Research Note

Operational Risk Challenges to the U.S. Election Infrastructure

Jeff Leonard

Published: September 2018
Written: May 2018

Keywords: elections, democracy, election fraud,

Abstract: This paper discusses the risks to the most recently identified critical infrastructure sector, election infrastructure (the facilities, technologies, people, processes, political parties, and legal frameworks required to conduct elections). This paper examines the risks, and identifies a system design, the technologies, and an operational architecture that would mitigates the risks to which modern election processes are currently exposed.

Introduction

In 2001, after butterfly ballots, pregnant and hanging chads, the "Brooks Brothers riot"[1] and a five to four Supreme Court decision, awarding George W. Bush the presidency, the U.S. population at large became aware, as never before, of the imperfect technology used in its voting infrastructure.[2] And in 2002, the Help America Vote Act (HAVA) was passed which mandated improving voting systems and addressed issues with voter access that were identified following the 2000 election.[3] At that, time the state of the art was first generation hand marked optical scan systems, but the more typical systems were lever action hole punch systems, while many smaller locales still used hand processed paper ballots. During the last eighteen years, new technologies have been created and deployed that were ostensibly intended to address the deficiencies of the old systems that were problematic during the 2000 election. Yet arguably, from a risk perspective, the U.S. election infrastructure is in a worse place than it was before the turn of the century. While new technologies addressed deficiencies such as confusing placement of candidate names and eliminated the potential of "pregnant" or "hanging chads," they introduced much greater systemic risks from lack of auditability and the potential for undetectable widespread manipulation of the results. Those old paper based systems are, from an operational risk point of view, superior in many ways to the electronic systems that replaced them in the aftermath of the election. They generated paper artifacts that allowed for independent audits. They had reasonable error rates. They were not susceptible to large-scale manipulation. However, as we saw in the 2000 election, they have their own drawbacks and those error rates were large enough to make a difference in a close race.

What is Critical Election Infrastructure?

When considering the risks related to the voting systems, it is necessary to examine the environment in which they operate. Today, critical infrastructure is defined by Presidential Policy Directive 21, which recognizes 16 critical infrastructure sectors.[4] If this paper had been written just 18 months earlier, election infrastructure would not have been considered critical infrastructure.

> "On January 6, 2017 DHS Secretary Jeh Johnson designated U.S. election systems as part of the nation's critical infrastructure… Critical infrastructure is a DHS designation established by the Patriot Act and given to systems and assets whether physical or virtual, so vital to the United States that the incapacity or

> destruction of such systems and assets would have a debilitating impact on the security, national economic security, national public health or safety, or any combination of those matters."[5]

In this context, critical election infrastructure is defined as the facilities, technologies, people, processes, political parties, and legal frameworks required to conduct elections. More specifically, these are polling centers (schools, fire stations, city halls, shopping centers, malls and other places where people vote), tabulation centers where ballots are collected and counted, storage locations where equipment is stored between elections, data centers where results are stored or processed, post offices where mail-in and absentee ballots are transmitted. Technologies including voting machines, communication networks, voter registration databases, result-tabulation systems, paper ballots used for mail-in and absentee voting, and electronic systems.

After the Bush v. Gore decision, many states opted to update their voting rights laws at the same time the Help America Vote Act was being legislated. Many of these states issued Requests for Comments (RFC) on the topic of how to prevent another Bush v Gore from occurring and recommendations going forward. Though not a California resident, I submitted a comment[i] to the State of California RFC pursuant to their revised voting rights act of 2001.[6] In that letter, I laid out a systems design, technologies, and an operational architecture that would impart desirable properties to the election processes. Systems built according to my recommendations would produce a transparent, tamper evident and auditable election infrastructure. Such a system could not be tampered with without producing tangible evidence of the tampering. It could be trusted by voters to produce measurable and accurate results; the accuracy of the results could be verified by both the voter and by audits. If the system failed it would fail in a predictable and visible way. These suggestions are still timely and will be revisited in greater-detail and updated when discussing recommendations going forward. I believe, but I am not positive that my comment to the state of California predates the "Computer Technologists' Statement on Internet Voting,"[7] which is undated but appears to have been published in 2004 at the earliest and from which I will subsequently quote profusely. The signatories are all share tremendous expertise on the subject.

The Election Assistance Commission (EAC) was created in 2005 under the auspices of the Help America Vote Act of 2002 but was not brought under the umbrella of DHS until the January 6, 2017 declaration by Jeh Johnson.

HAVA and the New Types of Voting Equipment

HAVA mandated replacing outdated election technology like lever-action systems and punched-card-based technology and so a new generation of voting equipment was manufactured in the early 2000s. These new systems can be classified into three general categories. Optical scanning devices, Ballot marking devices and Direct Recording Electronic devices.

"Optical or Digital Scanning devices are systems that tabulate paper ballots. Ballots are marked by the voter, and may either be scanned on precinct-based optical scan systems in the polling place or collected in a ballot box to be scanned at a central location."[8] These systems have the risk mitigating benefits of producing an auditable paper artifact and depending on the polling station, the voter may be able to scan the ballot before submission to ensure it reflects the correct intent. This type of system also allows for deduction of voter intent during recounts and audits.

A Direct Recording Electronic (DRE) voting system is a:

> "Voting machine that is designed to allow a direct vote on the machine by the manual touch of a screen, monitor, wheel, or other device. A DRE records the individual votes and vote totals directly into computer memory and does not use a paper ballot. Some DREs come with a Voter-Verified Paper Audit Trail, a

[i] I lived in northern Virginia, in what are considered suburbs of Washington, DC, a place hostile to HAVA. Unfortunately, I no longer have access to this White Paper; it is on a hard drive in an old dead computer system.

> permanent paper record showing all votes cast by the elector. Voters who use DRE voting machines with paper trails have the opportunity to review a paper record of their vote before casting it."[9]

These systems are not auditable in any meaningful way unless they have an option of producing a paper trail at the kiosk so the voter can verify intent. However, this paper trail is, in my opinion, insufficient to verify that the correct vote is ultimately tabulated. I rate these as the riskiest systems to use. With no paper trail, the voter cannot verify the vote was recorded correctly. There is no artifact from which to deduce voter intent or to audit. A precinct's results may not be auditable at all. Diebold Systems of this type used in the 2004 election stored data in an unencrypted database and their laughable idea of auditability was reprinting a report of what was stored in the database. One of these systems was hacked as a demo during a recent DefCon.[10]

A Ballot Marking Device (BMD) is a technology that marks a paper ballot for the voter:

> "A voter's choices are usually presented on a screen in a similar manner to a DRE, or perhaps on a tablet. However, a BMD does not record the voter's choices into its memory. Instead, it allows the voter to mark the choices on-screen and, when the voter is done, prints the ballot selections. The resulting printed-paper ballot is then either hand counted or counted using an optical scan machine. BMDs are useful for people with disabilities, but can be used by any voter. Some systems produced printouts with bar codes or QR codes instead of a traditional paper ballot. Security experts have pointed out that there are risks associated[11] with these types of systems since the bar code itself is not human readable."

In my opinion, these are the best systems from a risk mitigation point of view as long as the marked ballot is user readable. They are auditable, voter verifiable and the voter intent can be deduced from the ballots. Additionally, these systems have the potential to allow for voter audits that verify how their vote was counted.

Finally yet importantly are the mail-in paper and absentee ballots. These ballots are user marked and delivered via the postal service. They are difficult to tamper with at scale but they are susceptible to interception in transit (especially for foreign cast ballots). Paper ballots allow for deduction of intent as well as auditability. They are also user verifiable but not third party verified.

Risks, Themes and Challenges

All electronic systems are vulnerable to being hacked, potentially allowing for misrepresentation of votes at a massive scale. However, systems following the recommendations in the letter, "Computer Technologists' Statement on Internet Voting"[12] can mitigate this risk to great extent through implementing systems with the properties described. These include producing auditable artifacts. Their audit trails must be reliable, strongly unforgeable, and unchangeable. The system must be resilient to disruption at scale. Votes must be recorded with integrity and in a non-repudiable way. The entire system must be reliable and verifiable. Vulnerabilities inherent to particular voting systems (paper ballots, mail-in ballots, absentee ballots, scanning based systems, electronic systems) make this difficult if not impossible. In particular, DRE systems with no paper trail are completely vulnerable to undetectable electronic manipulation by both insiders and third parties. However, vote by mail and absentee ballots have their own drawbacks, possibility of interception, voter coercion, and bias introduced variations in the quality and timeliness of mail delivery being foremost among them.

Risks from technology are not the only risks to the voting systems. There are also risks from political interference. Politicians pass laws to disadvantage classes of voter like students and minorities.[13] Election officials shut down polling places before everyone in line has voted. Legislatures create obstacles to registration; disenfranchise classes of citizens such as convicted felons and Census reapportionments can be gerrymandered to render votes irrelevant. There are issues of fairness and bias that come from fairness of treatment like treating one area differently to another when the area correlates with a demographic. There are risks from solutions that introduce larger risks than the perceived problems they are solving. Like solutions to fraudulent in person voting that prevent more legitimate votes than they prevent fraudulent ones. Not to mention how ties are handled.

- There are risks to disruption of facilities. Polling places are generally government or civic facilities like schools, fire houses, libraries, city halls, churches, court houses that can be soft targets vulnerable to attack.
- There are risks from illegal behavior. Poll taxes, knowledge tests, intimidation, and dissemination of false information such as was prevalent during Jim Crow fall into this category.
- There are risks inherent in a constitutional system that does not weigh votes equally, of which the U.S. Electoral College system is an example. In three of the last five elections, the candidate with the most votes did not win.
- There are risks from foreign interference. Foreign governments have used big data to run micro-targeted PR campaigns seeking to influence populations. State sponsored entities have executed large-scale attacks on election systems. Both foreign and domestic entities have funded candidates in order to disrupt local elections.[14]

Current Mitigations

The biggest operational mitigation of the risk of widespread manipulation is the decentralized nature of the U.S. voting system. It is comprised of 527 independent voting districts that compartmentalizes the risk into 527 chunks that must be manipulated separately. However, each district has its own unique risks. The next big operational mitigation is the diversity of systems and control. Five companies produce the certified voting systems in use today.

The U.S. Department of Homeland Security (DHS) Government Facilities Sector-Specific Plan[15] lays out guidelines for understanding and mitigating risks to facilities. It also specifies a COSO-like Governance, Risk and Compliance (GRC) process for monitoring operational risks. This is based on industry best practices (though the G, R and C are voluntary). The EAC certifies voting machine integrity, maintains a glossary of critical infrastructure.[ii] EAC can assist state and local government in performing Gap Analysis, implementing best practices and can run tabletop exercises to help train personnel. EAC maintains voluntary processes for evaluating processes and systems, maintains an internal task force with the capacity to perform cybersecurity Assessments and provide Cyber Emergency Response Team services. Finally, EAC has the authority to grant secret clearance to state and local election officials so the can receive classified cyber threat briefings. Note that this is by no means a complete detailing of their capabilities.

Recommendations

- *Add Election Infrastructure as a 17th DHS Critical Infrastructure Sector*. The fact that Election Infrastructure was designated in January 2017 as critical infrastructure under the government facilities sector is a good start but the election infrastructure is so cross-sector and deals with so much more than just facilities that it merits designation as a sector in its own right. It is also worth noting that this designation occurred during the transition period. It was not widely publicized, and it is unknown what level of support it has within the current administration. Given the current administration's propensity to undo everything accomplished by the previous administration, it is an open question whether even the current designation will survive to the next presidential election.
- *States and localities should implement the Government Facilities sector specific plan as appropriate*. In particular, storage facilities, information systems, and communication networks should be fortified and

[ii] Or at least it says it does, I was unable to track it down.

made resilient in the face of disruption.

- *States and localities should also implement a COSO-like framework for managing risk.*[16] In general, the sector specific plan recommends best practices that are harmonious with COSO and GRC (although the C is voluntary).
- *Increase the diversity of certified systems across all voting districts.* Only five companies currently produce all of the certified machines. A more diverse set of compliant products will increase the resiliency of the electoral systems overall.
- *Decertify the DRE type systems.* These systems do not implement two of the most important properties in the "Computer Technologists' Statement on Internet Voting,"[17] verifiable accuracy and resistance to large-scale disruption. DRE systems are used in about twenty percent of the systems certified by the EAC and in five percent of districts overall (counting mail-in states and non-certified states).
- *Implement dedicated infrastructure to minimize attack surface and protect data in transit.*[18] Election infrastructure must be capable of undergoing independent validation and verification and audits of all hardware and software. These requirements put it above the level of the public infrastructure upon which it currently relies.
- *Investigate the use of block chain as a way to implement a robust audit trail of system activity.* That being reliable, unforgeable, unchangeable voter-verified records. Votes need provenance proving the path they took from the voter to tabulator, to compilation to announcement of results. This is almost a canonical problem solved by the block chain ledger.[19]
- *Investigate e-coins as means of implementing voter audits of their own votes.* The coin plus the provenance should be sufficient to prove the vote was tabulated as cast.
- Finally, *implement Trustworthy Voting System Guidelines*, which is a superset of the guidelines in "Computer Technologists' Statement on Internet Voting."[20] Namely, voters should be authenticated. Votes should be accurately recorded and non-repudiable. Votes should be verifiable by both the voter and an auditor. Privacy of the voter should be protected in that user identifiable data should not be captured in the voting process. Additionally, there should be a stronger guarantee that votes should be confidential. Third parties should not be able to reverse engineer the identity of individual voters. Voters should receive a token after voting that they can use to prove that they voted and that they can use to self-audit and verify that their vote was counted as intended. This could be an e-coin. Systems should produce tangible artifacts with integrity and provenance. This again is could be a canonical implementation of the blockchain ledger. Results should be independently verifiable and auditable from the tangible artifacts.

The voting process should be transparent. There should be no black boxes in any of the operational systems involved in voting. The processes should be capable of undergoing government independent validation and verification audits. Additionally, hardware designs should be public, verifiable, and auditable. Systems and processes should be tamper evident. It must not be possible to tamper with any part of the system without creating evidence of the tampering. For, example ATM machine keypads are internally encrypted and built to self-destruct if taken apart.[21]

Conclusion

Since the passing of HAVA in 2002, voting systems and processes have migrated to IT based systems. These voting systems fall into three categories: optical scanning systems, ballot marking systems and paperless direct recording systems with related back end IT systems. These systems have introduced systemic risks that make them arguably riskier to the integrity of elections than the systems they replaced. The DHS has recently included election infrastructure under government facilities as a critical infrastructure sector. Under this designation, the EAC has developed an organization and standards for protecting and mitigating the risks to the election infrastructure. The EAC needs to use its authority to reduce the risks inherent in the current generation of voting technology. Finally, it is recommended the election infrastructure be promoted out from under government facilities to its own critical infrastructure sector, that state and local governments implement the EAC guidelines and that future systems be developed following a set of recommended principles and in concordance with these principles, direct recording type voting systems be phased out.

[1] Padgett, Tim. "Mob Scene in Miami." *Time Magazine*. 26 Nov. 2000. Accessed May 2018 <www.time.com>.

[2] "Bush v. Gore Law Case" *Encyclopaedia Britannica.* 16 Nov. 2017. Accessed May 2018 <www.britannica.com>.

[3] "Help America Vote Act." U.S. Election Assistance Commission. N.D. Accessed May 2018 <www.eac.gov>.

[4] "Critical Infrastructure Sectors." U.S. Department of Homeland Security. N.D. Accessed May 2018 <www.dhs.gov>.

[5] *Starting Point: U.S. Election Systems as Critical Infrastructure*. U.S. Election Assistance Commission. Jun. 2017. Accessed May 2018 <www.eac.gov>.

[6] "AB-182 California Voting Rights Act of 2001." California Legislative Information. 26 Jan. 2015. Accessed May 2018 <leginfo.legislature.ca.gov>.

[7] "Computer Technologists' Statement on Internet Voting." Verified Voting Foundation, Inc. Sep. 2012. Accessed May 2018 <www.verifiedvoting.org>.

[8] "Types of Voting Equipment." National Conference of State Legislatures. Apr. 2018. Accessed May 2018 <www.ncsl.org>.

[9] *Ibid.*

[10] "How the Vote Hacking Was Done at DefCon25." AlienVault. 1 Aug. 2017. Accessed May 2018 <www.alienvault.com>.

[11] Cohn, Jennifer. "What Is the Latest Threat To Democracy? Bar-Codes and Ballot Marking Devices A.K.A. 'Electronic Pencils.'" *Medium*. 6 Mar. 2018. Accessed May 2018 <www.medium.com>.https://medium.com/@jennycohn1/what-is-the-latest-threat-to-democracy-ballot-marking-devices-a-k-a-electronic-pencils-16bb44917edd

[12] "Computer Technologists' Statement on Internet Voting."

[13] Hasen, Richard L. "Scalia's Goal of Unwinding Voter Protection is Becoming a Reality." *Talking Points Memo*. 2 Apr. 2018. Accessed May 2018 <www.talkingpointsmemo.com>.

[14] Kurtz, David. "Watch This One Very Closely." *Talking Points Memo*. 31 May 2018. Accessed May 2018 <www.talkingpointsmemo.com>.

[15] *Government Facilities Sector-Specific Plan An Annex to the NIPP 2013*. U.S. Department of Homeland Security. 2015. Accessed May 2018 <www.dhs.gov>.

[16] Moeller, Robert R. *COSO Enterprise Risk Management: Understanding the New Integrated ERM Framework*. Wiley. Jul. 2007.

[17] "Computer Technologists' Statement on Internet Voting."

[18] Zetter, Kim. "The Myth of the Hacker-Proof Voting Machine." *The New York Times*. 21 Feb. 2018. Accessed May 2018 <www.nytimes.com>.

[19] Konst, Stefan. "Secure Log Files Based on Cryptographically Concatenated Entries." Institute of Theoretical Computer Science, *Technische Universität Braunschweig*. Aug. 2000. Accessed May 2018 <www.konst.de>.

[20] "Computer Technologists' Statement on Internet Voting."

[21] "ZT595 ATM Keypad, Encrypted Keypad." SZZT Electronics Co. N.D. Accessed May 2018 <www.szztelectronics.com>.