Why Election Security Matters

Carsten Schürmann

IT University of Copenhagen
DemTech
carsten@demtech.dk

September 6, 2017
The Use of Voting Technologies in Elections
DREs (no VVPAT): 5 states
Optical Scan/DREs (no VVPAT): 7 states
Optical Scan/DREs (w/wo VVPAT): 3 states
... Voter-verifiable paper audit trail (rest)
Fax Only: 7 states
Email + Fax: 20 states
Internet Portal: 4 states
Hostile and Adversarial Environment
**18 August 2016**

**Alert Number**

T-LD1004-TT

**WE NEED YOUR HELP!**

If you find any of these indicators on your networks, or have related information, please contact FBI CYWatch immediately.

Email: cywatch@ic.fbi.gov
Phone: 1-855-292-3937

*Note: By reporting any related information to FBI CyWatch, you are assisting in sharing information that allows the FBI to track malicious actors and coordinate with private industry and the United States Government to prevent future intrusions and attacks.*

In furtherance of public-private partnerships, the FBI routinely advises private industry of various cyber threat indicators observed during the course of our investigations. This data is provided in order to help cyber security professionals and system administrators to guard against the persistent malicious actions of cyber criminals.

This FLASH has been released **TLP: AMBER**: The information in this product is only for members of their own organization and those with DIRECT NEED TO KNOW. This information is NOT to be forwarded on beyond NEED TO KNOW recipients.

**Targeting Activity Against State Board of Election Systems**

**Summary**

The FBI received information of an additional IP address, 5.149.249.172, which
**Nation States**

- Very capable intelligence services
- Often driven by geo-political motives

**Example from the 2016 US election**

- Registration systems in
- Suspected Nation State: Russia

**Sources:**

- U.S. Homeland Security
- National Intelligence
- Companies: CloudStrike
Nation States

▶ Very capable intelligence services
▶ Often driven by geo-political motives

Example from the 2016 US election

▶ Registration systems in
▶ Suspected Nation State: Russia

Sources:

▶ U.S. Homeland Security
▶ National Intelligence
▶ Companies: CloudStrike
Honest but Curious Insider

Who: Polling stations workers, Observers, Volunteers
What: System configuration, access to hardware, access to databases.

Example: Volusia County, Precinct 216
- Presidential election 2000
- Diebold voting machine recorded “minus” 16022 votes for Gore

[https://blackboxvoting.org]
Honest but Curious Insider

Who: Polling stations workers, Observers, Volunteers
What: System configuration, access to hardware, access to databases.

Example: Volusia County, Precinct 216
- Presidential election 2000
- Diebold voting machine recorded “minus” 16022 votes for Gore

[https://blackboxvoting.org]
Advanced Voting Solutions WinVote2000
HACKING THE WINVOTE 2000

DEMTECH RESEARCH PROJECT
Greetings from the Defcon voting village where it took 1:40 for Carsten Schurmann to get remote access to this WinVote machine.
Confidence and Control
The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.
The Legal Framework

- What constitutes a vote?
- How to guarantee transparency?
- How to guarantee a trustable election result?
Accountability

The Legal Framework

- What constitutes a vote?
- How to guarantee transparency?
- How to guarantee a trustable election result?

The Technical Framework

- Voter registration [3-6 months before]
- Advanced voting, collecting vote abroad [1 month before]
- DRE machines, paper trails, curation [Election day]
- Vote tabulation [Election Day]
- Election auditing [Days after]
The Thirst for Internet Voting

Reasons

- Vote abroad
- Postal services
- Geographic challenges
- Mobile phone coverage
- Why not?

New Technology New Challenges

- Receipt freeness?
- Coercion resistance?
- Evidence production?
Eos - A Coercion Resistant Voting Protocol
Eos - Idea

- Conditionally Linkable Ring Signatures
- Multiple Pseudo-Identities
  - green envelopes
  - red envelopes
- Two Mixing Phases
  1. Parallel Mix: Identity Confidentiality
  2. Regular Mix: Ballot Secrecy
     [Sako Killian’95, Wikström’11, ...]
- Zero-Knowledge Proofs of Knowledge
  [Patachi + CS:EOS - a coercion-resistant voting protocol, E-VoteID 2017]
Eos - In Action

Public Bulletin Board

Parallel Mixing

Mixing

Tallying Phase

Ballot Verification Phase

Voting Phase

 alice

 bob

 0110...
Eos - Properties

- Individual Verifiability: Public bulletin boards
- Universal Verifiability: ZKPKs
- Secrecy: Crypto system
- Receipt-freeness: Two mixing phases
- Coercion-resistance: Pseudo-identity selection mechanism
Some Thoughts about Block-Chain Voting
Block The Vote: Could Blockchain Technology Cybersecure Elections?

**Capital Flows, CONTRIBUTOR**

Guest commentary curated by Forbes Opinion. Avik Ray, Opinion Editor. FULL BIO

Opinions expressed by Forbes Contributors are their own.

**GUEST POST WRITTEN BY**

Jackie Burns Koven

Ms. Burns Koven is a Research Assistant of Technology & Public Policy at Columbia’s School of International and Public Affairs.

A voter casts his primary vote on Aug. 30, 2016, at Precinct 33, in Hialeah, Fla. (AP Photo/Alan Diaz)

With accusations of election rigging and an unprecedented hack of a political party’s emails, voting security has not been this hot of an issue since Bush v. Gore and the Florida recount of 2000.

**How Blockchain Will Disrupt Our Election System**

**IN BRIEF**

- During this time of unprecedented talk of election rigging, Blockchain could prove to be a completely transparent and secure way to vote.
- The disrupting power of the Blockchain is not just limited to voting, it also has the potential of making government more transparent and accountable for corruption.

The presidential election of 2016 is a watershed event in American and global politics. This is true for a number of reasons. What interests me most as a technologist working with blockchain, especially Ethereum, is the mounting evidence we’ve seen through its lens that the world is becoming increasingly decentralized, and that the power of decentralizing technologies to affect current and future political outcomes—and even the internal structuring of nation states—is growing exponentially.

The simplest example is how in the past, presidential candidates came straight from the halls of official authority, where they held titles as governors, senators, congressmen, etc. This year we departed from that model, fielding a candidate more likely to be caught in a government building facing off a lawsuit than writing policy. By tapping into the prevailing disenfranchisement of Main Street, this “populist” candidate was actually able to participate in the finish line to the finish line.
What is it?

- Gigantic whiteboard in the sky
- Permanent markers only
Block Chain Technology

What is it?
- Gigantic whiteboard in the sky
- Permanent markers only

How is it implemented?
- Peer-to-peer consensus protocol
- Chain of blocks containing transaction information
- Public key cryptography provides identity
- Limited supply of blocks
- Smart contracts
Preliminary Evaluation of Block Chain Technology for Voting

- Verifiable bulletin board!
- Centralization vs. decentralization?
- Identity management?
- Timeliness?
- Eligibility verifiability?
- Secrecy of the vote?
- Universal Verifiability?
- Dispute Resolution?
- Coercion-resistance?
- Receipt-freeness?
- Accountability?
Resolve, To Study Using Blockchain Technology in Conjunction with Paper Ballots in Maine Elections

Emergency preamble. Whereas, acts and resolves of the Legislature do not become effective until 90 days after adjournment unless enacted as emergencies; and

Whereas, this resolve establishes the Commission to Study Using Blockchain Technology in Conjunction with Paper Ballots in Maine Elections; and

Whereas, the study must be initiated before the 90-day period expires in order that the study may be completed and a report submitted in time for submission to the next legislative session; and
Conclusions
Challenge #1
Election Security is necessary to build and preserve TRUST and LEGITIMACY.
  ▶ Challenge: Secrecy and integrity must coexist!
  ▶ Setting: high risk and high value!

Challenge #2
Internet and blockchain elections make Election Security and good legislation really difficult. Election Security must be broadened to include verifiability, accountability, trustability!

Open Question
How can we conduct a meaningful audit of an internet/block-chain election to increase trust?
Thank You!
Risk-Limiting Audits
Denmark National Referendum 2015

This referendum was on whether to convert Denmark’s current full opt-out on home and justice matters into an opt-out with case-by-case opt-in similar to that currently held by Ireland and the United Kingdom. Approval of the referendum was needed for Denmark to remain in Europol under the new rules.

[Wiki Page]
Denmark National Referendum 2015: Results

YES 1.375.862 46,9%
NO 1.558.437 53,1%

Total number of valid votes 2.934.299
Blank votes 48.216
Other invalid votes 7.746
Total number of invalid votes 55.962
Total number of votes 2.990.261

Eligible to vote: 4.153.041
Voter participation: 72%
Building Confidence in an Election Outcome

“Risk-limiting audits provide statistical assurance that election outcomes are correct by manually examining portions of the audit trail — paper ballots or voter-verifiable paper records.”

[Stark ’12]

**Risk-Limiting Audits**

- Statistical Theory
- Validates published election result against paper trail
- Designed to detect election fraud and human error
- Draws a random sample
- Worst case: Triggers a full manual count.
- Can be repeated if necessary

[CS. A Risk-Limiting Audit For Denmark, E-VotelD’16]
1: function DRAW(string e; int k; int n)
2:     i = 1
3:     bs = {}
4:     while i ≤ k do do
5:         x = e + "," + intToString(i)
6:         y = sha256(x)
7:         z = decimal(y)
8:         b = z mod (n − 1)
9:         bs = bs ∪ {b}
10:     end while
11:     return(bs)
12: end function
Doing the Comparison Risk-Limiting Audit