Voting Security in the United States

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Amanda Murray

Spring, 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature  Date 4/26/2020

Amanda Murray

Approved _____ Date _____

Michael Gorman, Department of Engineering and Society

Voting Security in the United States

Introduction

One of the difficult tasks of maintaining a democracy at such a scale as the United States is implementing a voting system that is secure, reliable, fair, private, and accessible to all eligible voters. Despite commendable efforts, it is arguable that there has never been such a system in the United States. The methods used to try and address the problem have always had some caveat; hand counting votes requires a balance between privacy and fairness, mechanical machines can be confusing and difficult to operate, and electronic machines are prone to cybersecurity attacks.

Despite the risks, the United States has shifted to rely more and more heavily on direct recorded electronic (DRE) voting. This has created a recent surge in discussions about the security of elections in the United States. Could an election be hacked? What would the impact of such a hacking be? How could such a hacking be prevented? This thesis explores voting machines in the United States, the likelihood of such a machine being hacked, and analyzes possible means of prevention for such a hacking.

Background on Voting Machines

Early in the history of the United States voting was done without the aid of any machines. Ballots were cast using simple scraps of paper provided by the voters (Jones, 2003). While simple and reliable, this early method of voting did not guarantee a fair and private voting system. It was difficult to balance privacy and honesty. If officials checked that each person provided only one vote, they would deny the voter privacy and if they did not check they could not guarantee every voter's honesty (Jones, 2003).

In 1892, the first pull-lever voting machine was used in Lockport, New York and in 1896 this style of voting machine was used for the first time in a large election in Rochester, New

York (Jones, 2003; Harris, 1934). These voting machines were large contraptions where the voter would step in and pull a series of levers to cast their votes and the machines would then record the votes by incrementing mechanical counters (Edwards, 2004; “Voting Technology”, n.d.). Pull-lever voting helped solve problems around privacy and ballot box stuffing and sped up turnaround time for counting votes (Jones, 2003). They dropped the time to tally the votes from a few days to less than an hour in Rochester (Edwards, 2004). Slowly these machines took over America, becoming prominent in most urban centers by the 1930s, thus beginning a new voting paradigm (Jones, 2003).

Following this paradigm there came punch-card voting machines. Developed in the 1960s, these machines used pre-scored pieces of paper to record votes and card readers to tally the votes (“Voting Technology”, n.d.). These machines were cheaper, lighter, and just as fast as the pull-lever machines (Fessenden, 2000). They quickly became prominent in the United States; by the 1980s a majority of states were using pull-lever or punch-card machines for elections (“Voting Technology”, n.d.).

For several decades after the 1980s, there were no large-scale changes in voting technology. The next major shift would come in the wake of the 2000 presidential race between George Bush Jr. and Al Gore. It was an incredibly close presidential election, with narrow margins in the electoral college. Both leading candidates needed the 25 electoral votes from Florida and only a few hundred votes separated the candidates in Florida (Elving, 2018; “Media Recount: Bush Won the 2000 Election”, 2001). This forced a recount in the state (“The election of 2000”, n.d.).

The recount of votes in Florida exposed severe issues around the machinery used for voting in the United States. The ballots cast in Florida were confusing. Many had “dimpled” or

"hanging" chads that made it impossible to truly understand the voter's intentions (Elving, 2015). In Florida alone there were 171,000 contested presidential ballots, including 111,000 ballots where more than one candidate was selected (Payson-Denney, 2015). In a study by the Massachusetts Institute of Technology and the California Institute of Technology it was estimated that there were between 1.5 and 2 million presidential votes uncounted due to difficulties using voting equipment and confusing ballots ("Voting What is and What Could Be", 2001). The study also uncovered additional barriers to voting regarding voter registration and absentee voting ("Voting What is and What Could Be", 2001).

In an effort to address these problems, the Help America Vote Act (HAVA) was passed in 2002. HAVA created mandatory minimum standards for election administration, and provided funding to help states reach these standards ("Help America Vote Act", n.d.). The act allocated $3.9 billion for states to carry out important upgrades, such as to their voting machinery (Gambhir & Karsten, 2019). A large portion of those upgrades were switches to DRE voting machines, which were seen as accessible and convenient (Gambhir & Karsten, 2019). This led to the latest shift in voting technology: the shift to DRE and optical scanner voting machines.

DRE Voting, Security, and Reliability

Most states now use either electronic or optical scan voting machines ("Voting Technology", n.d.). DRE voting machines are "essentially portable computers" ("Voting Technology", n.d.) that allow the user to select from a list of candidates. Even early on in the adoption of DRE voting, professionals had reason to be concerned about the security and reliability. The report generated by the Massachusetts and California Institutes of Technology listed DRE's the second least reliable machines for recording votes in the United States ("Voting What is and What Could Be", 2001). In the early 2000s Diebold, also known as Premier Voting

Solutions, was found to be producing machines that all had the same PIN code, which was "1111" (Schwartz, 2003). That same company's source code was also published to the internet, later to be found and critically analyzed by computer scientists (Wofford, 2016).

Nearly two decades later, there is still a critical eye on the security and reliability of these machines. In a new, greater wave cybersecurity experts and lay-people alike are concerned about the security of elections in the United States. For the past three years at Def Con people passionate about cybersecurity and hacking have had the opportunity to take a crack at the voting machines used around the United States in election (Collier, 2019). The results from these trials have been enough to concern Oregon Senator Ron Wyden (Telford, 2019). However, it is important to understand the scale of the problem and to understand the potential impact of such a problem. In order to try and understand the problem this thesis examines the ES&S IVotronic, a machine which was used in the 2016 election ("Election Systems and Software (ES&S) IVotronic", n.d.). ES&S is one of the biggest producers of electronic voting equipment in the United States (Mehrotra and Newkirk, 2019). While this exploration likely won't capture the whole picture of voting in the United States, it should be able to provide a meaningful glimpse.

Two separate states have funded investigations of the ES&S IVotronic machines or their source code which looked for possible flaws in the security and reliability of the machines. Ohio funded the Evaluation and Validation of Election-Related Equipment, Standards and Testing (EVEREST) Project, which studied the hardware, software, and firmware of the machines and Florida supported the Software Review and Security Analysis of the ES&S IVotronic 8.0.1.2 Voting Machine Firmware (SAITL Software Review), which studied only the firmware for the IVotronic. While these studies had differing goals, both reported several potentially hazardous security flaws in the system.

The EVEREST Project uncovered over a dozen serious security flaws in the IVotronic voting system or the Unity system used to manage elections. The technical skills required to take advantage of these holes in security range from unplugging a cable to creating a complex piece of malware. Two of note require almost no technical skills: the touchscreens can be recalibrated to block the selection of some candidates, and the Real Time Audit Log printers can be unplugged without any tools (McDaniel et al., 2007). A few more technically intense security flaws of note are the Unity System's buffer overflow vulnerability when reading the Master Personalized Electronic Ballot (PEB), the ease with which PEBs may be emulated, and the various attacks that can be performed with an emulated PEB.

Each of these attacks require different levels of access and target different aspects of the voting process. In order to recalibrate the touchscreen, one must have access to a PEB used for quality assurance (QA), which would not usually be given to a voter at the polls (McDaniel et al., 2007). The people who would usually have access to such a tool would be those administering the election. However, any QA PEB compatible with an ES&S IVotronic machine will suffice, as there is no authentication to ensure the validity of the PEB (McDaniel et al., 2007). This means that anybody who has been involved in administering an election that uses IVotronic machines in the past or present could utilize this security hole to attack the election. The primary motivation of an attack such as this would be to limit the number of votes cast for a certain candidate. It's highly visible and may be noticed and fixed as soon as somebody tries to vote for that candidate.

In contrast, some low-tech attacks could remain unnoticed for the whole of an election and may be carried out by anybody with physical access to the machine. The cable for the Real Time Audit Log printer can be unplugged without any tools or hardware. By disabling a RTAL

printer an attacker is sabotaging the means of auditing an election. By doing so, in the case of an audit, the validity of the whole election can come in question, even if there has been no tampering otherwise.

The first of these security holes comes in the form of a buffer overflow attack. A buffer overflow is when an array, which stores data as a list-like sequence, overflows out of its assigned memory (Black & Bojanova, 2016). A buffer overflow vulnerability occurs when a program does not process inputs in a safe way (McDaniel et al., 2007). When exploited a buffer overflow can open the door to an attack taking control of the entire system (McDaniel et al., 2007).

While there are many buffer overflow vulnerabilities in the ES&S voting system, the most concerning exist in the Unity subsystem. The Unity subsystem is a suite of tools that allows one to manage an election, including important functions such as creating the ballot and reporting the results (McDaniel et al., 2007). There exists a buffer overflow attack within Unity's Election Reporting Manager, which reports results (McDaniel et al., 2007). This buffer overflow attack can be carried out using any PEB that can be read using a PEB reader (McDaniel et al., 2007). The Election Qualification Code, a security code that could be used to verify the legitimacy of a PEB, is not checked, which means that any PEB, including those which have been taken from other precincts or those that have been doctored, can be used in this attack (McDaniel et al., 2007). There is restricted access to this exploit, however; few individuals will have access to the Unity manager. The SAITL Software Review in Florida found similar security holes using PEBs. They noted the fact that such an attack would not likely be discovered during standard testing for each voting machine (Yasinsac et al, 2007). They also highlighted that the risk of such an attack could be reduced with the use of "procedural and physical security defenses" (Yasinsac et al, 2007).

The EVEREST Project also found that PEBs can also be very easily emulated. They discovered that if somebody could understand the IR protocols which the PEBs use, they could easily emulate the PEB with a small magnet and a Palm Pilot (McDaniel et al., 2007). The implications of this security flaw are striking: with the ability to emulate a PEB an attacker could carry out a "wide range of serious poll worker and voter attacks" (McDaniel et al., 2007). The simplest of which is allowing a voter to cast multiple votes (McDaniel et al., 2007). The resulting impact from such an attack could be very small when carried out by an individual, but a group of only 25 casting 10 extra votes would amount to 250 extra votes—the Florida election was only won by a few hundred votes. Furthermore, if the RTAL printer remains untampered with, these votes would be recorded in the paper trail, and considered authentic in an audit.

These are just a few select vulnerabilities in the system around voting using the ES&S IVotronic system. Examining just these it is clear that there exists sufficient potential for malicious actors to cause untold damage to an election which uses these systems. There are similar problems in other popular voting systems in the United States; The Sequoia AVC Edge, which was also used in the 2016 election has hardware which could easily be manipulated and the Hart InterCivic eSlate has been found to have a large list of issues ("Sequoia (Dominion) AVC Edge", n.d.; Appel, 2011; Proebstel et al, 2007).

Anticipatory Governance and Voting Security

These results are not shocking. Cybersecurity is an already difficult field and is rapidly growing and increasing in complexity. Even if these machines were found to be flawless in the reviews completed on them there is a good chance that in time they would be outdated and vulnerable to new attacks. It's arguable that machines such as these will never be completely secure. There is, however, still hope: there is potential for mitigation of risks. The Hart

InterCivic eSlate has received expert approval for usage in elections despite its flaws; the vulnerabilities found in its investigation were able to be protected through the addition of election procedures (Proebstel et al, 2007).

This kind of policy making, where one looks forward to potential disasters and tries to prevent them, can be referred to as Anticipatory Governance, as useful sociotechnical philosophy. Anticipatory Governance is a socio-technical framework where the practitioner attempts to anticipate and manage behaviors around emerging technologies while management is still possible (Guston, 2014). The United States can utilize Anticipatory Governance in several areas to protect elections in the scope of voting machines: in the design and testing of voting machines, in the federal legislature passed, in state and local legislature, and in the public.

Guston explains that Anticipatory Governance "considers the meaning and ramifications of decisions that are being made in the here-and-now" (pg. 233, 2014). He explains that the purpose of having a social scientist in the nanotech labs he works in to ask the scientists important questions about their decisions. To apply this concept to design of voting machines, companies can hire, as a parallel to Guston's resident social scientists, groups of computer scientists and cybersecurity experts to act as both consultants and sanity check for the in-house developers. A third-party group of cybersecurity professionals asking the developers "Why?" and "How?" creates a first-line-of-defense, anticipating human error in the development of these machines.

The next step is to anticipate that even after several iterations of quality assurance, there will be things missed. Machines should be tested by a large-scale group of ethical hackers, such as those who completed the EVEREST investigation. These hackers can produce similar reports for federal or state governments to work with.

Federal governments are the next stage where Anticipatory Governance can play a key role in the protection of an election. HAVA has already given the United States a tool to protect their elections via Anticipatory Governance; the bill created the U.S. Election Assistance Commission (EAC), which sets out guidelines for states to follow to when selecting voting equipment ("Help America Vote Act", n.d). The EAC is an ideal position to leverage reports from ethical hackers and cybersecurity experts to design criteria for each voting machine to be used securely. Using the IVotronic as an example, one can see that a large number of weaknesses in the system occur when a PEB falls into the wrong hands, or when physical security is not sufficient. The EAC can create guidelines for strict control of PEBs and require certain amounts of physical security, such as mechanisms locking in and protecting certain cables. These steps can help protect against a large number of potential attacks.

State and local governments can also use Anticipatory Governance to protect voting machines. A powerful tool in the fight against election hacking is the audit. Often, DRE machines will produce paper trails that can be audited if an election comes into question. While this may be effective, it can be costly to hand-count all of the ballots produced and difficult to decide when that cost is warranted. In this context, each state can look to the past and collect data which can be used to understand themselves and anticipate future outcomes. In the case of elections, it is well known that many locations are "red" or "blue" and that those colors rarely change. States and districts that understand this and are aware of their own tendencies are capable of recognizing when a result does not seem to fit what they would expect and when an audit may be necessary. There is little doubt that an audit will be necessary in each state at some point in time; setting up tools to let you decide when that it ahead of time is a form of Anticipatory Governance.

The final, and perhaps most important field where the United States can apply Anticipatory Governance is in the public space. By teaching the public how to vote correctly and how to respond to problems when voting the country can leverage its most plentiful resource: people. Sufficient technical literacy and understanding on the part of the voter cannot be assumed. The United State should take steps to ensure each voter is using each machine correctly. In machines where a ballot is printed, each voter should know to check that ballot for accuracy. In other machines, voters should know what tools and mechanisms are being used to confirm their votes are being cast correctly.

Furthermore, voters should be educated on what they should be concerned about seeing at the polls. They should be able to tell when, for example, a printer cable that should be plugged in is unplugged, and they should know who to speak to about it. The responsibility for protecting the vote can be placed just as heavily into the hands of vigilant citizens. Public education initiatives that help voters recognize machine tampering can act as a final layer of Anticipatory Governance which protects citizens from election fraud and misrepresentations about voting in the media.

Conclusion

The history of voting in the United States is a long and complicated one. Unfortunately, it seems that efforts to make voting more reliable haven't been as successful as they could. Voting machines in modern America are riddled with security flaws, vulnerabilities, and downright dangerous coding practices that open the United States up to election fraud. These flaws are severe in nature and could allow for consequences from ineffective audits, to chaos, to elections being swung in the wrong way. Flaws such as this are not confined to only one model or brand of voting machine, either.

However, these issues do not invalidate these important tools of democracy. By utilizing anticipatory the United States can reduce the risk of malicious actors carrying out successful attacks on democracy. Anticipatory governance can be applied to several different social systems, each of which has their own important role to play. Implementing these layers of governance allows the United States to anticipate, prevent, and react to election hacking in clean, precise ways.

Future Work

Potential future work could be done in two very interesting realms: attacks on voter registration and the use of voter registration enact modern Jim Crow laws. There are numerous examples of state officials dropping people of color from voter registrations illegitimately in the states across the country, and many theorize these are new methods of enacting Jim Crow-style restrictions.

Another potential field for future work is looking into the security of voter registrations. If a malicious actor was interested in undermining democracy or causing chaos in the United States, could they find a way to drop voters from the state registrations without authorities noticing? Voter registrations are often able to be viewed and, in some cases, modified or updated using the internet.

References

Appel, A. W. (2011). Security Seals on Voting Machines. ACM Transactions on Information and System Security, 14(2), 1–29. doi: 10.1145/2019599.2019603

Black, P. E., & Bojanova, I. (2016). Defeating buffer overflow: A trivial but dangerous bug. IT

Professional, 18(6), 58–61. https://doi.org/10.1109/MITP.2016.117

Collier, K. (n.d.). Hackers find voting machines used throughout the US are vulnerable to attack. CNN. Retrieved April 7, 2020, from https://www.cnn.com/2019/09/26/politics/hackers-voting-machines/index.html

Edwards, O. (2004, November). When Pulling a Lever Tallied the Vote. Smithsonian. Retrieved from https://www.smithsonianmag.com/smithsonian-institution/pulling-lever-tallied-vote-98774074/

Election Systems and Software (ES&S) IVotronic. n.d. Retrieved October 27, 2019, from https://www.verifiedvoting.org/resources/voting-equipment/ess/ivotronic/.

Elving, R. (n.d.). The Florida recount of 2000: A nightmare that goes on haunting. NPR.Org. Retrieved April 7, 2020, from https://www.npr.org/2018/11/12/666812854/the-florida-recount-of-2000-a-nightmare-that-goes-on-haunting

Fessenden, F. (2000, November 19). Counting the vote: The machine; new focus on punch-card system. The New York Times. https://www.nytimes.com/2000/11/19/us/counting-the-vote-the-machine-new-focus-on-punch-card-system.html

Gambhir, R. K., & Karsten, J. (2019, August 14). Why paper is considered state-of-the-art voting technology. Brookings. https://www.brookings.edu/blog/techtank/2019/08/14/why-paper-is-considered-state-of-the-art-voting-technology/

Guston, D. H. (2014). Understanding 'anticipatory governance.' Social Studies of Science, 44(2), 218–242. https://doi.org/10.1177/0306312713508669

Harris, J. P. (1934). Election Administration in the United States. By Joseph P. Harris. Washington: The Brookings Institution. Retrieved from https://babel.hathitrust.org/cgi/pt?id=mdp.39015020809649&view=1up&seq=14

Help America Vote Act. (n.d.). Retrieved April 7, 2020, from https://www.eac.gov/about_the_eac/help_america_vote_act.aspx

Jones, D. W. (2003). A Brief Illustrated History of Voting. Retrieved from http://homepage.divms.uiowa.edu/~jones/voting/pictures/#punchcard.

McDaniel, P., Butler, K., Enck, W., Hursti, H., McLaughlin, S., Traynor, P., Aviv, A., Cerny, P., Clark, S., Cronin, E., Shah, G., Scherr, M., Kemmerer, R., Balzarotti, D., Bankd, G., Cova, M., Felmesteger, V., Roberston, W., Valeur, F., … Quilter, L. (2007). EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing

Media recount: Bush won the 2000 election. (2001, April 3). PBS NewsHour. https://www.pbs.org/newshour/nation/media-jan-june01-recount_04-03

Mehrotra, K., & Newkirk, M. (n.d.). Expensive, Glitchy Voting Machines Expose 2020 Hacking Risks [News]. Bloomberg. Retrieved April 7, 2020, from https://www.bloomberg.com/news/articles/2019-11-08/expensive-glitchy-voting-machines-expose-2020-hacking-risks

Payson-Denney, W. (n.d.). Who really won Bush-Gore election? - CNNPolitics. CNN. Retrieved April 7, 2020, from https://www.cnn.com/2015/10/31/politics/bush-gore-2000-election-results-studies/index.html

Proebstel, Elliot & Riddle, Sean & Hsu, Francis & Cummins, Justin & Oakley, Freddie & Stanionis, Tom & Bishop, Matt. (2007). An analysis of the hart InterCivic DAU eSlate. 3-3.

Schwartz, J. (2003, December 3). Ohio study finds flaws in electronic voting. The New York Times. https://www.nytimes.com/2003/12/03/us/ohio-study-finds-flaws-in-electronic-voting.html

Sequoia (Dominion) AVC Edge. n.d. Retrieved October 27, 2019, from https://www.verifiedvoting.org/resources/voting-equipment/sequoia/avc-edge/.

Telford, T. (n.d.). Hackers were told to break into U.S. voting machines. They didn't have much trouble. Washington Post. Retrieved April 7, 2020, from https://www.washingtonpost.com/business/2019/08/12/def-con-hackers-lawmakers-came-together-tackle-holes-election-security/

The election of 2000 (Article). (n.d.). Khan Academy. Retrieved April 7, 2020, from https://www.khanacademy.org/humanities/us-history/modern-us/1990s-america/a/the-election-of-2000

Voting technology. (2019). Retrieved October 28, 2019, from https://electionlab.mit.edu/research/voting-technology.

Voting What is What Could Be. (2001). Massachusetts Institute of Technology and California Institute of Technology.

Wofford, B. (August 05, 2016). How to hack an election in 7 minutes. POLITICO Magazine. Retrieved April 7, 2020, from https://politi.co/2K2OGOv

Yasinsac, A., Wagner, D., Bishop, M., Baker, T., Medeiros, B., Tyson, G., Shamos, M., & Burmester, M. (2007). Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware. Florida State University.