GBBC Open Source Ideas:
'State of Global Voting Systems, Technology, and Government'

Part II: Examining Vulnerabilities of Voting Machines

GBBC
Global Blockchain Business Council

06 May 2020

Washington, D.C.

Introduction

In Part I of the Global Blockchain Business Council's 'Open Source Ideas': State of Global Voting Systems, Technology, and Government, we recommended that the U.S. look to more technologically agile countries that have leveraged innovations to improve the voting process, which we examined in three distinct stages:

1. identity and voter registration;
2. casting votes; and
3. verification, accuracy, and security.

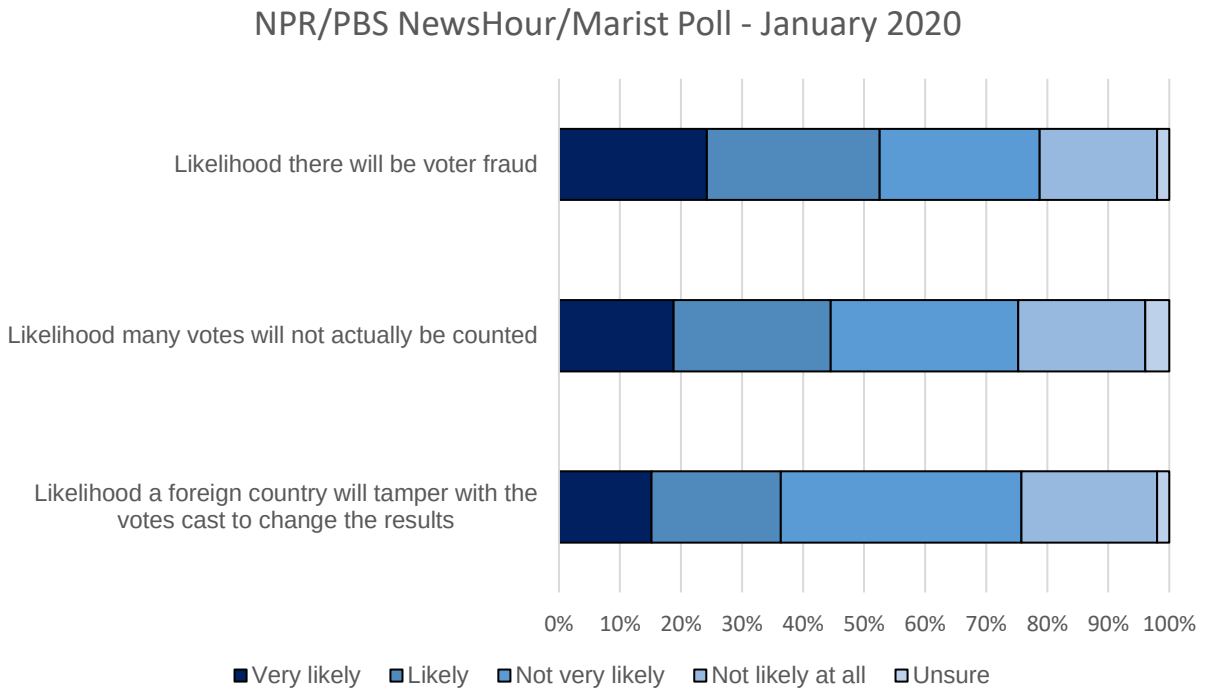
At this point in time, blockchain technology holds the potential to improve the identity and voter registration stage, as there are numerous, relatively straightforward problems associated with traditional voter rolls that the technology could address.

Stages two and three, on the other hand, are far more controversial and are the focus of this Part II report. Most recently, the American Association for the Advancement of Science, as well as the Brennan Center for Justice, Computing Research Association, Verified Voting, and more stakeholders from advocacy groups and academia, wrote a letter to governors, secretaries of state, and state election directors asserting that "Internet voting is not a secure solution for voting in the United States, nor will it be in the foreseeable future. We urge you to refrain from allowing the use of any internet or voting app system." Regarding blockchain technology, they stated that "Blockchain systems do not address the fundamental issues with internet voting. Blockchain-based voting systems introduce additional security vulnerabilities."[i]

However, in the face of the COVID-19 pandemic, some states are turning to online voting, with Delaware allowing those with disabilities to cast an online ballot in its upcoming primary election using Democracy Live's platform; New Jersey is reportedly considering a similar system.[ii]

To dive deeper into verification, accuracy, and security we asked REMTCS Inc. to perform an overview of existing voting machine and software manufacturers and present their thoughts on how these voting machines might help or hinder the voting process. As you will read, many voting machines in the U.S. have security flaws that could be exploited. While these flaws differ, what is true across jurisdictions and machines is that a lack of cybersecurity expertise amongst election officials puts vote security at risk. This holds true across many industries and applications – a 2017 survey of 5,000 businesses around the world found that careless/uninformed staff were a contributing factor in 46 percent of cybersecurity incidents.[iii] Some of the most fundamental security problems related to voting will not be solved until the government prioritizes bringing cybersecurity experts

into the voting process. The time to secure America's elections is now: a January 2020 survey found 41 percent of those surveyed believed the U.S. is not very prepared or not prepared at all to keep the upcoming election safe and secure; 37 percent stated it was likely or very likely that a foreign country would tamper with votes cast to change the results, 44 percent believed it was likely many votes would not be counted, and 52 percent believed it was likely there would be voter fraud.[iv]



Given the ongoing COVID-19 pandemic and uncertainty regarding a return to normality, it is imperative that all potential voting process weaknesses be addressed. Deployed voting systems will likely be stressed by the unusual circumstances -- a lack of experienced personnel, including poll workers and technical support, who have been relied upon in the past to address anomalies, may strain voting systems in the upcoming election. Mail-in voting systems will also be strained, as some states move quickly to expand mail-in while relying on a strained U.S. Postal Service. The GBBC and REMTCS advocate for the federal government to take legislative action to secure this year's elections, and to explore what technological advancements are required to reach the ultimate desired outcome: secure, tamper-proof remote voting that is available to all.

REMTCS Findings of Existing Voting System in USA

REMTCS has researched existing voting platforms, assessed publicly available information, carefully considered potential technical vulnerabilities, and through experience can recommend mitigation strategies for the examined technology. The

vulnerabilities found can be classified into three categories: hardware, software, and communications.

Hardware: Many of the manufacturers that produce hardware-based ballot tabulation and pollbook platforms suffer from similar vulnerabilities. Accessibility of communication ports, removable storage media, unencrypted storage media, and overall lack of physical security over the internal hardware components plague virtually every manufacturer. Hardware should be properly safeguarded from unauthorized physical access using more secure hardware containment, in the form of lockable cases with inaccessible, and potentially, disabled communication ports, as well as inaccessible removable storage media and internal components. Additionally, all storage media (removable or internal) should be encrypted to an acceptable standard of AES256 or better secured utilizing Public Key Infrastructure (PKI) certificates.

Software: Many of the hardware manufacturers also suffer from similar software vulnerabilities in their platforms. Operating systems (OS) are utilized with default settings, and too often user and administrative accounts use weak and/or default passwords, putting them at risk of easily being accessed by unauthorized individuals, and allowing unauthorized software or code to be executed. REMTCS recommends that operating systems be fully patched and hardened to an appropriate industry standard, a strong password policy be enforced on the OS, and application whitelisting be implemented to prevent unauthorized code from being introduced and executed on the system. Hardware systems connected to the internet for remote administration should have software firewalls configured to whitelist communication with only known voting organization and/or vendor networks to prevent potential remote access by unauthorized actors. Additionally, a proper network security stack should be implemented to analyze and protect network traffic to and from the voting machines.

Blockchain should be utilized as the transaction database for voting. Each vote, as well as each inclusion of a vote into the tabulation should be digitally signed, preferably by a quantum-resistant signature to ensure integrity of each transaction, and to provide an audit trail for each vote while demonstrating that each vote was included in the total.

Vendors that produce software or mobile voting platforms also have software vulnerabilities that increase the risk of compromise. Software and mobile apps should follow best security practices in the development process, mitigate currently recognized software vulnerabilities, ensure that user data and other Personally Identifiable Information (PII) is stored in encrypted, protected storage on the device, and that applications and other software check for patch levels of the underlying device.

Communications: REMTCS discourages the use of networked voting machines. However, it is clear that some hardware vendors' models depend on networking for vote tallying, remote administration and support, and more; with that comes many risks.

Additionally, mobile voting apps are predicated on the existence of network connectivity and thus are inherently exposed to the cybersecurity risks of being connected to the internet. REMTCS recommends that PKI device authentication be utilized in all communication between the client and server, Transport Layer Encryption (TLS) be implemented to protect the confidentiality of the communication and prevent man-in-the-middle (MITM) attacks. Additionally, proprietary software and communication protocols should be opened up to security researchers and subject to a bug bounty. Network communications should be analyzed by a robust network security system to detect and mitigate network attacks and malware.

Overview of existing voting machine/software manufacturers

Clear Ballot Group, Inc. is a company based in Boston, MA that manufactures software for the production of ballots (ClearDesign), accessible voting for the disabled (ClearAccess), and auditing (ClearAudit.) They also manufacture machines for the precinct level (ClearCast) and central tabulation of ballots (ClearCount). Publicly available information shows that Clear Ballot's machines utilize encrypted hard drives. However, hardware appears to be commercial off-the-shelf (COTS) hardware that likely lacks any hardening (i.e. reduction of cybersecurity vulnerabilities) of the hardware or OS. Certain products that communicate between scanners and servers do not use encryption for data in transit, nor do they use digital signatures or hashing algorithms to verify integrity of transmitted data.[v]

Dominion Voting Systems Corp. is a company based in Denver, CO that produces several software and hardware products under the ImageCast brand, such as the Precinct tabulator, the Evolution ballot marking device, and the Central count software. Recent testing of the Precinct scanner showed that USB and RJ45 ports and CF card slots are freely accessible and that the machine could be booted off of a USB drive from these ports. The COTS OS contains many medium- and high-level vulnerabilities. Ballot images and device configuration files are stored unencrypted and unsigned on a removable CF card that is easily accessible. The devices file system is also vulnerable to remote modification when connected to a network. Dominion's products also offer remote access for administration, which introduces a slew of attack vectors.[vi]

Election Systems & Software (ES&S) is a company based in Omaha, NE that manufactures many hardware-based ballot tabulators and pollbooks, as well as software election management systems. Many of ES&S' machines utilize COTS hardware and operating systems. These hardware platforms do not utilize any hardening or security measures, and the operating systems are not hardened or patched. USB, SD card, and other ports are all accessible and have been shown to be active and allow booting from media. File systems are unencrypted and default passwords are weak and stored unencrypted, leaving voting data and configurations vulnerable to exploitation. In some

cases, third party software such as Netflix, Hulu, Internet Explorer, etc. was still installed and exploitable. ES&S' products also offer remote access for administration, which again introduces a variety of attack vectors.[vii]

Hart Intercivic, Inc. is a company based in Austin, TX that produces a wide array of software and hardware voting systems, including ballot scanning, ballot marking, and ballot printing machines. The Hart machines are known to lack data integrity measures, such as digital signatures, allowing manipulation of data. Election data is stored in an unencrypted database on an unencrypted PCMCIA card, and using basic UNIX commands can be viewed, manipulated, or erased.[viii]

Microvote General Corp. is a company based in Indianapolis, IN that manufactures hardware-based paperless and paper ballot counting machines. Paperless ballot machines are inherently insecure, as they are unable to be verified against paper ballots. The Microvote Infinity is known to have exposed and exploitable USB and RJ45 communications ports. Voter data is stored in a proprietary database on an unencrypted CF card.[ix]

Open Source Election Technology (OSET) Institute is a nonpartisan, nonprofit research foundation based in Palo Alto, CA whose goal is to produce an open source, highly secure election technology platform for the purpose of "preserving the operational continuity of democracy." OSET has developed a framework for public election technology called ElectOS that is available for any entity to utilize.[x]

Smartmatic USA Corp. is a company based in Boca Raton, FL that produces software for election management, remote voting, and central counting, as well as machines for electronic pollbook, ballot marking devices, and tabulators. The company was founded with a grant and subsequent contracts from the Venezuelan government and has been the subject of multiple Committee on Foreign Investment in the United States (CFIUS) investigations due to its ties; at one point a Venezuelan government agency owned a 28% equity stake in the firm.[xi] It has been documented that during the 2016 election in the Philippines, Smartmatic was funneling voting data between servers outside the footprint of the Commission on Elections.[xii] Security researchers have found that Smartmatic systems' "seals, locks, labels, and sensors can all be bypassed" and that accessible USB ports allow unrestricted access to and the ability to boot the underlying computer hardware.[xiii]

Scytl is a company based in Tampa, FL that produces software for online voting. The software is currently in use in Switzerland and NSW Australia. It has been found that when votes are decrypted, verification can be faked, passing fraudulent votes to the back-end system. Another flaw was found in their software that could be used to prove an election outcome that had been manipulated.[xiv]

Unisyn Voting Solutions is a company based in Vista, CA that manufactures software for central tabulation and hardware systems for optical ballot scanning and tabulation, and tablet voting for people with disabilities, all under the brand OpenElect. It is known that the precinct components communicate with a central server, from where election configurations, passwords, parameters, and ballots are sent to the precinct. While it is likely encrypted communication, systems can also transfer voting data via USB port, which likely has many of the same vulnerabilities as other systems with active USB ports.[xv]

Votem Corp. is a company based in Cleveland, OH that produces an online voting registration and mobile voting platform based on blockchain and a proprietary Proof of Vote protocol, which is publicly reviewable on Github.[xvi] At this point it is apparent that there are known vulnerabilities for the Votem platform.

Voatz is a company based in Boston, MA that makes an online, mobile voting application. While Voatz claims to use blockchain, end to end encryption, voter anonymity, and a verified audit trail, it has recently been discovered that some of these features can be bypassed or compromised. Researchers found that "an attacker with root privileges on the device can disable all of Voatz's host-based protections."[xvii] There appears to be no public key authentication as part of the device handshake with the server, thus there is no verification of the device. This exposes the possibility of an MITM attack to intercept data. There is no method of verifying that the ballot was counted in the blockchain. The Voatz app also appears to expose the user's IP address, which has significant anonymity implications. Additionally, at least on Android devices, the user's PIN and other login information are not stored in protected storage and are stored in the app's memory; a remote attacker could steal this data and impersonate a voter.

Appendix A delineates which states are using which providers of voting machines and technology, based on information from Verified Voting.

Conclusion

Americans' faith in the country's voting system has been wavering, tested by foreign interference, malfunctions, and, most recently, the COVID-19 pandemic. Since 2016, little progress has been made to secure U.S. elections, and the 2020 primary season was kicked off by the now-infamous Iowa caucus and followed by more problems. Wisconsin was forced to rapidly expand its vote-by-mail operation after a Supreme Court decision blocked extended absentee voting proposed due to the coronavirus. As a result, at least "9,000 absentee ballots requested by voters were never sent, and others recorded as sent were never received. Even when voters did return their completed ballots in the mail, thousands were postmarked too late to count — or not at all."[xviii]

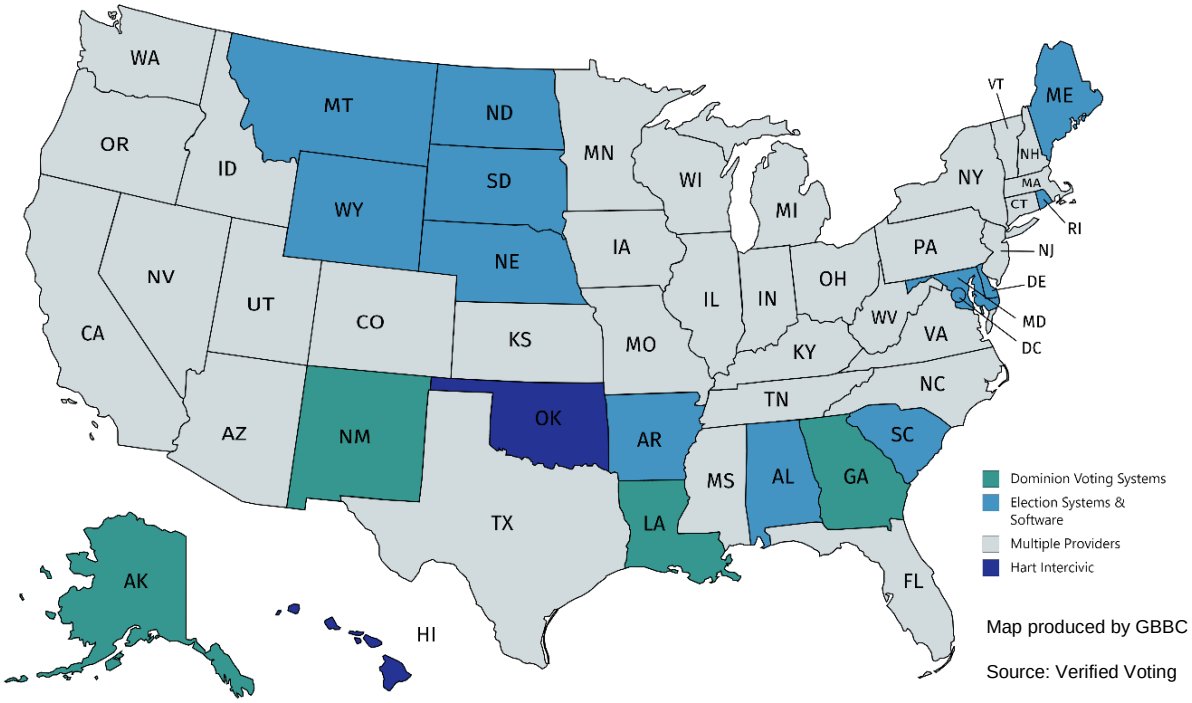
While many are skeptical of the security of voting by mail, and many are even more skeptical of remote voting, as REMTCS' team has elucidated, traditional voting machines may also have significant security flaws that cannot be ignored. Furthermore, relying primarily on physical voting machines could have serious consequences: in Wisconsin, state health officials have discovered at least 40 people who voted in-person or worked at a polling site and subsequently tested positive for COVID-19.[xix] It is necessary for the government to explore all possible options to enhance the security of voting systems and protect the health of all Americans.

Looking ahead to Part III, GBBC and its partners will map out a possible next-generation voting system from Stages One through Three by taking a security and risk-mitigation based approach, balanced with real world needs to provide a robust and inclusive voting system which upholds and defends the democracy citizens want. If you have any questions or comments, or would like to discuss collaborating on Part III, please email ideas@gbbcouncil.org.

The analysis of the above voting machine manufacturers was performed by REMTCS' team of Cyber Security Experts who utilized not only their years of experience but also the proprietary AI-based security tools developed by REMTCS to detect cyberattacks and determine the vulnerability of software, networks and enterprise systems.

Appendix A

State-by-State Map of Voting Machine / Technology Providers*



*Based on publicly available information

[i] https://www.aaas.org/sites/default/files/2020-04/AAAS%20EPI%20Center%20group%20letters%20on%20internet%20voting_0.pdf
[ii] https://www.npr.org/2020/04/28/844581667/states-expand-internet-voting-experiments-amid-pandemic-raising-security-fears
[iii] https://www.kaspersky.com/blog/the-human-factor-in-it-security/
[iv] https://www.npr.org/2020/01/21/797101409/npr-poll-majority-of-americans-believe-trump-encourages-election-interference
[v] https://www.eac.gov/sites/default/files/eac_assets/1/6/ClearVote_1.4_Certificate_and_Scope_FINAL_2.8.18.pdf
[vi] https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf
[vii] https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf
[viii] https://www.usenix.org/legacy/events/evt08/tech/full_papers/butler/butler_html/index.html
[ix] https://www.verifiedvoting.org/resources/voting-equipment/microvote/infinity/
[x] https://www.osetfoundation.org/
[xi] https://www.nytimes.com/2006/10/29/washington/29ballot.html

[xii] https://www.manilatimes.net/2016/07/22/news/top-stories/smartmatic-admits-using-unofficial-servers/275442/275442/
[xiii] https://votingsystems.cdn.sos.ca.gov/vendors/LAC/vsap2-func.pdf
[xiv] https://people.eng.unimelb.edu.au/vjteague/iVoteDecryptionProofCheat.pdf
[xv] https://www.verifiedvoting.org/resources/voting-equipment/unisyn/openelect/
[xvi] https://github.com/votem
[xvii] https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf
[xviii] https://www.chicagotribune.com/politics/elections/ct-nw-nyt-wisconsin-election-problems-20200410-rdea6424ynecjemkwwfyjqcyqq-story.html
[xix] https://thehill.com/homenews/campaign/494984-health-officials-say-36-coronavirus-cases-possibly-exposed-through