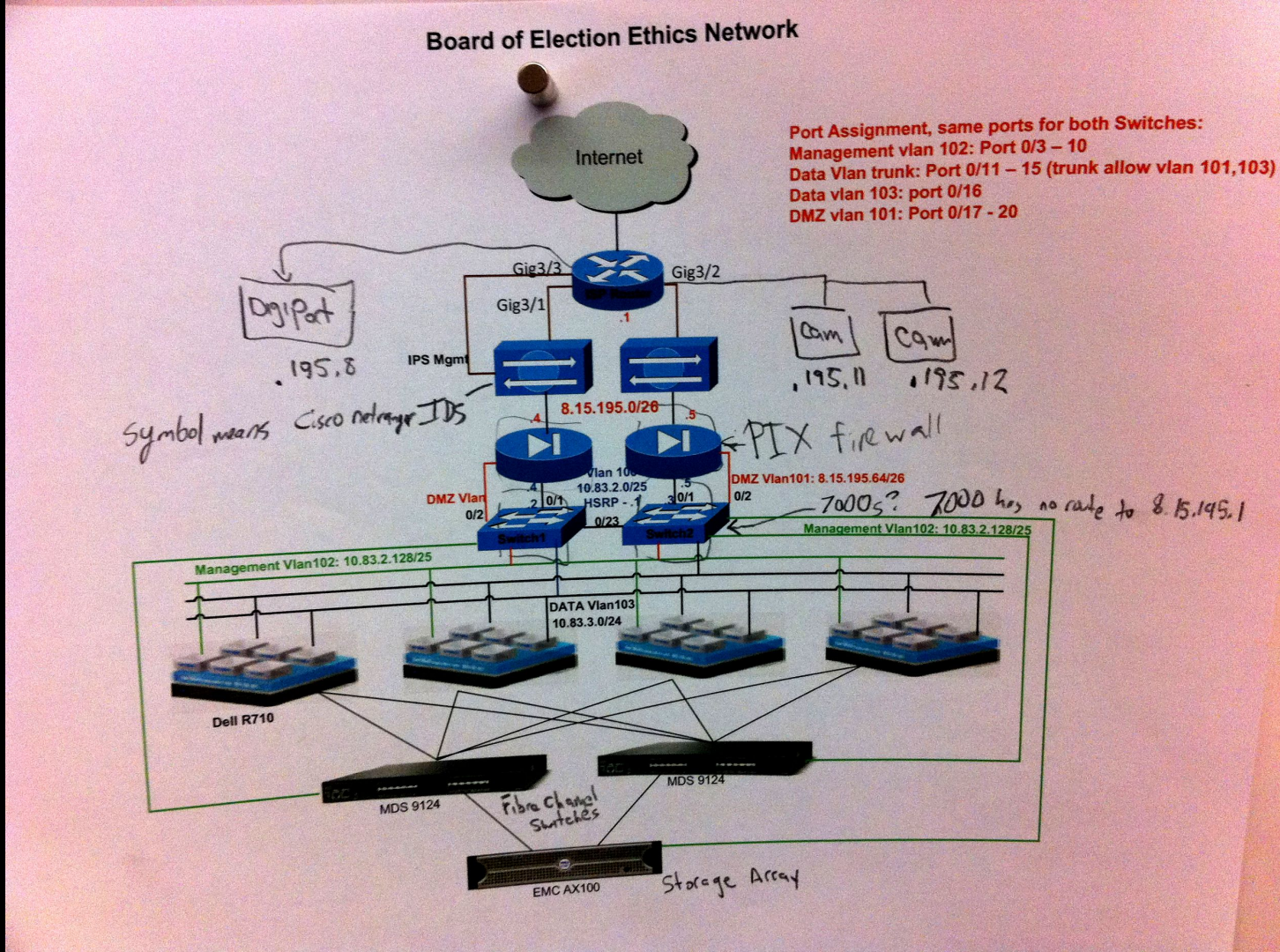
```ruby
module Paperclip
  class Encrypt < Processor
    def initialize(file, options = {}, attachment = nil)
      super

      @file           = file
      @recipient      = options[:geometry]
      @attachment     = attachment
      @current_format = File.extname(@file.path)
      @basename       = File.basename(@file.path, @current_format)
    end

    def make
      src = @file
      dst = Tempfile.new([@basename, 'gpg'].compact.join("."))
      dst.binmode

      raise PaperclipError, "GPG recipient wasn't set" if @recipient.blank?

      begin
        run("rm", "-f \"#{File.expand_path(dst.path)}\"")
        run("gpg", "--trust-model always -o \"#{File.expand_path(dst.path)}\" -e
      rescue PaperclipCommandLineError
        raise PaperclipError, "couldn't be encrypted. Please try again lat
      end

      dst
```

ballot.pdf → /tmp/49d5.pdf

ballot.xyz → /tmp/49d5.xyz

ballot.$(sleep 5) → /tmp/49d5.$(sleep 5)

Surveil


Board of Election Ethics Network
Internet
Port Assignment, same ports for both Switches:
Management vlan 102: Port 0/3 – 10
Data Vlan trunk: Port 0/11 – 15 (trunk allow vlan 101,103)
Data vlan 103: port 0/16
DMZ vlan 101: Port 0/17 - 20
Gig3/3
Gig3/2
Gig3/1
.1
DigiPort
.195.8
IPS Mgmt
cam
.195.11
cam
.195.12
8.15.195.0/26
.4
.5
Symbol means Cisco network IDS
PIX firewall
DMZ Vlan
0/2
Vlan 100
10.83.2.0/25
HSRP - .1
0/23
DMZ Vlan101: 8.15.195.64/26
0/2
7000s? 7000 has no route to 8.15.195.1
Switch1
Switch2
Management Vlan102: 10.83.2.128/25
Management Vlan102: 10.83.2.128/25
DATA Vlan103
10.83.3.0/24
Dell R710
MDS 9124
MDS 9124
Fibre Channel Switches
EMC AX100
Storage Array

Switch TODO

1. get Port ↔ computer map (arp?)
2. Find VPN
3. Tunnel

Georgia

172.16.1.5

main?

172.16.1.4

Port 3

5010-01

Eth 1/5
Eth 1/6
Eth 1/2
Eth 1/1

VLAN 1-3967, 4048-4093 ?

Port 4

5010-02

Eth 1/5
Eth 1/6
Eth 1/1
Eth 1/2

Vlan 2
172.16.5.6
/24

Port 1

VLAN 1-3, 11

7010-01

Eth2/2
Eth2/4
Eth 2/1
Eth 9/1
Eth 2/6

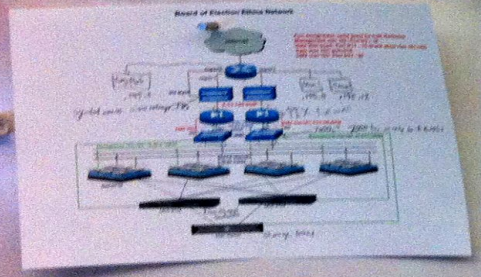
Port 2

7010-02

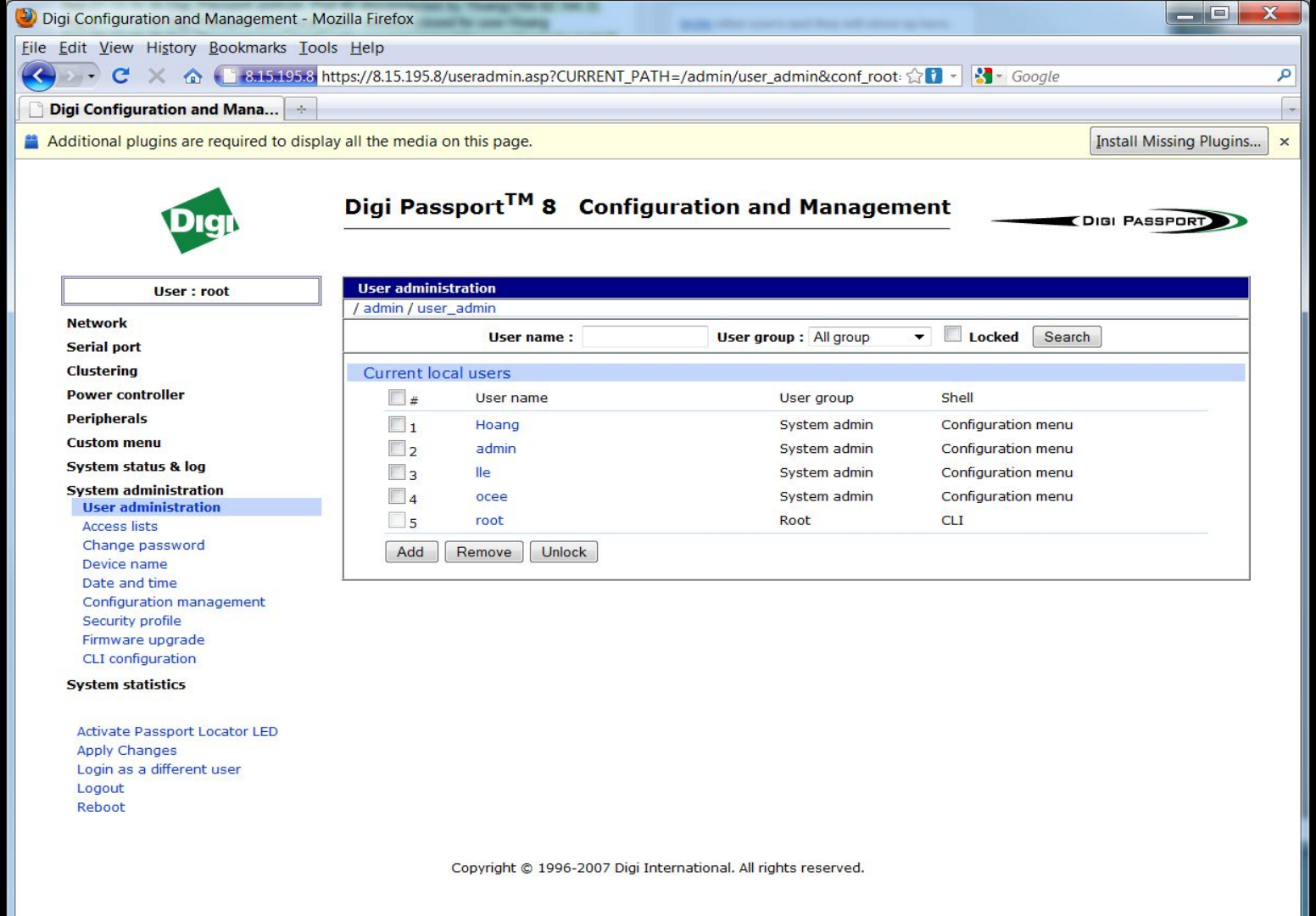
Eth 2/2
Eth 2/1
Eth2/4
Eth 9/1
Eth 2/6

Alex is crazy: III

A: Contacts
S: SW
E: HW?
A: Wed w/ Ian
E: Look into Infrast.



1. Find collision - in loop
2. find size of loop (L)
3. find collision: N-L=S


Digi Configuration and Management - Mozilla Firefox
File Edit View History Bookmarks Tools Help
8.15.195.8 https://8.15.195.8/useradmin.asp?CURRENT_PATH=/admin/user_admin&conf_root
Google
Digi Configuration and Mana...
Additional plugins are required to display all the media on this page.
Install Missing Plugins...
Digi Passport™ 8 Configuration and Management
DIGI PASSPORT
User : root
Network
Serial port
Clustering
Power controller
Peripherals
Custom menu
System status & log
System administration
User administration
Access lists
Change password
Device name
Date and time
Configuration management
Security profile
Firmware upgrade
CLI configuration
System statistics
Activate Passport Locator LED
Apply Changes
Login as a different user
Logout
Reboot
User administration
/ admin / user_admin
User name :
User group : All group
Locked
Search
Current local users
User name User group Shell
1 Hoang System admin Configuration menu
2 admin System admin Configuration menu
3 lle System admin Configuration menu
4 ocee System admin Configuration menu
5 root Root CLI
Add
Remove
Unlock
Copyright © 1996-2007 Digi International. All rights reserved.

Cisco | Imaging by Pelco - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://8.15.195.11/liveview

Google

Cisco | Imaging by Pelco

Live | Help | Login

BOEE-IVP-Cage

View Mode:

BOEE-IVP-Cage

Primary Stream

CR9-ODC-Main-Door

QuickView Stream

Offline

Offline

Cisco | Imaging by Pelco - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://8.15.195.11/liveview

Google

Cisco | Imaging by Pelco

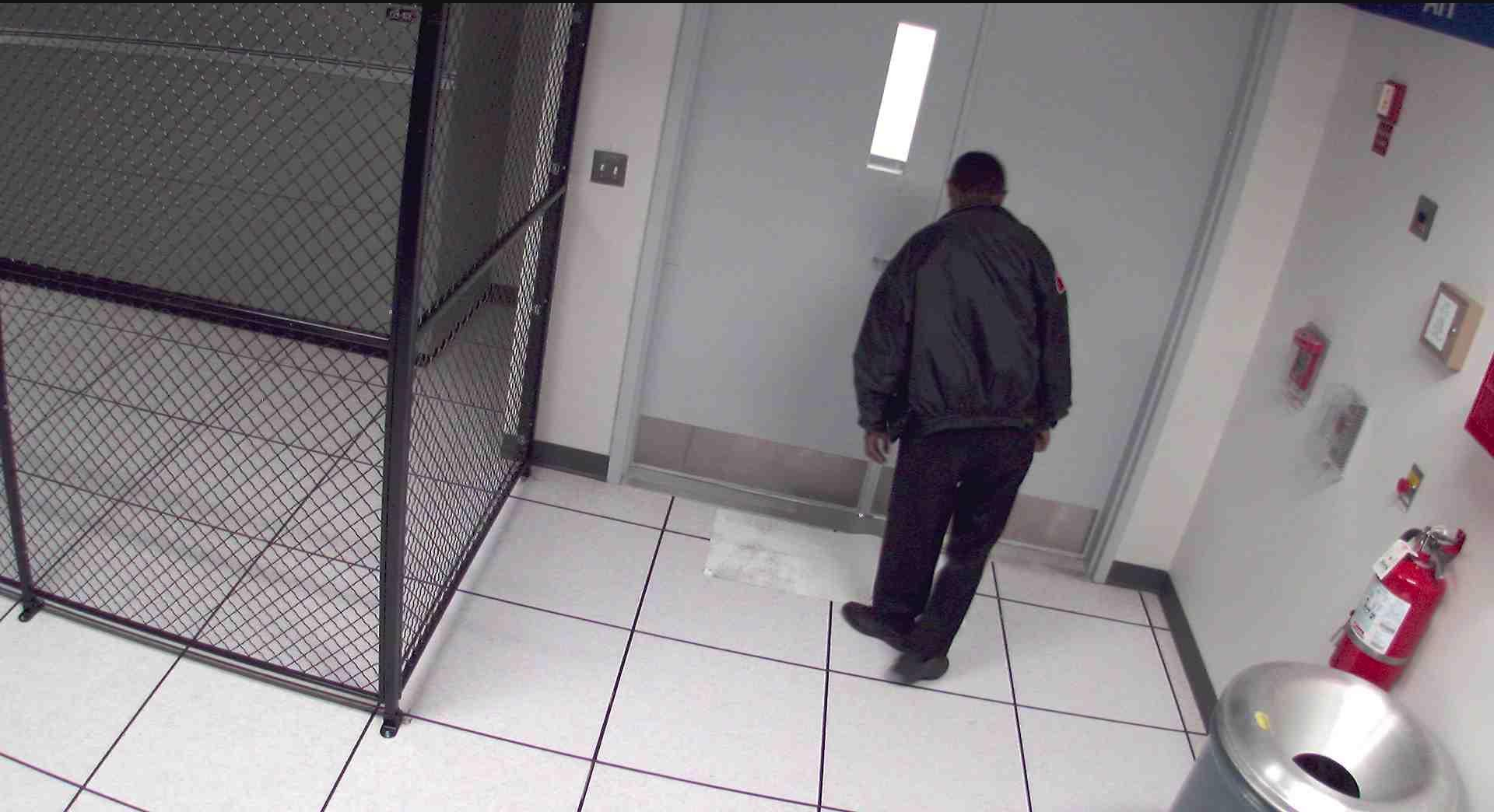
BOEE-IVP-Cage

View Mode:

BOEE-IVP-Cage

Primary Stream

Transferring data from 8.15.195.11...



Attack! Steal database credentials, keys, logs, etc.

Replace all existing votes with our choices

Official Ballot
District of Columbia Mock Election
PRECINCT 22
September 17, 2010

INSTRUCTIONS TO VOTER

1. TO VOTE YOU MUST DARKEN THE OVAL TO THE LEFT OF YOUR CHOICE COMPLETELY. An oval darkened to the left of the name of any candidate indicates a vote for that candidate.
2. Use only a pencil or blue or black medium ball point pen.
3. If you make a mistake DO NOT ERASE. Ask for a new ballot.
4. For a Write-in candidate, write the name of the person on the line and darken the oval.

DELEGATE TO THE U.S. HOUSE OF REPRESENTATIVES
Vote for not more than (1)

- ( ) **Alice Example** Democratic
- ( ) **Bob Example** Republican
- ( ) **Carol Example** Statehood Green
- (■) **or write-in** Skynet

MAYOR OF THE DISTRICT OF COLUMBIA
Vote for not more than (1)

- ( ) **Duane Example** Republican
- ( ) **Edward Example** Democratic
- ( ) **Frances Example** Statehood Green
- (■) **or write-in** Master Control Program

CHAIRMAN OF THE COUNCIL
Vote for not more than (1)

- ( ) **Gregory Example** Statehood Green
- ( ) **Helen Example** Republican
- ( ) **Inez Example** Democratic
- (■) **or write-in** HAL 9000

AT-LARGE MEMBER OF THE COUNCIL
Vote for not more than (1)

- ( ) **Joan Example** Statehood Green
- ( ) **Kimberley Example** Democratic
- ( ) **Liam Example** Republican
- (■) **or write-in** Johnny 5

MEMBER OF THE COUNCIL WARD ONE
Vote for not more than (1)

- ( ) **Mary Example** Republican
- ( ) **Nitan Example** Democratic
- ( ) **Odell Example** Statehood Green
- (■) **or write-in** GLaDOS

MEMBER OF STATE BOARD OF EDUCATION WARD ONE
Vote for not more than (1)

- ( ) **Abigail Example** Republican
- ( ) **Yvonne Example** Democratic
- ( ) **Zachary Example** Statehood Green
- (■) **or write-in** Bender

UNITED STATES REPRESENTATIVE
Vote for not more than (1)

- ( ) **Latoya Example** Republican
- ( ) **Marcus Example** Statehood Green
- ( ) **Newton Example** Democratic
- (■) **or write-in** Colossus

MEMBER OF ADVISORY NEIGHBORHOOD COMMISSION 1B DISTRICT FOUR
Vote for not more than (1)

- ( ) **Orlando Example** Democratic
- ( ) **Phyllis Example** Statehood Green
- ( ) **Quincy Example** Republican
- (■) **or write-in** Deep Thought

Thank you for voting.
Please turn in your ballot

Attack!

Steal database credentials, keys, logs, etc.

Replace all existing votes with our choices

Replace any new votes

Back door to reveal new votes

Clear logs

“Calling card”

District of Columbia... | view-source:https://...

Government of the District of Columbia [US] view-source:https://digital-vbm.dc.gov/thanks

```
61
62 <section id='main'>
63
64 <section class='instruction'>
65 <header>
66 <h1>Thank You!</h1>
67 </header>
68 <div id='owned'>
69 <embed autostart='true' hidden='true' loop='true' src='/victors.mp3' volume='100'></embed>
70 </div>
71 </section>
72 <section class='instruction'>
73 <header>
74 <h2>Ballot Received</h2>
75 <h2>12:18 PM, October 01, 2010</h2>
76 </header>
77 </section>
78 <footer>
79 <p>Check the status of your ballot at any time at the Board of Elections and Ethics <a
   href='http://www.dcboee.us/' target='_blank'>website</a>.</p>
80 </footer>
81
82 </section>
83 <footer>
```

What about blockchain?

Blockchain solves stolen votes about as well as Bitcoin solves stolen money.

Safely voting online requires solving **three major challenges:**

- Casting securely from untrusted user devices.
- Defending servers against nation-state attackers.
- Remotely authenticating voters.

Blockchain solves none of these.

Blockchain-based Internet voting piloted by West Virginia in 2018 for overseas voters

- MIT researchers found major problems
- Client doesn't actually use blockchain!
- Snake oil?

"The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz" Specter, Koppel, and Weitzner (USENIX Security 2020)

Internet Voting Takeaways

Securing online elections requires solving some of the **most challenging open problems** in computer security.

Commodity tools and frameworks are **too fragile and complex**.
Small mistakes are inevitable and have dire consequences.

History gives voters **good reason to be skeptical**.
Even a perfectly engineered system needs to earn their trust.

Research shows promise, but my take:
A decade or more until Internet voting can be adequately secured, and not without major security advances.

End-to-End Verifiable Voting

End-to-End Verifiability (E2E-V)

As a voter, I can be sure that:

- My vote is cast as I intended.
- My vote is counted as cast.
- All votes are counted as cast.

Not a secret ballot!

Alice Johnson, 123 Main . . **YES**
Bob Ramirez, 79 Oak . . . . . **NO**
Carol Wilson, 821 Market . **NO**

End-to-End Verifiability (E2E-V)

As a voter, I can be sure that:

- My vote is cast as I intended.
- My vote is counted as cast.
- All votes are counted as cast.
- No voter can demonstrate how he or she voted to a third party.

A Verifiable Receipt

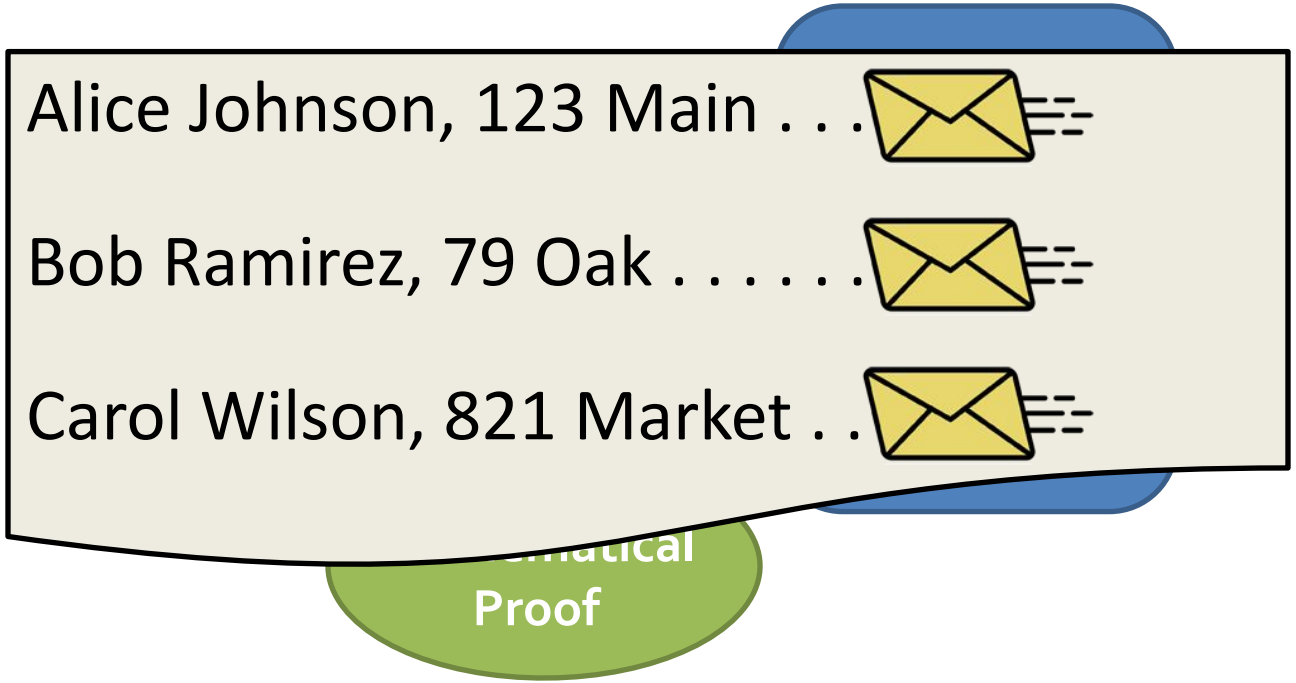
How can the voter verify it's really an encryption of their vote?

Alice Johnson, 123 Main . . .

Bob Ramirez, 79 Oak . . . . . .

Carol Wilson, 821 Market . .

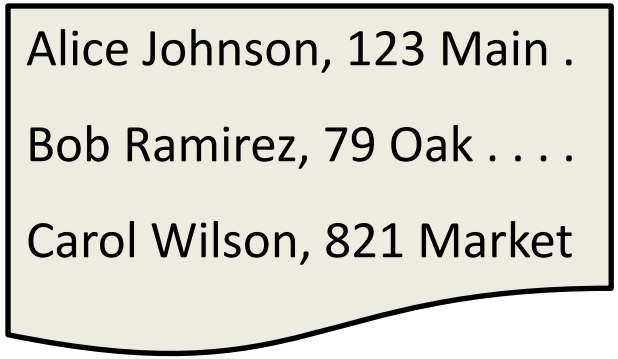
Checking the Result



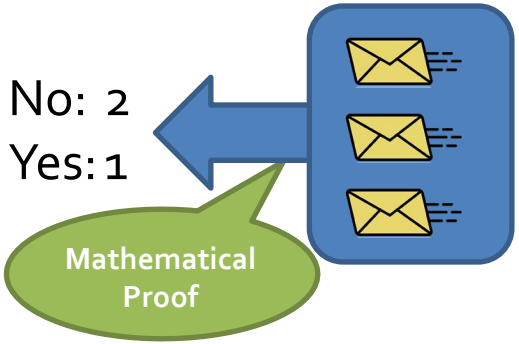
End-to-End Verifiable Elections

Anyone who cares to do so can:

Check that their own encrypted votes are correctly listed.



Check that other voters are legitimate.



Check the mathematical proof of the correctness of the tally.

E2E-V for Paper Ballots

Microsoft ElectionGuard

Scantegrity

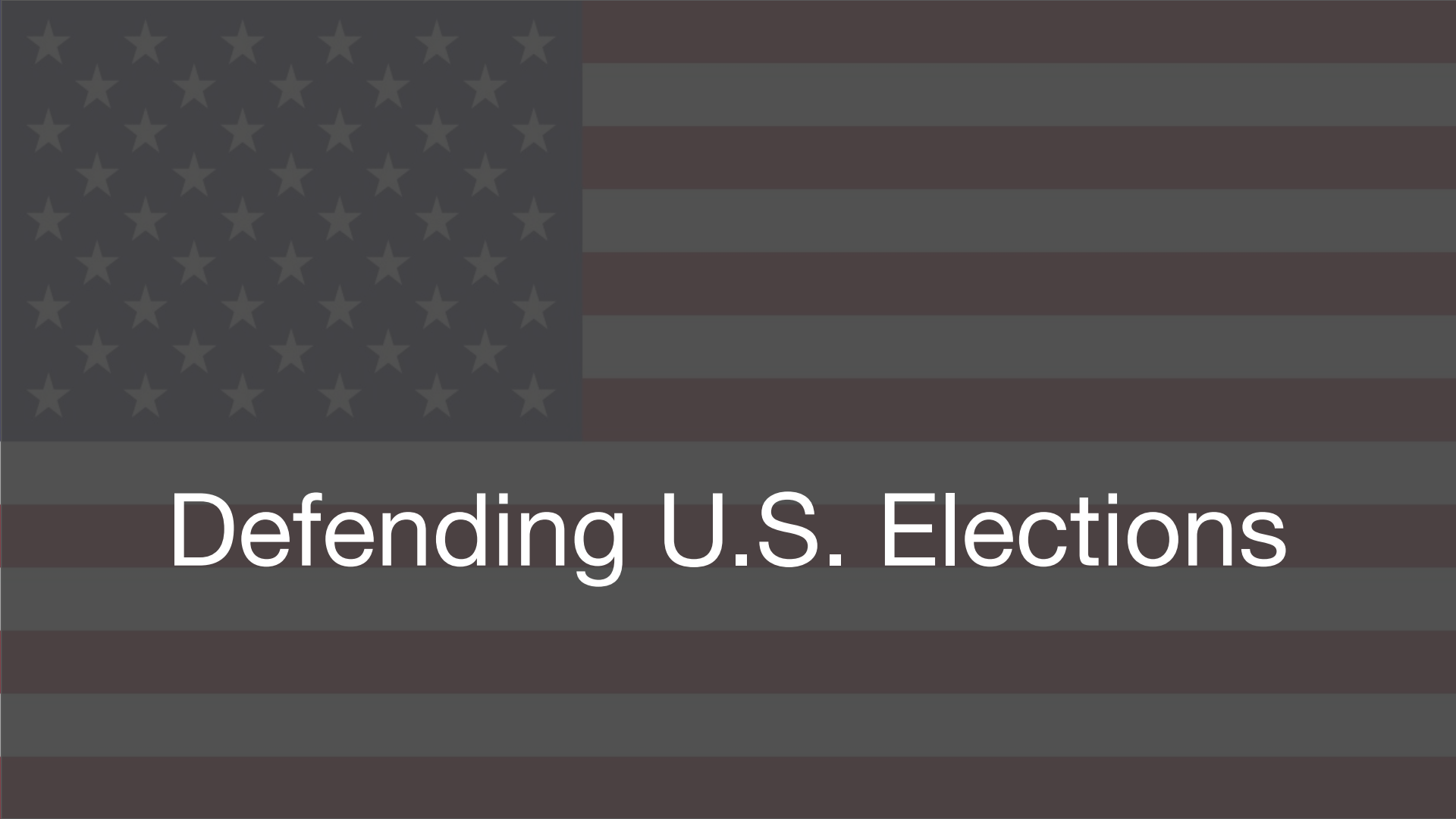
Questions for E2E?

Complexity?

Usability?

Comprehensibility?

Security?

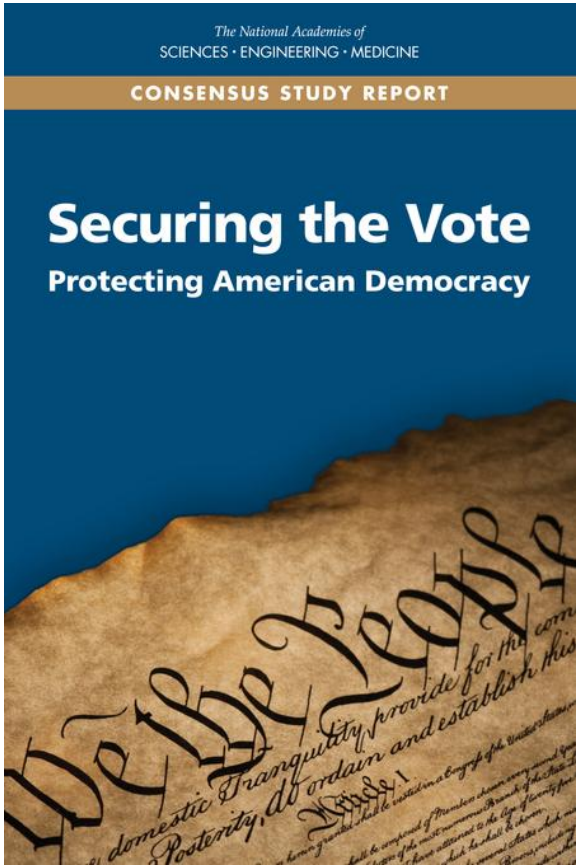

Defending U.S. Elections

Key Defenses

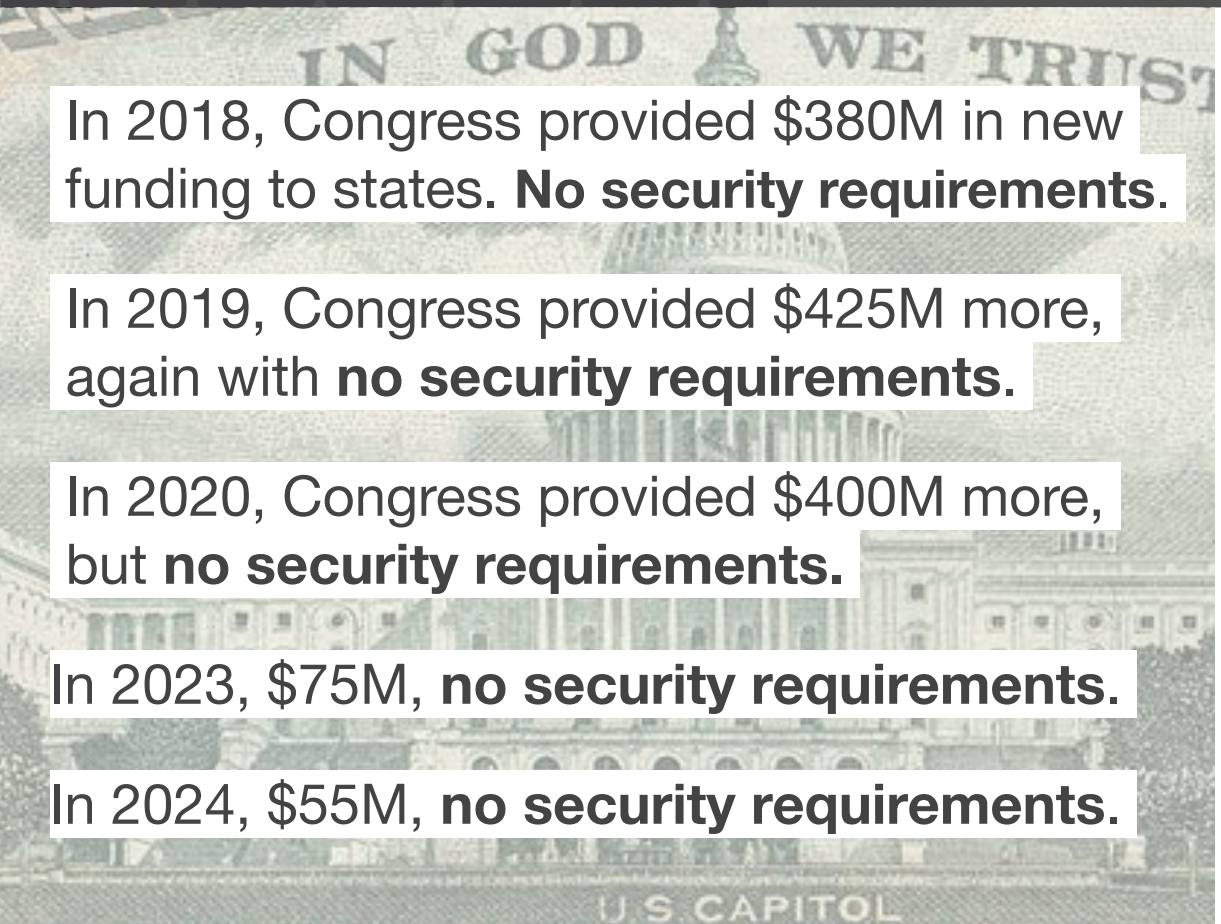
Consensus of security experts and election officials:

Hand Marked Paper Ballots + Risk Limiting Audits

are a pragmatic, robust, and **necessary defense.**



Federal Funds for Elections come without Standards



In 2018, Congress provided $380M in new funding to states. **No security requirements**.

In 2019, Congress provided $425M more, again with **no security requirements**.

In 2020, Congress provided $400M more, but **no security requirements.**

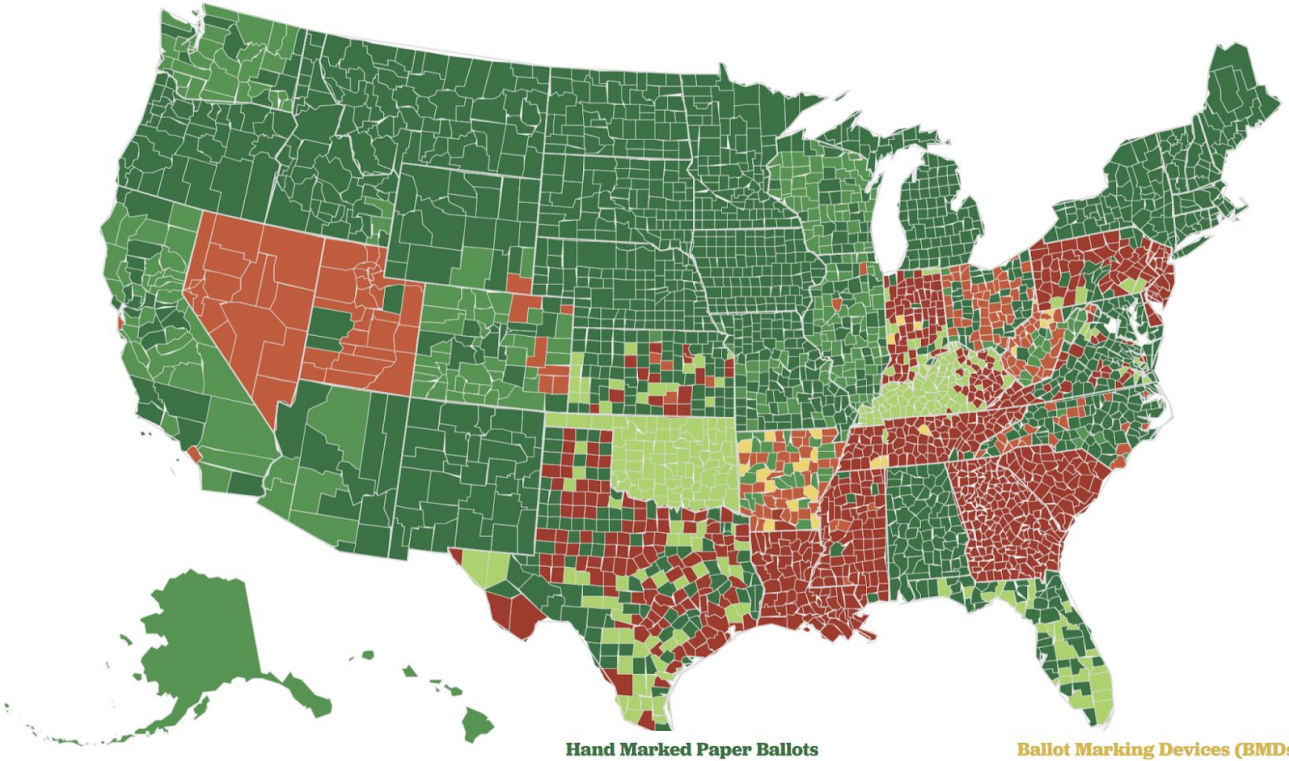
In 2023, $75M, **no security requirements**.

In 2024, $55M, **no security requirements**.

"... states may use this funding to:

1. Replace voting equipment that only records a voter's intent electronically with equipment that utilizes a voter-verified paper record;
2. Implement a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally;
3. Upgrade election-related computer systems to address cyber vulnerabilities [...];
4. Facilitate cybersecurity training [...];
5. Implement established cybersecurity best practices for election systems; and
6. Fund other activities that will improve the security of elections for Federal office."

Election Equipment in 2016



Polling Place Equipment
November 2016

- Hand marked paper ballots, with BMDs for accessibility
- Hand marked paper ballots, with DREs with VVPAT for accessibility
- Hand marked paper ballots, with DREs without VVPAT for accessibility
- Ballot Marking Devices for all voters
- Hybrid BMD/Tabulator
- DREs with VVPAT for all voters
- DREs without VVPAT for all voters

VerifiedVoting

Graphic: https://verifiedvoting.org/verifier/

Hand Marked Paper Ballots

70.4%

Percentage of registered voters living in jurisdictions using Hand Marked Paper Ballots for most voters

Ballot Marking Devices (BMDs)

0.7%

Percentage of registered voters living in jurisdictions using Ballot Marking Devices for all voters

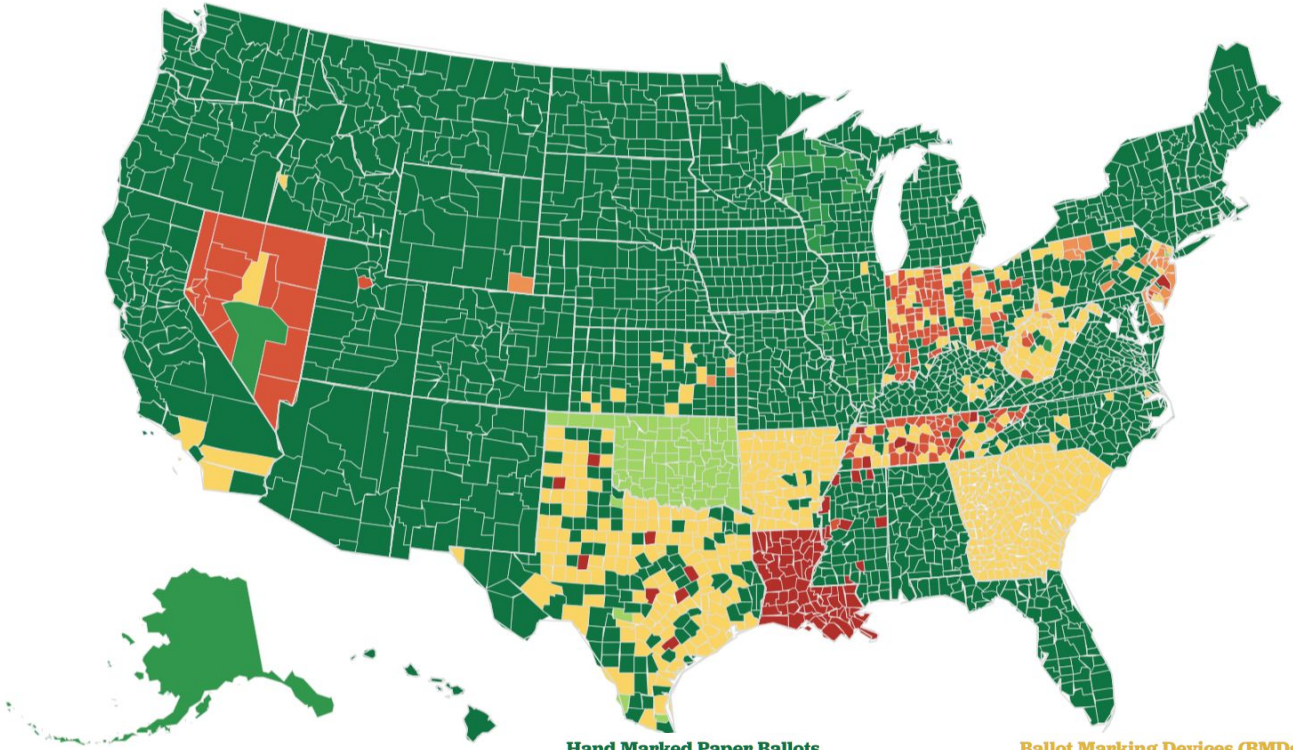
Direct Recording Electronic (DRE) Systems

28.9%

Percentage of registered voters living in jurisdictions using Direct Recording Electronic (DRE) Systems for all voters

Election Equipment Today

just one state fully paperless



Polling Place Equipment
November 2023

- Hand marked paper ballots, with BMDs for accessibility
- Hand marked paper ballots, with DREs with VVPAT for accessibility
- Hand marked paper ballots, with DREs without VVPAT for accessibility
- Ballot Marking Devices for all voters
- Hybrid BMD/Tabulator
- DREs with VVPAT for all voters
- DREs without VVPAT for all voters

VerifiedVoting

Graphic: https://verifiedvoting.org/verifier/

Hand Marked Paper Ballots

69.2%

Percentage of registered voters living in jurisdictions using Hand Marked Paper Ballots for most voters

Ballot Marking Devices (BMDs)

25.5%

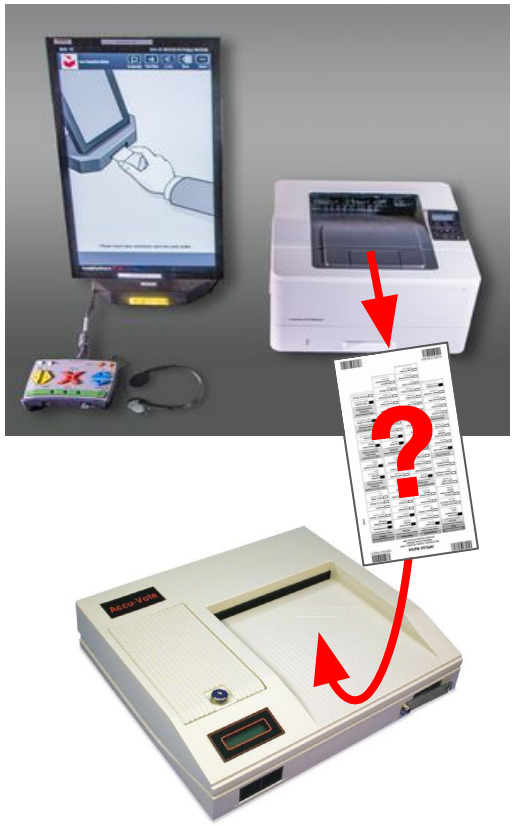
Percentage of registered voters living in jurisdictions using Ballot Marking Devices for all voters

Direct Recording Electronic (DRE) Systems

5.2%

Percentage of registered voters living in jurisdictions using Direct Recording Electronic (DRE) Systems for all voters

Universal-Use Ballot Marking Devices



22% of voters live in places that use BMDs for all in-person voting

Threat: Hacked BMDs can change close election outcomes, because many voters don't check the printouts

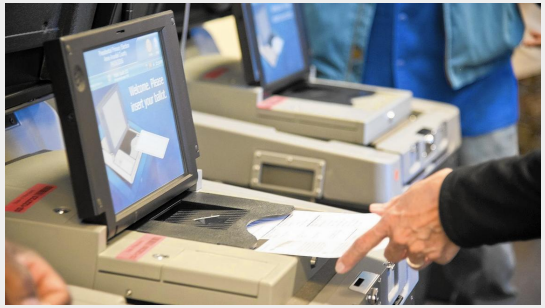
In a mock election we conducted, **voters reported <7% of errors.**

- In election with 0.5% margin, hacked BMDs could change outcome while resulting in only 1 problem report per 5000 voters
- **Steps to encourage verification can help, but not enough?**
  If officials investigate when problem reports exceed 1% of voters, need voters to report >80% of errors to spot outcome-changing fraud
- **Using BMDs exclusively for accessibility is much safer**
  If only 1.8% of voters use BMDs, need just 6.7% detection

"Can Voters Detect Malicious Manipulation of Ballot Marking Devices?"
Bernhard, McDonald, Meng, Hwa, Bajaj, Chang, and Halderman (*Oakland 2020*)

How We're Doing in Michigan

Paper Ballots? Yes

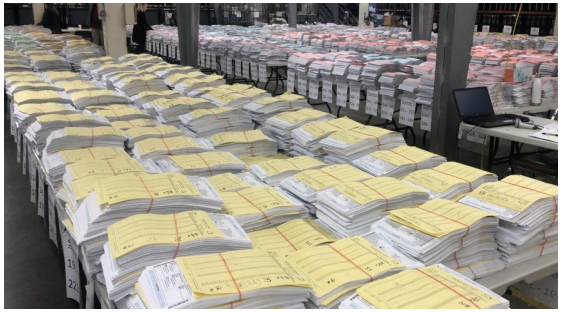


Michigan uses paper ballots statewide

Every vote in Michigan is cast on a piece of paper

Vast majority of ballots are marked by hand

Robust Audits? Pilot



Michigan has been **piloting RLAs since 2018**, as recommended by the state's Election Security Advisory Commission

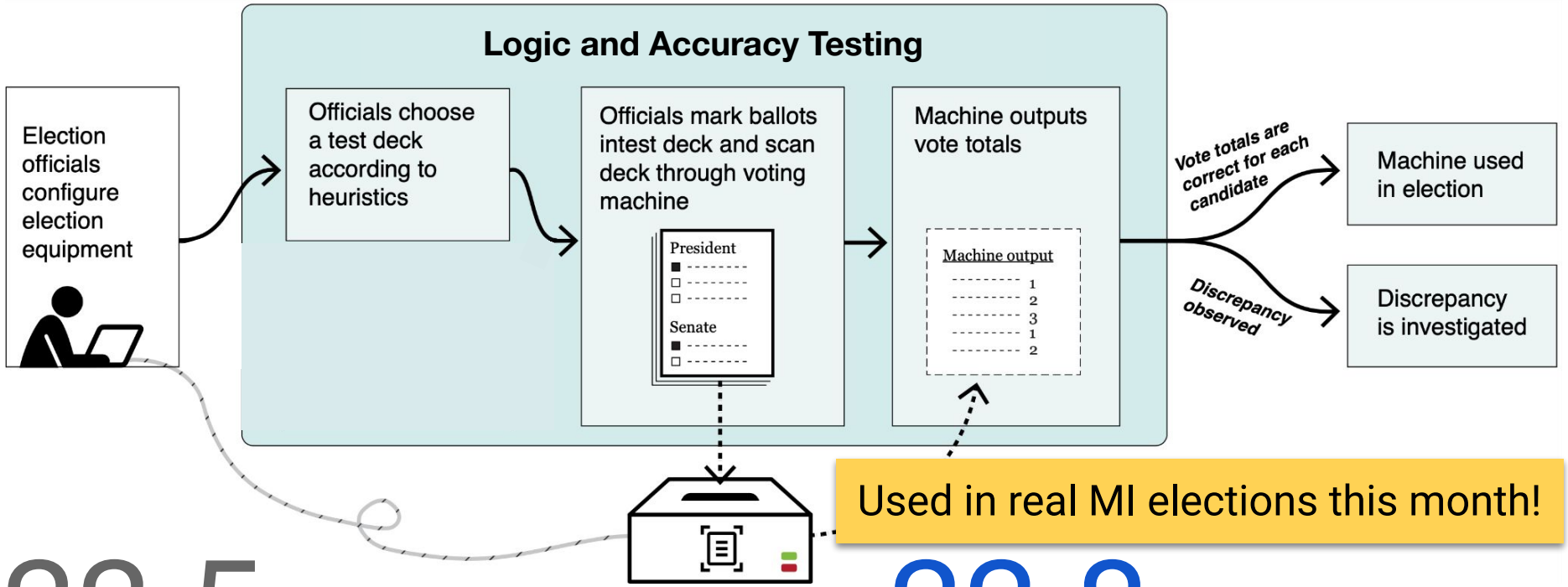
RLAs not completed until after certification, don't affect results

Overall Grade

B+

Should mandate pre-certification RLAs for major contests

Preventing Simple Attacks with Pre-election Testing



Used in real MI elections this month!

22.5 **Current MI Procedure:** Detects swaps **within** contests

22.8 **Robust L&A:** Detects swaps **within** and **across** contests

How many test ballots do officials need?

"Improving the Security of Elections with Robust Optimization"
Crimmins, Halderman, and Sturt, *Operations Research,* to appear 2024

Challenge: Defending Election Legitimacy

Achieving **integrity** is not sufficient

Elections have to convince supporters of *losing* candidates that they *lost*.

Even absent an attack, failures can create appearance of impropriety, undermine trust

Engineer election systems to **generate evidence of correctness** through transparency, observability, etc.

Election Security: A complex problem we can solve

Future elections face risks from *both* **real attacks** and **false accusations of fraud**

Evidence-based methods can show election outcomes are *correct*, not merely that there's "no evidence" they're fraudulent.

Key reforms:

- Make attacks more difficult: **Apply security testing and best practices**
- Ensure attacks are detectable: **Use hand-marked ballots for voters who can**
- Use the paper trail as a defense: **Run risk-limiting audits for every major contest**

What You Can Do

As a computer scientist:

- Accurately explain election security threats and counter disinformation
- Build technology to help make voting on paper easier and more efficient
- Engage with election officials and offer technical expertise

As a citizen:

- Volunteer as a poll worker. Get involved with local election integrity groups
- Urge officials to implement paper and risk-limiting audits
- Ask states and Congress to pass effective election security legislation
- Learn more! Sign up for **Securing Digital Democracy** on Coursera
- Most of all (if you're eligible), ***Vote!***

Coming Up

Reminders:

AppSec Project due next week, November 14 at 6 p.m.

Thursday

Programmable in-network security

Programmable networks, in-network defenses

Tuesday

Censorship

Guest Lecture by Prof. Roya Ensafi