Deliverable 0

Team Members: Levi Hagan, Richard Marshall and Hannah Posch

Our sources have been divided between three categories based on what the source describes and how the source will help us as we move forward to tackle the project this semester.

Security

Security is a huge problem in the modern world which is the reason we chose to explore specific references that describe the security problems associated with electronic voting. Source [3] is useful to our project design and implementation as the authors take a very detailed look into the cryptology and security behind a voting system. The authors discuss what will most likely get attacked by a hacker and the security issues that can arise with an electronic system. Publication [3] is also useful because the authors look at the software engineering side of the voting system and the coding style and process that may be used. Source [3] will be very helpful to the team as we tackle the larger issues of security and what to expect should a hacker get a hold of our system as these cases may not necessarily be what we expect.

Article [5] begins by explaining Estonia's place in the tech world, and also it's potential vulnerability to hacking due to its reliance on electronic infrastructure. It goes on to briefly discuss a cyber attack used against the country in 2007 which was thought to be committed by Russia, though the evidence is circumstantial. The article goes on to explain through an interview that Estonia is using an internet voting system. The interview goes on to describe how the e-voting system works in its general use and how they address some basic security concerns. It goes on to talk about the concern of potential Russian attempts to hack their upcoming elections in 2019.

Article [6] recounts a Russian cyber attack on the staff of the member of the Democratic party during her campaign. While there is no information on the success of this attack, the author does make mention of the same sort of attack's success during the 2016 presidential campaign. They also make mention of phishing attempts made against three candidates in the ongoing midterm campaigns. Talking with an expert in the field who previously worked on the pentagon's cyber defense team, [6] explains that there were likely more attacks or attempts that went undetected. It goes on to explain some of the issues with securing an election, as campaigns and elections usually bring on new or volunteer staff without experience. Finally, it makes mention of two factor authentication as a potential way to mitigate such phishing attempts.

Article [7] begins by explaining that despite the odd political climate surrounding the elections, US intelligence has gathered quite a bit of evidence on the extent of Russian hacking and interference in the 2016 election. The first point the author brings is the disinformation and 'fake news' campaign Russia launched against US social media. It goes on to explain they breached the Democratic party as well as a number of state agencies and county. According to [7], the attacks have not ceased either. The author then goes on to explain that most states have not taken steps to address current security concerns with their voting system, not replacing old machines or updating software. Additionally, with the lack of audits to attempt to recognize tampering, [7] suggests more interference is likely to occur in coming elections.

Article [9] talks about Florida's annual Hackathon DEFCON and how thirty children ages 8 to 16 were able to hack into replicas of Florida's state election site and change everything form candidate names to the election results. Article [9] states that the replicas they created for the event were in many ways tougher to access the real sites. This has drawn concern form the public, however the Florida's legislative has giving little acknowledgment to the results of the event. The organizers of DEFCON are hoping the results of the hackathon will show the public the real threat of voter interference.

Article [10] talks about smartphone voting. [10] then talks about the tech company, Voatz, a startup company that has designed a voting app for smartphones and the app is now going to be available for West Virginia voters serving overseas. [10] explains the app has come with huge backlash from security analyst and the public alike with the ongoing Russian election interference news. Several security architects have been mortally critiquing the app from its "out-of-date encryption and authentication service" to its poor UI. Showing that with recent events and security concerns mobile voting is not the best course of action.

Performance

This category of sources reveal many performance issues and real-life scenarios describing the reliability of electronic voting. Reference [2] contributes to the project as it breaks down the process of voting and the issues associated with electronic voting. The author, Ted Selker, highlights the problems with inaccurate voting results and how they stemmed from the use of electronic voting and databases. Selker notes different events, in which the electronic voting did not go according to plan and the problems that occurred. The publication [2] is useful for this project as it highlights the problems we could potentially run in to and the most common issues faced with voting. Reference [2] is useful as we tackle our requirements and can use the realistic scenarios to test with.

Usability, Functionality

Usability and functionality are two vital portions of creating successful software which is the reason we chose to find sources that contribute to understanding these two categories in relation to electronic voting. Source [1] contributes to the project as it outlines the typical user interface for the South Carolina voter system, and illustrates the order in which the user would cast their vote. Publication [1] illustrates the production requirements that are listed in the assignment and shows how they could be implemented via the traditional voting system. The South Carolina Election Commission outlines the messages the user would receive as they vote and updates should they choose to return to a different menu. The South Carolina Election Commission also describes a user writing in a name to vote, rather than specifically choosing from a list, which is more than the functional requirement calls for, but could make the voting experience more realistic.

Reference [4] describes in greater detail many of the requirements needed for this assignment. The author, Ghassan Qadah, organizes the requirements into diagrams and images which will be especially helpful in our design phase as a team. Reference [4] also describes how to work on a database for the voting system and the Oracle and Microsoft tools that were used for that specific portion of the system. The database is a medium to low requirement, but should definitely be considered through the design process, which makes this source useful. Qadah also provides a great glossary for us to study and work from as we begin this project without a previous background in voting system creation and will allow for better communication to complete the requirements.

Article [8] by Dion Lefler talks about how poor design of voter software caused issues during the Kansas governor election back in August. The system was not properly designed to handle more than four candidates. With twelve candidates running, having to flip through displays of four candidates was described as “confusing” and “annoying” by many voters. Article [8] continues by stating the company who designed the software would have a patch ready for the software by Tuesday's primary and plans to do further patches if the need arises. Source [8] is helpful by showing a possible problem that could have arisen in our software and to design software that is easy to use.

References

[1]South Carolina Election Commission, "1-2-3 Vote How To Use South Carolina's Voting System", *Dc.statelibrary.sc.gov*, 2016. [Online]. Available: https://dc.statelibrary.sc.gov/bitstream/handle/10827/23145/ELE_1-2-3_Vote_2016.pdf?sequence=1&isAllowed=y. [Accessed: 26- Aug- 2018]

[2]T. Selker, "Fixing the Vote", *Scientific American*, vol. 291, no. 4, pp. 90-97, 2004.

[3]T. Kohno, A. Stubblefield, A. Rubin and D. Wallach, "Analysis of an Electronic Voting System", *Johns Hopkins University Information Security Institute Technical Report*, pp. 21-23, 2018 [Online]. Available: http://avirubin.com/vote.pdf. [Accessed: 26- Aug- 2018]

[4]G. Qadah, *Requirements, Design and Implementation of an e-Voting System*. American University of Sharjah, 2018, p. 5 [Online]. Available: https://pdfs.semanticscholar.org/5c68/de8ebe21c7457e23a2bf1b9289326f52c3d5.pdf. [Accessed: 27- Aug- 2018]

[5] M. F. Callejon, “Estonia a test case for Russian hacking threat,” Global Journalist, 02-Nov-2017. [Online]. Available: https://globaljournalist.org/2017/11/estonia-test-case-for-russian-hacking-threat/. [Accessed: 29-Aug-2018].

[6]M. Parks, “Russian Hackers Targeted The Most Vulnerable Part Of U.S. Elections. Again,” *NPR*, 28-Jul-2018. [Online]. Available: https://www.npr.org/2018/07/28/633056819/russian-hackers-targeted-the-most-vulnerable-part-of-u-s-elections-again. [Accessed: 29-Aug-2018].

[7]M. Matishak, A. Restuccia, L. Nelson, E. Geller, S. Issenberg, T. Alberta, B. Bender, and J. Shafer, “What we know about Russia's election hacking,” *About Us*, 19-Jul-2018. [Online]. Available: https://www.politico.com/story/2018/07/18/russia-election-hacking-trump-putin-698087. [Accessed: 29-Aug-2018].

[8]D. Lefler, "Software issue is confusing voters in election for Kansas governor", *Kansas*, 2018. [Online]. Available:

https://www.kansas.com/news/politics-government/election/article215991065.html. [Accessed: 28- Aug- 2018]

[9]M. Regan and M. Regan, "An 11-year-old changed election results on a replica Florida state website in under 10 minutes", *PBS NewsHour*, 2018. [Online]. Available: https://www.pbs.org/newshour/nation/an-11-year-old-changed-election-results-on-a-replica-florida-state-website-in-under-10-minutes. [Accessed: 28- Aug- 2018]

[10]M. Kosoff, "“A Horrifically Bad Idea”: Smartphone Voting Is Coming, Just in Time for the Midterms", *The Hive*, 2018. [Online]. Available: https://www.vanityfair.com/news/2018/08/smartphone-voting-is-coming-just-in-time-for-midterms-voatz. [Accessed: 29- Aug- 2018]