SAIS 2022 Proceedings

Southern (SAIS)

4-1-2022

The Effect of Homomorphic Encryption on Voters' Perceptions of Security in Election Systems

Jonathan Kaufman
Christopher Newport University, jonathan.kaufman.18@cnu.edu

Michael Lapke
Christopher Newport University, michael.lapke@cnu.edu

THE EFFECT OF HOMOMORPHIC ENCRYPTION ON VOTERS' PERCEPTIONS OF SECURITY IN ELECTION SYSTEMS

Jonathan Kaufman
Christopher Newport University
jonathan.kaufman.18@cnu.edu

Michael Lapke
Christopher Newport University
michael.lapke@cnu.edu

ABSTRACT

In the United States, elections play a critical role in maintaining the democracy that is the foundation of this country. In the last few election cycles, technology has started to play a large role in elections. This increase in technology may have played a role in the emerging lack of trust that has become a focal point in recent years. Online voting use has started to make an appearance and will likely continue to grow in the future (US Election Assistance Commission, n.d.), further exacerbating technological change in electoral systems. There are several complex factors in this system that this research intends to explore. How exactly does technological change affect a voter's perception of security? Would a technical solution, such as homomorphic encryption change the perception of security in election systems? We finally seek to determine the degree to which the perception of security affects electoral system use

Keywords

US Elections, Homomorphic Encryption, Voter Perception, US Election Security

INTRODUCTION

In the United States, elections on all levels play an important role at maintaining democracy. These elections determine who the leaders of the United States will be in addition to who the leaders of each state will be. In the last few presidential elections, the topic of election security has become one of the forefront topics discussed (Bernhard et al., 2017).

In the recent elections, technology use in US election systems has continued to grow and become widely used in the United States. According to the US Election Assistance Commission, elections in the United States are administered by the local and state government for all local, state, and federal elections. This results in lower overall cybersecurity posture due to limited funding and staff at the state and local level. Additionally, this would create the perception of risk even if there was actually no increase in the election. According to Verified Voting, in the 2020 US Presidential Election there were some states that used over 30 different models of systems. This therefore means that there is a critical need to ensure that the equipment remains secure.

A technological subset that is starting to make an appearance in elections is the use of online voting systems. Currently, there are 25 states that make use of an online or electronic voting system for a select portion of their population, usually including military personnel deployed overseas (Gal and Panetta, 2018). This movement has come partially from The Uniformed and Overseas Citizens Absentee Voting Act, which assists in ensuring that overseas citizens still can vote in elections while they are overseas (US Election Assistance Commission, n.d.).

The area of online voting and general technology used to administer will continue to grow in the amount of use as well as the technology itself will continue to advance. Therefore, it is critical to look at how to secure these systems in order to maintain the confidentiality, integrity, and availability of the systems. As technology, especially online voting, becomes more widely used the number of vulnerabilities that are present will continue to rise as well. This idea is demonstrated in the use of an online voting system in Australia that had a wide array of vulnerabilities present that went undetected by the security review by election officials (Halderman and Teague, 2015).

In the United States election system, there are many different factors that play a role in the election integrity issues/trust issues in the election results. Some of these factors include political polarization, social media, and the systems themselves. However, this is a technical paper where we are researching the role that technology and voters' perceptions of the technology play in the issues in the election system. Even though these other roles may play a big part of the issues, those factors go beyond the scope of this study.

There are many aspects of the process that could have interference with US elections. These areas include election infrastructure, campaigns, as well as the people and the mis/dis-information that can be spread throughout the election process (Cable, n.d.). When referring to the lens of election security, dealing with election infrastructure includes the equipment that is used in the election as well as the policies and regulations implemented in the system.

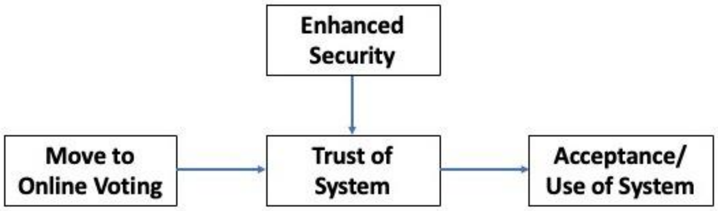

Figure 1 above demonstrates the relation between the move to online voting, enhanced security and the trust of the system. The figure also demonstrates the relationship between the trust of the system and the acceptance and use of the system. We believe that if a voter does not perceive the voting system as secure, they are less likely to accept the election system as a whole because of the perception. This perception is largely influenced by where the voters get their information relating to election security. This research will look at the acceptance of the current systems that are in use in US elections as well as look at some potential solutions that might be able to solve some of the security concerns relating to elections. The study hopes to determine the link between the trust of the voters in the system and how likely they would participate in the system. This research seeks to answer the following research questions:

RQ1: Do technical changes in electoral systems affect the perception of trust in these systems?

RQ 1a: Does moving to an online election system have a greater effect on the perception of trust in electoral systems than previous technological change?

RQ2: Do clear and present systems, such as homomorphic encryption, increase the trust of elections?

RQ3: Does the perception of trust of election systems affect the use of the system?

LITERATURE REVIEW

History of Election Integrity Concerns

The idea of election integrity being an issue is not a new topic and has been an issue in elections around the world since the beginning of democracy. In the early days of elections in Rome, there were many tactics that threatened the integrity of elections which included vote manipulation, violence, and bribery (Troxler, 2008). Early on, the Romans had casted their ballots through an oral vote, but in the late second century had switched to wax tablets due to the integrity concerns (Troxler, 2008). This demonstrates that this type of issue has always been a concern in the administration of elections; however, there are new complexities dealing with election integrity since technology is involved and the perpetrators could be outside US Jurisdiction.

Elections as e-Government

In the modern age and increasing technological abilities, many government functions have been transitioned to be completed electronically, which ultimately helps reduce the cost of government administration (Gritzalis, 2002). In recent elections, technology has played a crucial role in the administration of local, state, and federal elections, which for some election officials raise concerns about whether the elections systems are able to meet the legal requirements for this type of system (Gritzalis, 2002).

Electronic voting has become popular, especially with the development of a mobile app that allows certain voters to cast their ballot using the mobile app (Specter and Koppel, 2020). Using technology in elections solves some of the issues such as lowering the cost of election administration; however, it raises significant security concerns such as improper use of cryptography, privilege escalation, as well as poor software management (Choi and Kim, 2012).

Even though currently, e-Voting is only present in pilot runs, it is important to make sure the regulations that are in place adequately secure the systems to ensure accurate election results, as there are some present risks with these systems (Spector and Koppel, 2020). According to Gritzalis (2020), when developing the e-Government systems, specifically the eVoting systems, it needs to be carefully reviewed and designed to help improve the democratic process.

Lenses of Election Security

When discussing the idea of making an election more secure in the United States, there are a few lenses that need to be considered. In a presentation by Jack Cable, it mentions that the biggest areas are election infrastructure, the campaigns, and the people involved as well as the information that is spread throughout the election process (Cable, n.d.). Each of these components need to be analyzed in order to have a secure election. However, in this research, we are primarily studying the election infrastructure aspect of elections.

The lens that is likely to be thought about the most when considering election security is the infrastructure. The election infrastructure deals with the security of the ballot makers, ballot scanner, tabulators, poll books, and any other technology used in conducting the election. The primary security concerns within the lens of election infrastructure are the integrity and confidentiality of the data (Joaquim, Ferreira, and Ribeiro, 2013). The data confidentiality in terms of casting ballots in elections is privacy, the confidentiality after the ballot is cast is ballot secrecy and the data integrity is that the results are accurate. Securing the infrastructure will deal with encryption methods, authentication, hardware used, and data storage and processing. All these technological solutions help to secure certain aspects of the software and hardware that is used in the elections. This area covers the risks that lead to the occurrence of cyber-attacks on the election infrastructure.

Current State of Security in US Elections

According to Manpearl, as of the 2016 Presidential Election, there are over 9,000 local precincts (2018). This means that since elections are run on the local and state level, there are different standards on how to conduct elections in each jurisdiction (2018). With no federal standards on conducting elections, this leaves the potential for lower standards in each jurisdiction, especially regarding cybersecurity policies. As of January 6, 2017, the Secretary of the Department of Homeland Security has declared election infrastructure as critical infrastructure, which allows for more cybersecurity assistance to state and local officials (2017). By doing this, the government could produce stronger standards to ensure the integrity of elections. There are many mechanisms that exist that could be implemented to ensure the security of the election. However, the elected officials are trying to balance the security, cost, and convenience of the systems and measures that they enact within the US Election System. One major issue that is present within the current voting system in the United States is the potential for wide-spread election fraud due to the use of computer systems due to the inability to have a verifiable record of the election (Appel and Stark, 2019). Without the voter having the ability to know that their vote was recorded accurately; an audit of the election would be irrelevant if the ballots themselves were tampered with (Appel and Stark, 2019).

Election Equipment Used in the US

In the United States, there are several different models of voting equipment that are used throughout the country. When looking at the number of models used, it is important to consider the security implications of using so many types of machines. According to the data collected from Verified Voting shown in the table below, there are a total of 86 different models of voting equipment used in the 2020 Presidential Election. Among the different categories of equipment used in the United States for the 2020 Presidential Election, almost all categories have a significant number of models of each type which demonstrates that there is no standardization in election infrastructure in the US.

Security Concerns Related to Electoral Systems

As mentioned in the introduction of this paper, there has started to be a move to online voting systems. In a study done by Riedlberger (2020), they mention how moving to online voting would increase the voter turnout in elections. This would help resolve issues of low voter turnout and would make it more convenient for voters. However, Riedlberger (2020) also mentions how many countries have no longer been using online voting systems due to the risk and fear of cyber-attacks on their voting systems. This demonstrates the lower trust in the online voting systems.

There are many states that use electronic means to collect and store the votes cast in the election. Many states will implement a measure to make it seem like the security has increased, when this is not the case (Evans and Paul, 2004). One security concern is when there is no audit trail available for cast ballots, which would occur when the vote is fully electronic such as casting online, using an app, or with the use of DRE machines (Lindeman and Stark, 2012). This security risk will likely continue to grow as online voting continues to grow. This will not enhance the overall accuracy of the election as there is no record of the vote other than what was counted by the system (2004). Therefore, having a paper record or end-to-end verifiability of each vote plays a critical role in ensuring the integrity of the election is maintained. An important thing to note would be that if the code is maliciously written to alter votes cast, this would mean that an accurate audit most likely would not be able to be conducted since it could affect the audit record as well (2004).

As mentioned above, an increase in perceived security might not actually increase security, where an increase in actual security might not be perceived. According to Evans and Paul, an example of this would be when cryptographic methods are used (2004). This might not be able to be noticed unless the use of these cryptographic methods is made clear to the public (2004).

One form of security measure that can be implemented to increase the accuracy of the election would be end-to-end voter-verifiable ballots (Benaloh, 2015). One key aspect to ensure the election is secure and accurate as it relates to perception is to ensure that there is evidence to support the determined outcome of the election (Stark and Wagner, 2012). This security measure allows the voter to not have to place as much trust in the electronic system as they would have to place if there was no way to verify the recorded votes (2004).

In the 2020 US Presidential Election, there were some jurisdictions in two states, Utah and Washington, that used the Voatz mobile voting app in the election. However, according to Specter, Koppel, and Weitzner (2020) in research they conducted on this system, this system should not be used because of security exploits present in the system. In their research, they analyze attacks from the view of three different adversary types, which are attacker that has control of a user device, attacker that has control of API server, and a network adversary (2020).

If an adversary has root privileges on the user's device, this will allow them to perform a wide variety of attacks on the user (Specter, Koppel, and Weitzner, 2020). First, once they disable the malware protection that the app uses, they can fully control the user's app and collect personal data, including their PIN, and the individual's vote (2020). This is a critical flaw in the system as one of the key aspects of an election is ballot secrecy (Election Assistance Commission, 2021).

Another severe security risk in the application is that they were able to see the user's PIN in plaintext and that it is not protected when it is being stored (Specter, Koppel, and Weitzner, 2020). According to the researchers, the only piece of information needed to unlock the database is the PIN, which the app does not limit the number of attempts and must be an 8-digit pin (2020). Therefore, since the PIN must be numeric that means there is a character set of 10, which means the total number of possible PINs would be 10^8 which equals 100,000,000. According to the researchers, the PIN can be brute forced using a 3.1 GHz 2017 MacBook Pro in approximately 2 days (2020).

Another potential exploit that could occur is voter suppression, where the attacker causes the vote not to be counted while still showing the user the same dialog that would be shown if the vote was counted (Specter, Koppel, and Weitzner, 2020). In addition to suppressing a vote, an attacker could modify the vote to be for their desired candidate (2020).

Voter Perceptions

When thinking about the topic of election security, many individuals think of the measures put in place within the election systems themselves. However, not only does the integrity of the data have to be maintained, but the voters must believe and have confidence that the election results reflect the will of the voters (Evans and Paul, 2004). Without the voters having confidence, they will believe that the election was fraudulent and oftentimes try to find evidence to support their belief. When the voting system used does not produce a voter-verified paper ballot for each vote, auditing the results becomes difficult. This is a critical factor as it is important for the voters to know that their vote was recorded accurately. According to Weir (2018), only 40% of individuals had high confidence in the election results after the 2016 election.

This aspect of elections was a forefront topic that became relevant in the 2020 Presidential Election as a prominent group of individuals had a belief that the election had widespread election fraud. This belief continued even after the results of audits had been released by the states and the results were certified. In *Data Analytics to Enhance Election Transparency* by Bastian, et al (2021) mentions how in their research, there was no evidence of widespread election fraud when looking at the results from a few key states including Georgia. Their work discusses the topic of ballot harvesting and mentioned how the data demonstrated that these claims were unfounded (Bastian et al., 2021).

Previously, voters have usually accepted the reported results of the election as accurate; however, more recently as some elections have become more scrutinized, more and more voters have started to question the accuracy of the results (Evans and Paul, 2004). Therefore, it is becoming necessary to include more mechanisms to prove the accuracy of the election to the point where voters believe that the reported results are accurate (2004).

Homomorphic Encryption

As defined by Gentry (2010), homomorphic encryption is defined as "… a third party can perform complicated processing of data without being able to see it" (p. 1). This type of encryption has the potential to play a valuable role in elections as the purpose of this method of encryption is to maintain both the confidentiality and the integrity of the data. This is able to occur since the analysis operations are performed without the need to decrypt the data, which in the context of elections means that the identity of the voter does not need to be determined to maintain the integrity of the results (Sharma, 2016). This facilitates a "best of both worlds" scenario whereby you maximize secrecy while at the same time enabling complete functionality. Another aspect that is discussed in Sharma's (2016) work is that there are two forms of this encryption type which are fully homomorphic and partial homomorphic encryption (Benaloh, 1987). There are several uses for homomorphic encryption including healthcare and elections (Sharma, 2016). According to the dissertation by Gentry (2009), the first homomorphic encryption scheme that was used was the RSA encryption algorithm. Gentry (2009) discusses how one of the aspects needed to have a secure homomorphic encryption is semantically secure algorithm. The first encryption scheme that was semantically secure was developed by Goldwasser-Micali (Gentry, 2009).

METHODOLOGY

Theoretical Framework

The theoretical framework that will be used to collect the data for the research is the socio-technical model. This model looks at information systems from the human interaction side as well as the technological side (Bostrom and Heinen, 1977). There are multiple components which make up the socio-technical model, which are: structure, people, technology, and tasks (Bostrom and Heinen, 1977). Due to the high amount of human interaction with technology throughout the whole election system, this theory will be able to effectively analyze the election system from the perspective of voter perceptions.

The first component of this model on the social system side is the structure of the system (Bostrom and Heinen, 1977). In the context of US Presidential Elections, the structure of the system is complex. With the Presidential elections, it is a federal position, where the election is managed on the state-level and then the state has each locality run their election on behalf of the state. Therefore, this provides for the potential of weak policies and procedures for administering the election. This is the basic structure relating to the authority of election administration.

Now that the general structure of the administration of elections has been discussed, the structure of how ballot casting and ballot counting is conducted can be discussed. Every state in the United States makes use of technology in elections for casting ballots and counting ballots. This shows the structure aspect of the socio-technical model in the context of the US Presidential Elections.

The next area of the socio-technical model is the people (Bostrom and Heinen, 1977). When it comes to the election system, people play a critical role as humans interact with all aspects of the voting system from the campaigns prior to election day to counting the ballots. Another key area that humans affect in the election is the trust of the system. If an individual's belief is that the systems used to administer the elections are insecure then even if the systems are secure, it does not matter as much as the voters do not trust the system.

The third component of the socio-technical model is technology (Bostrom and Heinen, 1977). In the context of the United States Election System, the ballot counters, ballot markers, poll books, and other equipment used in the election administration would be the technology that falls under this component of the theoretical framework. These systems are critical in order to have a successful election.

The final component of the socio-technical model is the tasks (Bostrom and Heinen, 1977). The tasks deal with the interactions of the humans within the system. In the context of the election, this includes campaign ads, casting ballots, and ballot counting. These are just a few of the tasks that occur during the election and have critical effects on the overall election and the election results. If the processes involved in these tasks are tampered with in any way, it could potentially result in flawed results which in the end means the will of the voter was not maintained in the results.

Quantitative Approach

For this study, a quantitative approach will be used. This study will be conducted with a survey instrument in order to determine what voters' perceptions are as related to the use of homomorphic encryption within the election system in the United States. Before conducting the full study, a pilot study will be conducted in order to validate the survey instrument. For the pilot study, we will be collecting between 100-200 responses. After the survey has been validated, Survey Monkey Audience will be used in order to conduct the full study. For the study, we are looking for participants who are eligible to vote in the United States, which consists of US citizens who are 18 years or older and will be collecting between 390-1900 responses. The wide range is to account for the level of confidence, margin of error, as well as the cost needed to collect the responses. Between both studies, we will be looking to get responses from a wide variety of the US population in order to minimize any bias present in the study.

Conclusion

In this paper we wanted to define the problem, present the argument, review the prior work, and determine the methodology that will be used in this research study. Through the literature review, we found that the use of homomorphic encryption within election systems could be a beneficial solution in maintaining the ballot secrecy as well as the accuracy of the results. Therefore, this research will focus primarily on how this technical solution affects the voters' perception relating to the security of the system.

Approved for Public Release; Distribution Unlimited. Public Release Case Number 21-4034

REFERENCES

1. Appel, Andrew W., and Philip B. Stark. "Evidence-Based Elections: Create a Meaningful Paper Trial, Then Audit." *Geo. L. Tech. Rev.* 4 (2019): 523.
2. Bastian, H., Frye, E., Gary, C., Houck, D., Schneider, M., Thomason, F., & Werner, B. (2021). Data Analytics to Enhance Election Transparency.
3. Benaloh, J., Rivest, R., Ryan, P. Y., Stark, P., Teague, V., & Vora, P. (2015). End-to-end verifiability. *arXiv preprint arXiv:1504.03778*.
4. Bernhard, M., Benaloh, J., Halderman, J. A., Rivest, R. L., Ryan, P. Y., Stark, P. B., ... & Wallach, D. S. (2017, October). Public evidence from secret ballots. In *International Joint Conference on Electronic Voting* (pp. 84-109). Springer, Cham.
5. Cable, J. (2021). The Full Stack Problem of Election Security.
6. Choi, S. O., & Kim, B. C. (2012). Voter intention to use e-voting technologies: security, technology acceptance, election type, and political ide
7. Evans, D., & Paul, N. (2004). Election security: Perception and reality. *IEEE Security & Privacy*, *2*(1), 24-31.
8. Gal, S. (2018, November 2). *25 states allow some voters to submit their ballots electronically - here's how that works*. Business Insider. Retrieved December 21, 2021, from https://www.businessinsider.com/22-states-that-allow-you-to-vote-online-2016-9
9. Gentry, C. (2009). *A fully homomorphic encryption scheme*. Stanford university.
10. Gritzalis, D. A. (2002). Principles and requirements for a secure e-voting system. *Computers & Security*, *21*(6), 539-556.
11. Halderman, J. A., & Teague, V. (2015, September). The new south wales ivote system: Security failures and verification flaws in a live online election. In *International conference on e-voting and identity* (pp. 35-53). Springer, Cham.
12. Joaquim, R., Ferreira, P., & Ribeiro, C. (2013). EVIV: An end-to-end verifiable Internet voting system. *Computers & Security*, *32*, 170-191.
13. Lindeman, M., & Stark, P. B. (2012). A gentle introduction to risk-limiting audits. *IEEE Security & Privacy*, *10*(5), 42-49.
14. Manpearl, E. (2018). Securing US election systems: Designating US election systems as critical infrastructure and instituting election security reforms. *BUJ Sci. & Tech. L.*, *24*, 168.
15. Military *and overseas voting projects: U.S. Election Assistance Commission*. Military and Overseas Voting Projects | U.S. Election Assistance Commission. (n.d.). Retrieved November 19, 2021, from https://www.eac.gov/voting-equipment/military-and-overseas-voting-projects.
16. Riedlberger, K. (2020). *The impact of blockchain technology on the trustworthiness of online voting systems-an exploration of blockchain-enabled online voting* (Doctoral dissertation).
17. Sharma, T. (2016). E-voting using a homomorphic encryption scheme. *International Journal of Computer Applications*, *141*(13), 14-16.
18. Specter, M. A., Koppel, J., & Weitzner, D. (2020). The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in US federal elections. In *29th {USENIX} Security Symposium ({USENIX} Security 20)* (pp. 1535-1553).
19. Stark, P. B., & Wagner, D. (2012). Evidence-based elections. *IEEE Security & Privacy*, *10*(5), 33-41
20. *Statement by secretary Johnson on the designation of Election Infrastructure as a critical infrastructure subsector*. Department of Homeland Security. (2018, September 21). Retrieved December 20, 2021, from https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical
21. Troxler, H. (2008). Electoral Abuse in the Late Roman Republic.
22. United States Government. Election Assistance Commission. (2021). Voluntary Voting System Guidelines 2.0.
23. *Verifier*. Verified Voting. (n.d.). https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020.=
24. Weir, K. J. (2018). *Safeguarding democracy: increasing election integrity through enhanced voter verification*. Naval Postgraduate School Monterey United States.