Voting Security and Election Manipulation: Exploring the Incompatible Relationship Between Technology and Democracy

John Thiede, Evan Raab, Owen Kueter, Derek Choi, Jiahua Zhang, James Bongiovanni

Overview

This paper will cover the relationship between voting security and the potential election manipulation that may take place due to the implementation of electronic voting. From simple paper ballot voting, to large scale electronic voting, there exists entities and potential adversaries, at an increasing rate. This paper will explore the evolution of electronic voting and discuss real-world exploits that have proven the lack of security through a number of different attack surfaces. We will also discuss the past issues in the application of electronic voting and the result that follows. Finally, we will discuss the latest technology being used in electronic voting and the security flaws that are still present in today's voting securities.

Introduction

Many aspects of daily life nowadays are being completed online or with the assistance of technology. From online banking to self driving cars, technology is everywhere and provides unprecedented convenience. It is also a potential way to improve how people elect leaders and policy makers. However, it is not without risks. While technology can simplify the process of voting, it also brings a host of new security concerns. In order to determine the viability of e-voting, an in depth threat model of an e-voting system is necessary. The logistics of transitioning to an e-voting system is also an important factor. Much can be learned from the experiences of the countries that have tried to move to e-voting. Finally, it is important to

consider existing exploits on e-voting and voting machines, and methods to secure against such exploits.

II. Threat Modeling

To examine not just electronic voting, but voting in general, we need to identify all possible actors, their roles, any possible attack surfaces, and associated attacks. There are many entities even in a traditional paper voting system, most of which are not individuals, but rather broad groups and translate to a corresponding entity in a e-voting system in some way. First, there are the voters or citizens participating in the election, who will choose a candidate or a decision on a referendum, and submit this choice as their vote (Kumar et al). This is easily the broadest grouping of entities, as many of the other entities are voters themselves. Additionally, the candidates along with their associated campaigns and political parties are another entity in this system (Kumar et al): their aim is to convince voters to vote for them, or their candidates respectively. In close proximity to the candidates and their campaigns are political influencers, which consists of any group not actually a part of a campaign but has interest in seeing a particular candidate winning. Examples of these kinds of entities could be political action committees, special interest groups, labor unions, or even businesses and advertisers. These group tend to donate money to campaigns or create political ads on their chosen candidate's behalf. The votes have to be collected and counted to determine the results, and this is under the authority of the next entity in the system: balloting authorities, or "election managers" (Kumar et al). These entities are responsible for the process of receiving, processing, counting, and reporting the results to both the citizenry and other balloting authorities above them in scale. Due to the large scale of this process, these authorities are often set up as a distributed system

with local authorities reporting to regional ones, and so on up to the national level. Another entity, that is of great importance to the whole process, is the existing government itself. The government, like balloting authorities, is distributed across multiple levels of power, from local to state/provincial to federal. The government lays out laws and regulations the election must follow, and therefore is one of the most powerful entities in the whole system and must be considered, even if combating a malicious government is immensely difficult. Typically, the government directly controls a number of smaller entities which could play roles in this model, such as voter identification registries, which are systems used to verify the identities of voters registered in them, the aforementioned balloting authorities, and the military, which authoritarian governments could use to deter opposition to their regime.

Considering the various entities in a voting system, we can look the kinds of attacks possible when specific entities act maliciously. In a voting system, a single voter should only be able to cast a single vote for any given position or referendum they are voting for, but voters may not act honestly and abide by this restriction. Voter fraud occurs when voters act dishonestly and attempt to cast more votes than allowed, or vote in an election that they are not allowed to (i.e. voting in a senatorial race in a state they do not reside in). A great deal of trust has to be placed in the balloting authorities in the threat model, as the act of counting the votes is crucial to the outcome, and if they are to act maliciously there are substantial consequences. Vote rigging is an attack on the election process where the entities responsible for tallying the vote report false results, where the tally they report does not actually represent the decision of the voters. There are numerous ways in which candidates, campaigns, and political influencers can act unethically during an election, many of which fall out of the purview of a strictly security focused threat

model, but there are tangible ways in which they could compromise the election itself as well. These groups' goals are to get themselves or a candidate elected to office; if they are acting untruthfully, another potential exploit of the election system is vote buying. This is a situation in which one of the aforementioned groups attempts to "buy" votes from voters: promising some kind of compensation to voters who can prove that they voted for a specific candidate or decision. An inverse of this scheme is vote selling, where voters are in the more active role and seek to find entities who would pay them for voting a certain way. The existing government is the most powerful entity in the model and is potentially the most powerful adversary as well. The government can control, either directly or indirectly, many entities in the model, and can therefore perpetrate some of the attacks mentioned earlier on a grand scale. In the case of authoritarian states, elections may be held to uphold an illusion of democracy, but in actuality the entire process is farcical. It could be that the government fixes the vote so that the ruling party or leader always wins, or that opposition is suppressed through threat of violence or incarceration. These "fake elections" are perhaps the upper bounds of what an adversary is capable of under this system. As such it is likely that there is realistically very little that can be done to combat this, but it is still useful to delineate just what the most powerful adversary is capable of.

III. Evolution of the Threat Model with Technology

Of course, this threat model represents the issue of election security in only the broadest of terms, considering only the entities and threats present in any voting system. However, the implementation of the voting process is a critical factor that must also be considered. Based on the mechanics of the election, new entities and new attack surfaces may be introduced into the system. We can see how this threat model has evolved by looking at the ways in which

technology has been incorporated into elections, . In the earliest elections, the process had no automation: ballots are purely paper slips or some other object which voters mark and deposit into a collection box (Jones). These ballots are then removed by a balloting authority and counted by hand, and the results from their district are then reported to higher authorities until eventually a national tally is achieved. This is represented by the outlined threat model with very little alteration, a system consisting of only the most basic elements. While simple, the number of attack surfaces is relatively low, and is therefore possibly one of the most secure versions of a voting scheme.

However, this mode of vote counting does not scale very well, so automation is introduced in order to accommodate larger populations. This automation ranges from anything from lever based automated vote machines, to punch cards, all the way up to fully internet connected electronic machines and systems. The early lever based machines were designed to increase the speed, privacy, and usability of the whole election process (Jones), and while they do accomplish this, they add in a number of new entities into the threat system. The machines themselves have to be trusted to be in working order, and related to that their manufacturers have to be entities which ensure this. If either entity is malicious, the machine may not accurately record the voter's choice, or may compromise their privacy by leaking their choice to another entity. As such, the machine is a new entity, which adds new attack surfaces to the system. The largest jump in technology is the incorporation of electronic machines; specifically electronic machines which support connection to the internet. These machines, or other distributed systems, would not only allow for easier, more accessible voting and quicker counting, but could also be used by the government elected representatives during general assembly votes (Kurian). New

entities in the model that have to accomodate this are again the machines themselves, the databases which are storing these results, and potentially any router between the voter and these databases in the case of voting from a personal device. However, a machine connected to the internet opens a huge surface of attack for the sake of convenience and ease of use. Suddenly, if the vote process is connected to the internet, any device or user on the internet could theoretically be an entity we need to secure against. There is a great tradeoff of usability and security when considering an internet e-voting scheme, and one that needs further examination.

IV. Feasibility of Moving to E-Voting

In regards to the feasibility of moving to an e-voting system there are many things that must be considered. The best way to tackle this particular aspect of e-voting is to look at the cost/benefit analysis of moving to online voting, and whom that affects. The cost of e-voting is what matters most to the governing bodies, while the general public is most interested in the convenience factor.

The cost of moving to an e-voting system is of great concern to most government officials today, and whether or not the change is financially possible or reasonable for their country or state. A report out of the UK states that implementing on online voting system would cost the country 140 million pounds to implement and decrease the cost-per vote by 26% over time. (Pearson, 2017) On the other hand, some places using an e-voting system is looking to transition back to paper ballots. However, this cost is high as well. In the state of Georgia, officials are considering moving to paper ballots as their touch screen voting machines have no paper trail for citizens to confirm that their vote was received unaltered. Of the $380 million that are allocated to the states for election security funds, Georgia gets $10.3 million. Officials in

Georgia state that in order to change the current machines they would need 3 times that $10.3 million they have been given. (Newkirk, 2018)

Moving to an online voting system for all purposes seems to be a cost effective move to make for the government, and a relatively convenient change to make for the average citizen. Many of the complaints against the current system include the difficulty of finding a polling location, taking time off work to go to a physical location, and long lines at the location on election day just to name a few. All of these issues would be taken care of by moving to an online voting system, so the average citizen could vote on election day from the comfort of their own home or while at work.

An often overlooked group of citizens that must be included when thinking about the benefits of online voting are people who are non-users, or limited users of the internet. A recent report stated that 11% of Americans are non-users of the internet. (Anderson, Perrin, Jiang 2018) Another report states that in the UK, 90% of non-users are considered disadvantaged. Moving to an online voting system would certainly be casting away many people's ability and willingness to vote, and may lead to an unexpected disenfranchisement. Moving to an online voting system could be seen as a means of voter suppression on this particular group of people, which includes people of poor health, people in the lower classes, the elderly, and people who left school before the age of 16 (Yates, 2017). Non-users of the internet, along with individuals who are simply unable to access electronic voting, will be directly affected in the implementation of an online voting system.

Another group of people that must be considered are people with disabilities. A report was made during the 2017 UK general election about people with disabilities and their

experience with the current model of polling stations and voting by mail that is in place in the UK. Getting to the polling station and filling out a paper ballot was reported as being difficult by many, with reasons such as polling locations not being handicap accessible, polling booths not being large enough for people with wheelchairs, and polling location staff not being prepared to accomodate people with disabilities. When asked, this particular group was highly in favor of voting online, as that would alleviate many of the issues that affects their ability to comfortably vote on election day. (Electoral Commission, 2017)

While e-voting is extremely convenient for some of the population, and can save money in the long run for the government in some situations, there is still a large group of voters that would struggle with using the system. The ease of access in online voting is offset by the disenfranchisement of non-users of the internet, making the benefits of the transition less clear-cut.

V. Real World Exploits: What Can We Learn?

In August of 2018 at a hacking event called DEF CON 26, a group attempted to show fatal flaws in the United States voting equipment. For each piece of equipment they tried to exploit, they recognized that just because they found an exploit, doesn't mean it would be feasible in a real world scenario. In a paper that summarized the findings of the voting security group, it stated that a voting tabulator that is used in 23 states was susceptible to a remote network based attack. This attack would allow the hacker to change the results of the tabulator and gain the ability to change the voting count for 23 different states. This would allow the attacker to change the outcome of any election if they controlled enough of these machines. The only physical security that these machines had was a small lock that could be easily picked and

once an attacker had access to the internals of the machine, all they needed to do was connect a laptop through a simple connection process to obtain root access. (Blaze, 2018). The lack of security on such important machines leaves the entire country vulnerable to attack.

Another way voting machines are vulnerable is that they are able to be hacked in as little as 2 minutes with little to no equipment. All it takes is simply removing a plastic cover, disconnecting a wire, opening a lock with a ballpoint pen to get access to the restart button, and now the attacker has admin access. This presents a major problem, because the average American takes around 6 minutes to vote. (Blaze, 2018). Because the attack is such a quick process, realistically someone would be able to hack the machine within the socially acceptable amount of time they are allowed in the voting booth, and this means they may be able to get away with exploiting the machine.

A similar way voting can be influenced is by mobile reprogramming of electronic voting cards. This is done by reprogramming the card through near field communication, which is in most smartphones and gives the attacker the ability to reset the card after every vote. This is considerably easy, due to the fact that all of the voting cards have the same hard coded password. (Blaze, 2018). This means that any individual with a cell phone has the equipment necessary to hack the voting machine. This particular security flaw would allow to voter to vote as many times as they wanted, thus skewing the results of the election.

Thirty states allow some people, mainly individuals that are overseas or in the military, to vote via email. Email voting poses another threat to the security of elections. There's no secure protocol implement in email voting, which allows anyone to see the email. The attachment to the email can be altered to entirely change the person's vote from one person to another. This

process of changing the attachment can be automated, making email hacking a significant voter security risk. (Blaze, 2018).

The experiments done at DEF CON 26 shine a light on the number of flaws our electronic voting system has, and even with known exploits, we are still using these machines. The solution lies in implementing electronic voting testing to discover potential threats and exploits before an active elections takes place.

VI. Deployed Real World E-Voting Systems

Germany used electronic voting from 1998 to 2009, slowly scaling up how much it is used in important elections, until its first large-scale deployment in 2005's Bundestag elections. Up until that point, electronic voting machines were typically successful and seen favorably by the public. However, in 2009 two voters, political scientist Joachim Wiesner and his son, physicist Ulrich Wiesner brought a case to the German Constitutional Court. The two of them claimed that the electronic voting machines could be hacked and were unconstitutional because they were not transparent enough.

The court ruled in favor of the Wiesners that the machines were unconstitutional due to their lack of transparency. This ruling was based on Basic Law for the Federal Republic of Germany, similar to the US constitution. The Basic Law contained a principle stating that "all essential steps in the election are subject to public examinability". Extended to electronic voting, the ruling stated that "When electronic voting machines are deployed, it must be possible for the citizen to check the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge." (Sebes, 2009).

The problem was that it was difficult for an average person to understand all the steps of the process when they voted. The way that the machines recorded and counted votes could not be easily seen and understood without specialist knowledge. Due to this ruling, Germany returned to using paper to vote. As the ruling stated, "In a republic, elections are a matter for the entire people and a joint concern of all citizens. Consequently, the monitoring of the election procedure must also be a matter for and a task of the citizen. Each citizen must be able to comprehend and verify the central steps in the elections." (Sebes, 2009). The lack of public knowledge and transparency in Germany's online voting process, inevitably led to their return to paper voting.

From the late 1990s to 2007, the Netherlands used electronic voting machines extensively in their elections. During this time, there were few regulations on e-voting. The Dutch Elections Act stated that the machines needed some sort of certifying procedure and needed to guarantee that a person's vote was secret. To get a machine approved, a machine's prototype should be submitted to an independent agency that would test the machine against some regulations. These regulations had not been updated since 1997, and the results of the test were not made public.

These voting machines were generally well regarded and accepted until 2006, when a candidate obtained 181 votes at one voting station and a total of eleven votes at all the other stations combined. This suspicious voting pattern was further compounded since the candidate was a polling worker, as well as the person controlling the particular station where the 181 votes were earned. However, the Nedap machine used at the station had no paper trail, so there was no way of fixing this vote. However, after gathering evidence from voters in that district, the person was convicted of fraud.

With the new attention on this issue, a non-governmental organization, Wij Vertrouwen Stemcomputers Niet (We Don't Trust Voting Computers) managed to get ahold of a few Nedap machines and were able to crack the machine's security. On October 4th, the group took the machine onto live television to show how the security of the machine could be compromised. By taking out a few screws, the group exchanged two socketed EPROMS on the board and within five minutes, they had manipulated the results of the machine without anyone being able to detect it. The group also found that the machine didn't uphold the secrecy of votes, since the screen let out some radiation that could be read from a distance. This secrecy is guaranteed not just by Dutch law, but also by the European Convention on Human Rights.

From the work of Wij, the Dutch Cabinet began investigations on the machines and found that though the Nedap machines didn't radiate past 5 meters, another machine in use, the Sdu machine, could be read from over 30 meters away. The Sdu machines were left out of the elections that occurred around three weeks later.

Parliament then continued the investigation by creating two committees, one which would investigate how voting machines were approved in the past and another to look into new ways of doing the process. The first committee found that the Ministry's lack of technical knowledge allowed suppliers to have too much influence in the market and the decision making process. Over the years, responsibilities with elections and electoral legislation had shifted around several times, making the electoral system hard to understand and making the government unable to quickly respond to the issue brought up by Wij.

The second committee made recommendations related to the electoral process. They administered a new system, where one device would allow the user to input their vote and then

print it out, and then the printed paper would be put into another machine which could later count the votes. The voter would then be able to easily see the results of their inputs, as well as the paper trail of the vote.

Given these findings, the Regulation for Approval of Voting Machines, a law from 1997, was withdrawn on October 21st, 2007. All Nedap machines were decertified on October 1st, 2007. The Decree of 19 October 1989 was also amended, which removed the Minister's ability to make new regulations for voting machines. All in all, it was now impossible to certify new machines without new legislation, and the Dutch returned to paper voting schemes.

One of the newest technologies being considered to make online or electronic voting more viable is the use of blockchain. With blockchain, a network of computers each stores a copy of a database containing the votes. The computers all take turns changing the database. Each individual changes is a transaction, and the group of transactions a computer takes in a single turn is a block. Every block also contains in it a reference to the block before it. In this way, there is a chain of all the transactions that have happened to the data. This makes it easy to see if someone has made an unauthorized change to the data, and verifies who exactly has made the change. The chain also cannot be changed, since that is easily detected, making it immutable.

Immutability and verifiability are the two big benefits of blockchain. These prevent people from voting twice, since the record of the vote exists in the chain and is immutable. Votes cannot be deleted because again, the chain is immutable. A person can see what change was made because of them in the chain, so there is transparency. Lastly, the chain can be encrypted, so people's votes can be private.

A lot of places are working on or considering using blockchain voting technology for a new e-voting system. These include Catalonia, Ukraine, and South Korea. West Virginia has already tried a blockchain voting system, allowing military personnel overseas to cast their ballots through a mobile, blockchain-based platform. Although this trial was successful, the deputy chief to West Virginia's Secretary of State Mac Warner told the Washington State, "Secretary Warner has never and will never advocate that this is a solution for mainstream voting." (Wood, 2018).

There are several reasons that blockchain voting isn't considered a viable solution to the security of electronic voting. One issue is that voters could claim after the election to have voted for someone different, and it would be difficult to verify the validity of their claim, especially due to the difficulty of the public being able to understand how blockchain works. The complexity of the system makes it difficult for uninformed officials to make decisions for the uninformed public.

Another big issue with blockchain doesn't really have much to do with blockchain, but rather the infrastructure surrounding it. In a quote to CNN, Joseph Lorenzo Hall, a chief technologist at the Center for Democracy and Technology said "Mobile voting is a horrific idea. It's internet voting on people's horribly secured devices, over our horrible networks, to servers that are very difficult to secure without a physical paper record of the vote." (Dumas, 2018). The issue here is that the voting here is done on mobile phones, over unsecured wireless networks, all the way to other servers. All of these things still have security flaws, and since they cannot be managed by a single central authority they can never be fully secured.

VII. Conclusion

Advancement in technology and the implementation of electronic voting has proven to simplify the voting process, but inevitably poses many threats to the security and integrity of an election. As the voting process becomes easier and more user friendly, the amount of threats and entities involved becomes greater and more complex. Electronic voting may provide easier accessibility to voting, but some may argue that it is not financially feasible and can limit the ability of particular groups of voters. Currently, electronic voting cannot be implemented at a large scale with complete guarantee that an individual's vote will remain secure. The number of additional entities and attack surfaces in an electronic voting system is difficult to fully secure against. Despite the potential benefits, the drawbacks, especially in the security of the system, make electronic voting a dangerous proposition.

Works Cited

Anderson, Monica, Perrin Andrew, Jingjing Jiang. “11% of Americans Don’t Use The Internet. Who Are They?” Pew Research Center, 5 March. 2018 https://www.pewresearch.org/fact-tank/2018/03/05/some-americans-dont-use-the-internet-who-are-they/

Ayyash, Ali. “How Blockchain Will Make Electronic Voting More Secure.” *Hacker Noon*, Hacker Noon, 25 May 2018, hackernoon.com/how-blockchain-will-make-electronic-voting-more-secure-fba15d752bee.

Blaze, Matt, et al. “DEF CON 26 Voting Village.” *DEF CON*, Sept. 2018, www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf.

“Blockchain Technology in Online Voting.” *Follow My Vote*, followmyvote.com/online-voting-technology/blockchain-technology/.

Dumas, Breck. “West Virginia Is First in US to Allow Some Absentee Voting from Smartphones.” *TheBlaze*, TheBlaze, 26 Sept. 2018, www.theblaze.com/news/2018/09/26/west-virginia-is-first-in-us-to-allow-some-absentee-voting-from-smartphones.

“Dutch Citzens Group Cracks Nedap's Voting Computer.” *Heise Online*, Heise Online, 6 Oct. 2006, 10:45, web.archive.org/web/20070117143032/http://www.heise.de/english/newsticker/news/79106.

Jones, Douglas. “A Brief Illustrated History of Voting” *University of Iowa*. Web April 14 2019. http://homepage.divms.uiowa.edu/~jones/voting/pictures/

Electoral Commission. “Elections For Everyone: Experiences of people with disabilities at the 8 June 2017 UK Parliamentary general election.” Nov. 2017. https://www.electoralcommission.org.uk/__data/assets/pdf_file/0008/237194/Accessibility-report-call-for-evidence.pdf

Kurian, George T. "Polling, History of." *The Encyclopedia of Political Science.* Ed. Washington: CQ Press, 2011. 1309-1310. *SAGE Knowledge*. Web. 14 Apr. 2019, doi: 10.4135/9781608712434.n1213.

Kurian, George T. "Electronic Voting." *The Encyclopedia of Political Science.* Ed. Washington: CQ Press, 2011. 491. *SAGE Knowledge*. Web. 14 Apr. 2019, doi: 10.4135/9781608712434.n499.

Lee, Timothy B. “Blockchain-Based Elections Would Be a Disaster for Democracy.” *Ars Technica*, Ars Technica, 6 Nov. 2018, arstechnica.com/tech-policy/2018/11/blockchain-based-elections-would-be-a-disaster-for-democracy/.

Loeber, Leontine. (2008). E-Voting in the Netherlands; from General Acceptance to General Doubt in Two Years.. 21-30.

Newkirk, Margaret. “Advocates Say Paper Ballots Are Safest” Bloomberg, 10 Aug. 2018 https://www.bloomberg.com/news/articles/2018-08-10/advocates-say-paper-ballots-are-safest

Partz, Helen. “Catalan Government Considers Blockchain for Public E-Voting System.”

Cointelegraph, Cointelegraph, 19 Nov. 2018, cointelegraph.com/news/catalan-government-considers-blockchain-for-public-e-voting-system.

Pearson, Ben. "Cost of Voting: Report Launch" Webroots Democracy, 9 Nov. 2017, https://webrootsdemocracy.org/2017/11/09/cost-of-voting-report-launch/

"Re-Evaluation of the Use of Electronic Voting in the Netherlands." *NDI*, National Democratic Institute, www.ndi.org/e-voting-guide/examples/re-evaluation-of-e-voting-netherlands.

Reuters. "German Court Rules E-Voting Unconstitutional | DW | 03.03.2009." *DW.COM*, DW, 3 Mar. 2009, www.dw.com/cda/en/german-court-rules-e-voting-unconstitutional/a-4069101.

Kumar, S. Dinesh; Vamsikrishna Patchava; Tyagi, Akshat; Bommisetty, Dinesh; Babu Kandala, Hari. "Theoretical analysis of voting systems," *2016 International Conference on Communication and Electronics Systems (ICCES)*, Coimbatore, 2016, pp. 1-5.

Sebes, John. "Electronic Voting Banned in Germany." *TrustTheVote*, TrustTheVote, 2 Sept. 2009, trustthevote.org/blog/2009/09/02/electronic-voting-banned-in-germany/.

Suberg, William. "Ukraine Electoral Commission Uses NEM Blockchain for Voting Trial." *Cointelegraph*, Cointelegraph, 8 Aug. 2018, cointelegraph.com/news/ukraine-electoral-commission-uses-nem-blockchain-for-voting-trial.

"The Constitutionality of Electronic Voting in Germany." *NDI*, National Democratic Institute, www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany.

Wood, Aaron. "West Virginia Secretary of State Reports Successful Blockchain Voting in 2018

Midterm Elections." *Cointelegraph*, Cointelegraph, 17 Nov. 2018, cointelegraph.com/news/west-virginia-secretary-of-state-reports-successful-blockchain-voting-in-2018-midterm-elections.

Yakubowski, Max. "South Korean Government to Test Blockchain Use for E-Voting System." *Cointelegraph*, Cointelegraph, 28 Nov. 2018, cointelegraph.com/news/south-korean-government-to-test-blockchain-use-for-e-voting-system.

Yates, Simon. "The Real Digital Divide" Good Things Foundation, June. 2017 https://www.goodthingsfoundation.org/sites/default/files/research-publications/ofcom_report_v4_links.pdf