Voting Systems as Mission Critical Systems

Submitted Issues Paper for the National Secretaries of State Summer Conference 2023

By: Julia Berutti, Victor Berutti, and Bruce Holenstein

Studies show that trust in government institutions has a positive correlation with social cohesion, GDP, and overall wellbeing.[1] However, a significant portion of Americans lack faith in the voting process, according to recent polling data.[2] Specifically, they worry that someone might vote more than once or tamper with ballots already cast. They realize that the insider access of election officials creates opportunity for manipulation, and they fear that hackers might interfere with the vote count.[3] In order to help restore trust in the voting process, administrators should strengthen the security of their ballot collection and tabulation process using the principles of mission critical systems. This white paper will describe key principles of mission critical systems and illustrate how they can help election administrators secure ballots, prevent insider manipulation, and stop hackers. By reinforcing perceived vulnerabilities, administrators can effectively conduct elections and restore the trust of worried voters.

What is a Mission Critical System?

In 2017, the Department of Homeland Security officially designated voting systems as part of the nation's critical infrastructure.[4] This designation is reserved for systems "so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[5]

---

1 Organization for Economic Co-operation and Development. "Trust in Government: Assessing the Evidence, Understanding the Policies." 47th Session of the Public Governance Committee. Paris, France: Organization for Economic Co-operation and Development, 2013.

2 Gallup Inc. "Confidence in Election Integrity Hides Deep Partisan Divide." Gallup.com, 2022. https://news.gallup.com/poll/404675/confidence-election-integrity-hides-deep-partisan-divide.aspx .; Ipsos/ABC News. "Ipsos/ABC News Poll (December 27 – December 29, 2021)." Ipsos, 2022. https://www.ipsos.com/sites/default/files/ct/news/documents/2022-01/Topline%20ABC_Ipsos%20Poll%20January%206%202022.pdf .; Murray, Patrick. "National: Public Supports Both Early Voting and Requiring Photo ID to Vote." Monmouth University, 2021. https://www.monmouth.edu/polling-institute/documents/monmouth-poll_us_062121.pdf/.; Pew Research Center. "Two Years After Election Turmoil, GOP Voters Remain Skeptical on Elections, Vote Counts." Pew Research Center, 2022. https://www.pewresearch.org/politics/2022/10/31/views-of-election-administration-and-confidence-in-vote-counts/.; Trafalgar Group. "Nationwide Issues Survey." Trafalgar Group, 2022. https://www.thetrafalgargroup.org/wp-content/uploads/2022/11/COSA-ElectionTrust-Full-Report-1123.pdf.

3 Alvarez, R. Michael, Jian Cao, and Yimeng Li. "Voting Experiences, Perceptions of Fraud, and Voter Confidence." Social Science Quarterly 102, no. 4 (July 2021): 1225–38. https://doi.org/10.1111/ssqu.12940.

4 U.S. Department of Homeland Security. "Election Security." Homeland Security, 2023. https://www.dhs.gov/topics/election-security.

5 Cybersecurity & Infrastructure Security Agency. "Critical Infrastructure Sectors." CISA. Accessed December 31, 2022. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

In the field of computer science, a mission critical system is “a system that is essential to the survival of a business or organization.”[6] Though voting systems are critical infrastructure and certainly fall into this category, the methods used to process votes is less secure than similar mission critical systems in other industries. For example, financial institutions are confident in the security of monetary transactions when their processes follow the three key principles of a mission critical system: **Reliability, Availability, and Scalability (RAS).**

“**Reliability** is a measure of how well a system returns the same correct, consistent, and uncorrupted results each time, and relies on the underlying integrity of the database, application, and system components;

Availability is the percent of uptime achieved by the application in servicing users; and

Scalability is the capability to add resources when needed to handle the application load, and to return those resources when no longer needed.”[7]

Organizations around the world use the principles of mission critical systems every day to protect their data from software bugs, hardware errors, malware, chip-level vulnerabilities and other threats.[8] If this field-tested approach has seen so much success in similar systems, why not apply it to elections?

How Can a Mission Critical System Work for Elections?

An ATM network is an example of a mission critical system. When a customer inserts their card to withdraw funds, the ATM system matches the card to the correct bank account then validates the transaction both locally and in secure central data centers. This process allows financial institutions to approve transactions and keep several copies of records, which help detect hackers and other fraudulent activity. Voting systems can work in a similar fashion, while maintaining the anonymity critical to the voting process.

First, a globally unique identifier (GUID) on each paper ballot could work like an ATM card’s unique number to ensure that each vote cast is counted and legitimate without compromising the secrecy of a voter’s choices. Then, like the ATM’s validation process, paper ballots could be scanned locally, and the images could be uploaded to several redundant data centers via a secure connection. Each data center can then process the ballots and use a **Validation Architecture**[9] to make sure that all counts match between data centers. This way, the ballots would be counted several times, once at each polling place, and once in each data center. Any discrepancy in the counts would trigger an alert to election authorities. The security features that have emerged from mission critical principles can help strengthen the vulnerabilities that are of greatest concern to voters, specifically ballot security, insider manipulation, and hacking.

6 “Mission Critical.” In Wikipedia, June 4, 2023. https://en.wikipedia.org/w/index.php?title=Mission_critical&oldid=1158513696.

7 Holenstein, Bruce, Paul J. Holenstein, and Victor Berutti. “New Data Integrity Architectures for Mission Critical Systems.” The Connection, 2021. https://connect2nonstop.com/new-data-integrity-architectures-for-mission-critical-systems/.

8 Holenstein, Bruce, Paul J. Holenstein, and Bill Highleyman. “A Modern Look at Reliability, Availability, and Scalability – Part 1.” The Connection, 2019. https://connect2nonstop.com/a-modern-look-at-reliability-availability-and-scalability-may-june-2019/.

9 Ibid. 7

GUIDs Make Ballots More Secure

A GUID is an innocuous piece of identifying information, like a barcode or random alphanumeric string, that keeps tabs on all of the ballots in an election. The office in charge of creating the ballot GUIDs for each election, the Secretary of State for instance, could house a Ballot Master Database in a secure data center (or centers). The database would record the GUIDs for every ballot in election, both used and unused. After polls close, election administrators can simply scan any unused or spoiled ballots, so the system can mark them appropriately and ensure they are not counted during tabulation. This would prevent someone from trying to fraudulently submit them into the data stream. Once all of the ballot images are scanned, a secure software at each polling place would send the images and the system would cross reference the GUIDs against the Ballot Master Database to ensure there is no fraudulent activity, such as fake ballots or ballots scanned multiple times. Because the GUIDs would not contain any information that could be used to identify an individual voter, and itself would not be human-readable, election administrators can protect ballots without knowing who marked which ones.

Secure Data Transmission Prevents Insider Manipulation

GUIDs can prevent multiple counting of the same ballot or the submission of fraudulent ballots with help from the Ballot Master Database. After polls close, secure software sends images of the ballots for validation against the Ballot Master Database. Using such a system to accumulate ballots not only allows redundant processing but also secures the chain of custody from the local precinct to the state. It eliminates the need to move physical ballots to a centralized counting facility, during which ballots could be misplaced or tampered with. The redundant data centers also ensure that no one can alter results by scanning in extra ballots after polls close because the system counts all votes two or more times and would flag and report discrepancies across counts.

Redundant Processing Detects Hackers

RAS principles guarantee a series of safeguards against hacking that can detect potential threats at numerous points in the tabulating and auditing processes. Many voters fear that hackers could manipulate elections, but redundant processing means they would have to corrupt two or three different systems simultaneously without raising any alarms. If the system is correctly deploying RAS principles, this would be nearly impossible. Even in that very unlikely scenario, both the paper ballots and ballot images would remain available to election administrators to cross reference and recount during an audit.

Conclusion

Voting systems are vital to our nation's democracy and therefore should be treated as mission critical systems. The application of **Reliability, Availability, and Scalability (RAS)** through cutting-edge security features can help protect elections and strengthen trust in the system. The solution outlined in this white paper would:

- Catch unauthorized ballot copying and creation of fake ballots
- Allow for rescanning of ballots with no risk of duplicative counting
- Maintain ballot secrecy
- Secure the chain of custody from the local precinct to the state
- Reduce risk of insider attacks
- Prevent hackers from changing results

About Remark Innovations

Remark Innovations Inc. is a wholly owned subsidiary of Gravic, Inc., based in Malvern, PA USA. This company is dedicated to providing Innovative Solutions for Society.

Gravic, Inc. has been a world leader in providing innovative data collection, transformation, and distribution solutions for over 40 years. Our software product groups have produced technologically advanced solutions that improve the businesses and personal lives of our over 100,000 customers and tens of thousands of OEM end-user licensees. The company is 100% owned by USA citizens.

Learn More: For more information on a proof of concept implementation of a Validation Architecture implementing RAS for balloting, contact the Remark Innovations at information@remarkinnovations.com.