Identyti: Digital Storage of Personal Identification Documents

(Technical Topic)

Vulnerabilities of Voting Machines

(STS Topic)

A Thesis Project Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia Charlottesville, Virginia

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Amanda Murray

Fall, 2019

Technical Project Team Members: Eric Burbach, Chris Han, Sri Jayakumar, Samantha Kostleni, Gio Lee, Amanda Murray

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 Amanda Murray

Approved _____ **Date** _____

Michael Gorman, Ph.D., Professor, Department of Engineering and Society

Approved _____ **Date** 11/23/2019

Ahmed Ibrahim, Ph.D., Assistant Professor, Department of Computer Science

Vulnerabilities of Voting Machines

Introduction

It is arguable that there has never been a great way of counting votes in the United States. The United States is a country of vast size; to accurately document the wishes of every voting citizen is a task of a comparably vast size. In the past we've tried a variety of methods to conquer that behemoth, including hand-counting votes, large contraptions that increment mechanical counters, the infamous punch card, and, most recently, electronic voting. Inspired by recent claims of a hacked election, I plan to explore the history of voting machines, their current role in the United States, and the likelihood of one being hacked. In this exploration I hope to answer the question of why the United States popularly uses electronic voting machines and what are the societal impacts of their widespread use. Are these machines a trustworthy and reliable tool to record the vote of United States citizens? If they are vulnerable to hacking, how vulnerable are they and does it matter?

In my thesis I plan to approach these questions in a systematic way; first I will discuss the why and how for the integration of electronic voting in the United States. Following that I will analyze the reliability and vulnerability of voting machines by examining current research about voting machines, their interfaces, and their security. Finally, with those two things in mind I will apply Actor Network Theory and Threat Modelling, a tool borrowed from cybersecurity, to analyze the potential impacts of vulnerable or unreliable voting machines on American Democracy.

Background on Voting Machines

Early in the history of the United States voting was done without aid of any computers or machinery. In the very beginning ballots were simple scraps of paper provided by the voters

(Jones, 2003). These scraps of papers allowed for a slew of problematic behaviors, and it was difficult to balance privacy of the voter and honesty of the voter as there was no good way to ensure each voter only put one paper in the ballot box without an official checking that paper (Jones, 2003). At this time there were also struggles with political parties causing confusion and chaos around the ballot. For example, in Massachusetts, political parties would often split or merge with each other and print their own ballots for the voter to use, which made it difficult to know which ballots were official and which were not (Evans, n.d). According to the L. Bird, who curated the Smithsonian's "Vote: The Machinery of Democracy" online exhibit, regulations reforming these problems were popularly passed in the 1800s and early 1900s (n.d).

We hand counted votes until the 1890s, according the MIT Election Lab ("Voting Technology", n.d.). In 1892, the first pull-lever voting machine was used in Lockport, New York (Jones, 2003). In 1896 this style of voting machine was used for the first time in a large election in Rochester, New York (Harris, 1934). These voting machines were large contraptions where the voter would step in and pull a series of levers to cast their votes (Edwards, 2004). The machines would then record the votes by incrementing mechanical counters ("Voting Technology", n.d.). These machines helped solve problems around privacy and ballot box stuffing (Jones, 2003), and sped up turnaround time for counting votes. They dropped 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 (Jones, 2003), thus beginning a new voting paradigm.

In the 1960s we developed punch card machines, which would soon be used in across the United States in conjunction with lever machines ("Voting Technology", n.d.). These punch cards would become infamous in the election of 2000, which featured a tight race, small margins

in Florida, and difficulties understanding the wishes of the voters ("Media Recount: Bush Won the 2000 Election", 2001). For my thesis I plan to further explore the election of 2000 and how it would lead to the Help America Vote Act of 2002, which banned all punch card and lever machines and ushered in the era of electronic voting ("Voting Technology", n.d.).

DRE Voting, Security, and Reliability

According to the MIT Election Lab website most states now use either electronic voting—also known as Direct Recorded Electronic (DRE) voting machines— or optical scan machines ("Voting Machines"). DRE voting machines, which are the primary focus of my thesis, are "essentially portable computers" ("Voting Machines") that allow the user to select from a list of candidates. The media has recently raised a lot of concerns around the security and reliability of such systems. Articles such as "Voting machines pose a greater threat to our elections than foreign agents" by Lulu Friesdat (2019), an opinion columnist, or "Is the Internet a threat to America's democracy?" from Louisiana Weekly's Susan Buchanan (2018) are numerous and frequent, especially as the 2020 election looms. For my thesis I plan to research the extent of the security threats to these machines as known to the public, and to try to gauge the level of access a malicious actor would have to have in order to effectively alter a machine in a negative way. I'm going to do this by researching three voting machines: the ES&S IVotronic Machine, the Sequoia AVC Edge, and the Hart InterCivic eSlate. I chose these machines because they each were used in the 2016 election ("Sequoia (Dominion) AVC Edge", n.d.; "Hart Intercivic eSlate", n.d.;"Election Systems and Software (ES&S) iVotronic, n.d.") according the Verified Voting Project, and represent a machine each from the three largest venders of voting machinery in the United States ("Ranking Members Klobuchar, Warner, Reed, and Peters Press Election Equipment Manufacturers on Security").

The ES&S IVotronic has been studied quite thoroughly via the EVEREST project in Ohio, the SAITL project in Florida, and a top-to-bottom investigation of voting machines in California. The findings of two of these studies have been summarized by Micah Scherr, who helped perform the studies, in his testimony to the West Virginia Joint Judiciary Subcommittee in regards to voting machines (2009). In his summary Scherr claimed that "[t]he results of our investigation suggest that ES&S equipment lacks the fundamental security mechanisms necessary to ensure a reliable and trustworthy election under operational conditions" (2009). He went on to describe a variety of attacks that could be performed, which included unplugging the printer to sabotage any verifiable paper trails, creating a device to access the machine and directly modify votes or vote multiple times, and modifying information stored on device peripheries by taking advantage of the poor storage of encryption keys (Scherr, 2009). There also exists an attack wherein an attacker could propagate their attack from one machine to the next, thus infecting every machine in that precinct for that election and potentially future elections (Scherr, 2009). For my thesis I plan to delve further into the EVEREST, SAITL and Top-to-Bottom reviews.

The Sequoia AVC Edge is less studied by cybersecurity experts, but has had a few issues examined. One flaw of note is the ease with which one can attack the hardware of the voting machine and that attack remain undetected. The tamper-resistant seals and locks made to prevent one from tampering with the computer components of the machine are easily circumvented, with the exception to the circuit cover seal (Appel, 2011). However, this seal is routinely broken for maintenance and to change a set of batteries housed under that cover (Appel, 2011). As such, if any individual were to perform maintenance or replace these batteries and forget to replace the seal, an attack could go undetected. Or, of equal concern, the results of an election could be

called into question as a result of that same simple mistake. Furthermore, it is possible that an attacker could simple replace the seal themselves.

Hart InterCivic's eSlate is the last machine I plan to discuss. While this machine is not free of flaws, it's the only machine thus far where an investigation resulted in expert approval (Proebstal et al, 2007). Of the vulnerabilities found, most were mitigated by the procedures followed in the county the investigation took place in (Proebstal et al, 2007). However, this does not mean that InterCivic's system is completely free of issue. Even the aforementioned investigation turned out close to a dozen vulnerabilities. As a matter of fact, a result of California's top-to-bottom review was the temporary decertification of these machines (Dunn, 2018). Possible attacks on these machines include the removing data from the device's "Mobile Ballot Box" or MBB (Butler et al, n.d), eavesdropping on voter choices (Proebstal et al, 2007), and causing the machine to print multiple barcodes, which may be used to calculate votes, by shaking it (Proebstal et al, 2007).

Conclusion and Next Steps

To generalize my research so far, DRE's are incredibly vulnerable under conditions where an attacker has a large amount of time with a machine. While this means that votes cast with these machines are subject to change or deletion, there is still a glimmer of hope. Due to the nature of access required for an attacker to carry out an attack, there are a lot of low-tech methods we can use to protect our elections. On election days we can all work together to watch for suspicious activity and report it when we see it. Cities and counties can choose to store voting machines behind locked door until elections begin and to run thorough background checks on the people who we grant extended access of the voting machines to.

For my thesis I plan to use the information I have gathered and apply Actor Network Theory to analyze a network around these machines. I will model this network around voting in Nevada, as it was the only state, according the MIT Election Lab, to use entirely DRE Voting in 2016 ("Voting Technology", n.d.).

Once I have built a network, I will use Threat Modeling, a concept from cybersecurity, to analyze how the components of that network could play into one another. I plan to apply a strategy similar to the OCTAVE-S Approach (Alberts et al, 2003) to Threat Modeling. OCTAVE-S is designed to focus on organizations' structure and non-technical aspects to security, rather than on technological weaknesses (Alberts et al, 2003), which I believe would be an ideal lens through which to view the societal aspects around voting machine security. I plan to use the network I created using Actor Network Theory to perform Phase 1 of the OCTAVE-S approach, which is to Build Asset-Based Threat Profiles (Alberts et al, 2003). This phase prompts the examiner to understand what knowledge is and isn't an asset and who has that knowledge. In the context of voting machines, I believe this could include knowledge such as where the machines are stored and how to access them in administrator mode. Next, I will perform Phase 2 of OCTAVE-S, which is to identify vulnerabilities in the system (Alberts et al, 2003). From this I hope to understand where our voting network is weak. The final phase of OCTAVE-S is to create a security plan to deal with this. I plan to skip performing this step formally. Instead, I will opt to discuss potential solutions through the lens of anticipatory governance.

Anticipatory Governance is an STS framework where the practitioner seeks to manage behaviors around a technology while management is still possible (Guston, 2014). I plan to apply this by describing certain laws which may be useful in securing our voting systems that

anticipate and protect against the vulnerabilities found in the threat model analysis. I expect many of these laws to regulate the storage and operation of voting machines, such as not allowing them to be left unattended prior to the close of an election and running background checks on individuals with a large breadth of access to the machines.

Through this analysis I expect to be able to draw conclusions about the impact that the vulnerabilities of these machines could have on an election, and by extension, on society. While I am certain these vulnerabilities are a problem, I expect that the in order to exploit vulnerabilities, there must be a flaw in our voting network which exposes these vulnerabilities. I also expect to find additional flaws in our network that leave democracy vulnerable through pathways that don't involve significant technical know-how.

References

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2003, August). Introduction to the OCTAVE Approach. Retrieved from https://resources.sei.cmu.edu/asset_files/UsersGuide/2003_012_001_51556.pdf

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

Bird, W. L. (n.d.). An interactive exhibition about historic voting in the United States.

Buchanan, S. (2018, Aug). Is the internet a threat to America's democracy? The Louisiana Weekly Retrieved from http://proxy01.its.virginia.edu/login?url=https://search-proquest-com.proxy01.its.virginia.edu/docview/2085776423?accountid=14678

Butler, K., Enck, W., Hursti, H., McLaughlin, S., Traynor, P., & McDaniel, P. (n.d.). Systemic Issues in the Hart InterCivic and Premier Voting Systems: Reflections on Project EVEREST*. Retrieved October 30, 2019, from https://www.usenix.org/legacy/event/evt08/tech/full_papers/butler/butler_html/.

Butler, K. Q., Enck, W. Q., Hursti, H. Q., McLaughlin, S. Q., Traynor, P. Q., Blaze, M. Q., … Quilter, L. EVEREST: voting system review, EVEREST: voting system review (2007). Columbus, OH: Ohio Secretary of State.

Dunn, Michael & Merkle, Laurence. (2018). Overview of Software Security Issues in Direct-Recording Electronic Voting Machines.

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/

Evans, W. (n.d.). NINETEENTH-CENTURY POLITICAL BALLOTS. Retrieved October 28,

2019, from https://cdm.bostonathenaeum.org/digital/collection/p16057coll29.

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

Friesdat, L. (2019, October 4). Voting machines pose a greater threat to our elections than foreign agents. Retrieved October 26, 2019, from https://thehill.com/opinion/technology/464065-voting-machines-pose-a-greater-threat-to-our-elections-than-foreign-agents.

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

Hart Intercivic eSlate. n.d. Retrieved October 27, 2019, from https://www.verifiedvoting.org/resources/voting-equipment/hart-intercivic/eslate/.

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

Media Recount: Bush Won the 2000 Election. (2001, April 3). Retrieved from https://www.pbs.org/newshour/nation/media-jan-june01-recount_04-03.

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.

Ranking Members Klobuchar, Warner, Reed, and Peters Press Election Equipment Manufacturers on Security. (2019, March 27). Retrieved October 25, 2019, from

https://www.klobuchar.senate.gov/public/index.cfm/news-releases?ID=CB7B78C2-5313-4FA2-AB83-B4A7C85201F9.

Scherr, M. (n.d.). Testimony to West Virginia Joint Judiciary Subcommittee. Charleston, WV.

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

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

Identyti Perspectus

Introduction:

For our technical capstone we are working with Identyti, a Darden School of Business start-up seeking to change the way the world shares and receives identification documents. Currently, most identification documents (Drivers License, Passport, Insurance card, etc) are handled as strictly hard copies, and the process for getting those documents can be difficult. While there are currently some ways to verify the validity of someone's drivers' license online, those are predominately used for the sale of alcohol and other restricted substances and not for any official government identification (Larson, 2019). This means that people must keep hard copies of these documents and all the documents they need to apply for them, which can be burdensome. One could digitize their own documents, but that leads to another problem; there is no system designed for digital storage of sensitive personal documents. WIRED magazine recently published a "Guide to Your Personal Data (and Who Is Using It)" in which they detailed how companies like Google are collecting and storing every click and keystroke made in their web browser, store this data along with user identities, and use it to serve targeted ads to the users (Matsakis, 2019). In other words, major document storage companies (Google, Dropbox) collect data on their users and leverage that data for capital gain. Storing private documents on those servers makes users vulnerable.

System Design:

Identyti seeks to help users keep their private documents private, and to make everyone's life a little bit easier. Our deliverable to them will be a proof-of-concept showing documents that can be stored securely on the internet, which they'll use when meeting with investors and potential

stakeholders to garner support for this technology. As such, the fundamental goal of our project is to build a document storage service that is secure, easy to navigate, and allows users to access the product on mobile and desktop devices. Users should be able to upload, view, and download their documents on demand. We also want this product to support enterprise accounts which can issue personal documents and tell users what they need to have to apply for such documents.

Because the documents uploaded to this platform is typically highly sensitive, data security will be a critical challenge to tackle. Login authentication would be performed by Auth0 which already provides an array of mitigating web-app security breaches such as anomaly detection and force email verification (Poza 2018). Additionally, in order to allow clients to access their data from anywhere, the documents they upload will be stored in the cloud, specifically in an AWS S3 bucket. When uploading the documents, the application will save certain metadata associated with the document allowing the client to easily search/sort/categorize the document, making it convenient and faster to find it later. The International Data Corporation, who is a provider of market intelligence, conducted a study on their workers to gauge how much time they spend weekly looking for physical documents. In a group of 1200 workers, IDC found that “they spend an average of 4.5 hours a week looking for documents” (Biddle, 2017). Since Identyti is targeted at both consumers and enterprise clients alike, searching for these documents on Identyti, whether the client is an individual or a business, will be much faster than searching for physical documents.

One concern for storing sensitive data in the cloud is that these services can be compromised. However, in order to mitigate this issue, the plan is to encrypt the data stored in S3, so that even if the bucket is compromised, only encrypted data can be recovered. By storing

these encrypted files in the cloud, Identyti offers a secure and fast solution for clients, allowing them to easily share their documents with enterprises.

Identyti also provides benefits for enterprise clients. A major problem that large enterprises face is the sheer size of information they have to process and handle. Using Identyti, enterprises have the ability to create an account in order to manage all of their employees' data. For example, when onboarding a new employee, an enterprise client could request the necessary documents, such as identification and tax reports, from the new employee through Identyti. In this way, Identyti creates a secure and simple path of communication between enterprises and employees for personal, confidential documents. Instead of requiring users to carry physical documents and submit them to enterprises, Identyti creates a channel to share these documents electronically.

System Requirements:

To fulfill our goals we've identified these requirements:

Minimum

- As a user, I should be able to create a customer account, so that I can access persisted data.
- As a user, I should be able to login to my account, so that I can access persisted data.
- As a user, I would like to be able to upload my documents, so that I can store them for future use.
- As a user, I would like my documents to be stored, so that I can access them for future use.
- As a user, I should be able to view my documents, so that I feel confident my documents are stored.

- As a user, I would only like my documents to be accessed by those I have authorized, so that I feel confident in the security of my personal information.
- As a user, I would like to be able to easily locate my documents, so that I can find what I need when I need it.
- As a user, I should be able to retrieve my documents, so that I can use them when I need them.
- As a user, I should be able to access the application from a mobile device, so that I can upload or share documents on the go.

Desired

- As a user, I would like to be able to search for my documents, so that I can easily find documents when I need them.
- As a user, I would like different options for sorting and filtering my documents, so that I can easily find relevant documents when I need them.
- As a user, I would like the app to recognize what type of document (driver's license, birth certificate, etc) I am uploading, so that it is easy for me to organize and find my documents later.
- As a user, I should be able to create an enterprise account.
- As a user I should be able to authorize other users to view my documents, so that I can provide my documents when necessary.
- As an enterprise client, I should be able to request documents from other users, so that I can validate their identity and provide access to appropriate resources.

Optional

- As a user I should be able to limit the time another user can view my document.
- As an enterprise client, I should be able to create a new type of document with a list of required documents needed.
- As a user, I should be able to identify which required documents I am missing.
- As a user I should be able to delete my documents.
- As an admin, I should not be able to view user's documents.

Works Cited

Biddle, P. (2017, July 26). *Productivity, Lost Time, and the Power of AI to Make Search Easier.* Retrieved from Medium: https://medium.com/@diamond_io/productivity-lost-time-and-the-power-of-ai-to-make-search-easier-a59d4cd85a26

Larson, G. (2019). *Verifying Identity In Today's Digital Economy: A Look At Regulated Retail.* Retrieved from Forbes: https://www.forbes.com/sites/forbestechcouncil/2019/09/06/verifying-identity-in-todays-digital-economy-a-look-at-regulated-retail/#24546f551e62

Matsakis, L. (2019). *The WIRED Guide to Your Personal Data (and Who Is Using It).* Retrieved from WIRED: https://www.wired.com/story/wired-guide-personal-data-collection/

Poza, D. (2018, July 19). *How Auth0 Makes Your Apps More Secure.* Retrieved November 20, 2019, from Auth0: https://auth0.com/blog/how-auth0-makes-your-apps-more-secur