Innovation of Cyber Defense Technologies with Data Collection and Analysis

How have past cyberattacks affected how different social groups use and interact with software technology today?

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
School of Engineering and Applied Science
University of Virginia
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By
Michael Kosar

October 27, 2022

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.

ADVISORS

Rider Foley, Department of Engineering and Society

Rosanne Vrugtman, Department of Computer Science

Introduction:

People have become increasingly reliant on digital systems. This increasing reliance has led to an increase in cyber vulnerabilities throughout the world as more people switch to digital systems to store information. This is where nefarious actors and groups attempt to take advantage of flaws in software design for their own personal gain. Some of the largest and most damaging attacks in recent history include cyberattacks on the Colonial Pipeline, the Ukraine power grid, and the WannaCry ransomware attack (Atkins, 2022). The groups behind these attacks can be anyone from a person in their basement to a criminal syndicate sponsored by a foreign government. Their intentions are often malevolent and can be motivated by money, political power, or personal espionage. An often overlooked group involved in cyberattacks are called “certified hackers", or whitehat hackers. This social group does not carry out cyberattacks with a malevolent goal, but instead with the goal of preventing future attacks by penetration testing (Slayton, 2018). These different social groups can have either an adverse or beneficial effect on technology depending on their objective..

Whoever the actor is and whatever their purpose is, they can cause major damage to society and how we function. This is why major corporations and governments have begun to put an emphasis on cybersecurity and making sure their systems and information are safe. The reason why this is such a tough problem to solve is because of the vast ways of infiltrating software systems. Some basic methods include DDos, phishing, sniffing, and root-ware attacks. Among these attacks, there are various delivery methods such as trojan horses and viruses (Chapman, Leblanc, & Partington, 2011). These methods are improving everyday and there is constantly new malware and methods of delivery that appear. The reason for these vulnerabilities in software is because of the software designers themselves. Around 60% of vulnerabilities in code are due to the developers lack of careful development and maintenance. This is because developers allow security to take a back seat due to high customer pressure and demand to deliver features and requirements quickly (Larios-Vargas et al., 2022).

In order to solve these issues posed by hacker groups and new malware, we must look back at real world examples of these attacks and their effect on society. This will allow us to develop methods based on past experience and knowledge that will enable us to detect and prevent future attacks. In order to get a real world example of the efforts being made in cybersecurity, I will be writing my technical topic about my past internship with the U.S. Air-Force where they tasked me with determining a method to categorize radio-frequency interference in the X-band so that they could better identify and deter any potential adversarial threats to their software and hardware systems. I will then be discussing in my research paper how past cyberattacks have affected how software developers design and create software systems today. I will use Pinch and Bijker's Social Construction of Technology framework to frame this research topic and analyze it from a societal standpoint. The increasing threat of cyberattacks have led me to not only research their effect on society and the technology we build, but also get directly involved in the fight against them through my technical internship.

Technical Topic

I took part in an internship over the summer of 2021 with the National Security Innovation Network's X-Force. In today's world, there is a large effort, especially in our government, to determine how we can effectively analyze, acknowledge, and prevent cyberattacks before they occur. With cyberattacks on the rise, the biggest issue for companies is security issues and ease of access for cyberattacks, according to the Cyber Security Challenges

Model (Khan et al., 2022). In addition to the private sector, the federal government is having similar issues. The majority of the United States Air-Force's technologies rely on radar and transmission data. Typical aircraft have around 180 touch points across several networks as well as a variety of onboard processors (Maybury, 2015). This makes them prone to cyberattacks and interference from adversaries which is why they are putting a large effort into securing their systems and finding ways to identify threats before they occur. In partnership with the U.S. Air-force, I was tasked with designing a way to be able to identify the difference between normal, everyday radio-waves that are harmless to defense systems and the malicious adversarial radio-waves being sent by potential adversaries to disrupt communications. Specifically, I was tasked with doing this in the X-band, which is a band of frequencies typically from 8-12 GHz. This is the band in which radar, satellite communication, and wireless computer networks operate on. I was given large sets of raw data from real world military training scenarios that contained transmissions picked up by radar systems during the exercise. Using this data, I created a Python computer program using the NumPy library that combed through these large data sets, and separated the data into various categories based on the level of the frequency, the length of the transmission, and other outside factors such as altitude and location. These factors were used because they all play a role in determining if the disruption is a potentially malicious one. The program then compiles these data sets into a physical chart of various threat levels based on a sorting algorithm that uses the categorical determinations made previously. The chart consists of 5 different threat levels with Tier 5 being the highest threat level, indicating an active threat that could be catastrophic to the software system. Tier 1 is the lowest and indicates the transmission is a passive, everyday transmission such as a civilian radio communication. These levels can then be used by future software systems to detect the threat level of an incoming radio transmission. This program helps alleviate the problem of confusing radio interference and allows for quick identification and threat analysis of these frequencies.

The consequences of cyberattacks can include internal chaos, widespread disruption in the administration of the country, severe damage to the national economy, and many others (Li & Liu, 2021). This is why making sure that we evolve and learn from our past mistakes and flaws can help save money and lives in the future. In order to describe the human and social dimensions of this project, I will use the social construction of technology to help bridge our understanding of how social groups can help influence technology.

STS Topic

As the world moves toward more complete reliance on digital technology, the importance of ensuring its safety and security is becoming more important than ever. Cyberattacks have become extremely prevalent and have affected almost every aspect of the technology we use daily. They affect aviation, banking, defense, energy, water, power, and many other sectors of society. All of which have had prominent attacks to learn from (Malik et al., 2022). A major reason for developing a way to characterize radio-frequency interference, as I did in my internship, is because it allows the Air-Force to intercept and deter cyberattacks that use signal interference. Pinch and Bijker's social construction of technology (SCOT) will be used to analyze the effects of cyberattacks and the social groups behind them on software that we use today. SCOT is a framework that analyzes how different social groups in society have affected the construction, design, and implementation of various technologies. The first step in SCOT analysis is demonstrating that the technology is culturally constructed and interpreted. The second step is mapping mechanisms for the stabilization of an artifact. The third and final step is describing technologies by focusing on the meanings given to them by social groups (Pinch & Bijker, 1984). To relate these steps and framework to the issue of cybersecurity, we can analyze how various social groups of hackers, through cyberattacks, have influenced how software developers design and construct software today. To do this, I must first define these various social groups. The term ‘hacker’ was originally used to describe someone who explored the full-range of capabilities of themselves and their machine but it has since become a term for someone who deliberately attempts to undermine and infiltrate another person or company’s computer system for their own gain (Kleen, 2001). Using this definition as well as Kleen’s article, we can define various social groups of hackers that will be discussed in the paper. When a cyberattack is carried out, there is an immediate effect on society. This effect, which is almost always a negative one, prompts various companies and government agencies to spring into action and find ways to prevent these attacks and their consequences in the future. This leads to various bills, laws, regulations, and design implementations that are put forth to mitigate the threat of another attack as well as for political gain (Cavelty & Egloff, 2019). The federal and state governments have both taken responsibility to enforce stronger cybersecurity by passing bills such as California’s Notice of Security Breach Act and the federal government’s 2002 Homeland Security Act (Srinivas, Das, & Kumar, 2019). Another example would be the Strengthening American Cybersecurity Act which was passed following the Colonial Pipeline attacks (Serwin, Meshulam, & Javanshir, 2022). These regulations and implementations affect how software developers are able to design their software which in turn affects the users. Finally, I will discuss how cyberattacks are designed to affect human behavior by causing chaos and confusion. This in turn affects how users interact with technology and, subsequently, how software developers design their systems by being more cautious and conscious when securing their product (Cayirci & Ghergherehchi, 2011).

Research Questions and Methods

The research question that I will be analyzing is, how have past cyberattacks affected how different social groups use and interact with software technology today? This is an important question because cyberattacks have become very prevalent in today's society and preventing them is at the front of all software developers' agendas. Companies are even making software developers complete mandatory cybersecurity training to improve their skills (Gasiba, Beckers, Suppan, & Rezabek, 2019). Analyzing how past events have shaped our current methods will allow software developers to develop a clearer picture of why they do what they do and how they can improve it in the future. I will research this question by analyzing various case studies that cover past cyberattacks as well as how they impacted society. A few relevant case studies that will be covered are the recent Colonial Pipeline cyberattack (Mello, 2022) as well as the 2014 North Korean cyberattack on Sony Pictures (DeSimone & Horton, 2018). These will give us an insight into both foreign and domestic attacks. Another area to analyze is critical infrastructure such as ports which are constantly attacked (Ahokas, Kiiski, Malmsten, & Ojala, 2017). Using these case studies, I will collect data on past attacks and, specifically, data on who the attacker was, their motive, how they infiltrated their target, and what the consequences of the attack were. This data will allow me to analyze different types of hackers and their motives as well as their methods and the societal implications of various types of attacks. Among the data, I will also include the laws and regulations passed as a result of attacks. This data allows us to view how software development techniques and procedures have changed over time to adapt and adjust to these attacks.

Conclusion

There has been an increase in cyberattacks across the world due to the rise of technology in everyday life. These attacks affect every aspect of society and can change the way we function with some arguing that the psychological effects of cyberattacks can rival those of traditional terrorist attacks (Gross, Canetti, & Vashdi, 2016). If we can better understand how past attacks have affected us from a societal perspective, we will be better able to predict and deter future attacks. This allows society to put more trust in technology and function without the worry of everything coming to a standstill. I expect the results of this research paper to show that there is a direct connection between cyberattacks in the past and improved software security. I hope this will provide similar insight to Rahman's framework for predicting cyberattacks (Rahman, Al-Saggaf, & Zia, 2020). This will enable us to move forward as a society and ensure we have a safe, and secure future in technology.

References

Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L. (2017). Cybersecurity in ports: A conceptual approach. *Proceedings of the Hamburg International Conference of Logistics (HICL)*, *23*, 343-359. doi:10.15480/882.1448

Atkins, H. (2022, March 24). The Biggest Cyberattacks in History. Retrieved September 25, 2022, from https://www.historyhit.com/the-biggest-cyberattacks-in-history/

Cayirci, E., & Ghergherehchi, R. (2011). Modeling cyber attacks and their effects on decision process. *Proceedings of the 2011 Winter Simulation Conference (WSC)*. doi:10.1109/wsc.2011.6147970

Cavelty, M. D., & Egloff, F. (2019, June 20). The Politics of Cybersecurity: Balancing Different Roles of the States. *St Antony's International Review, 15 (1),* 37-57.

Chapman, I., Leblanc, S., & Partington, A. (2011). Taxonomy of Cyber Attacks and Simulation of Their Effects. *Proceedings of the 2011 Military Modeling & Simulation Symposium (MMS '11)* . doi:10.5555/2048558.2048569

DeSimone, A., & Horton, N. (2018). Sony's nightmare before christmas: The 2014 North Korean cyber attack on Sony and Lessons for US Government Actions in Cyberspace. Retrieved October 17, 2022, from https://www.jhuapl.edu/Content/documents/SonyNightmareBeforeChristmas.pdf

Gasiba, T. E., Beckers, K., Suppan, S., & Rezabek, F. (2019). On the requirements for serious games geared towards software developers in the industry. *2019 IEEE 27th International Requirements Engineering Conference (RE)*. doi:10.1109/re.2019.00038

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists, 72*(5), 284-291. doi:10.1080/00963402.2016.1216502

Mello, J. P., Jr. (2022, June 07). How the Colonial Pipeline Attack has changed cybersecurity. Retrieved October 27, 2022, from https://www.csoonline.com/article/3662776/how-the-colonial-pipeline-attack-has-changed-cybersecurity.html#:~:text=Another%20government%20reaction%20to%20the,ransomware%20payments%20within%2024%20hours

Pinch, T. J., & Bijker, W. E. (1984). The social construction of facts and artefacts: Or how the sociology of science and the Sociology of Technology might benefit each other. *Social Studies of Science, 14*(3), 399-441. doi:10.1177/030631284014003004

Khan, A. W., Zaib, S., Khan, F., Tarimer, I., Seo, J. T., & Shin, J. (2022, June 02). Analyzing and evaluating critical cyber security challenges faced by vendor organizations in software development: SLR Based Approach. *IEEE Access, 10*, 65044-65054. doi:10.1109/access.2022.3179822

Kleen, L. J. (2001). Malicious hackers: A framework for analysis and case study. Retrieved October 27, 2022, from https://scholar.afit.edu/etd/4646/

Larios-Vargas, E., Elazhary, O., Yousefi, S., Lowlind, D., Vliek, M., & Storey, M. (2022, May 24). DASP: A framework for driving the adoption of software security practices. doi:10.48550/arXiv.2205.12388

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments. *Energy Reports, 7*, 8176-8186. doi:10.1016/j.egyr.2021.08.126

Malik, A. W., Abid, A., Farooq, S., Abid, I., Nawaz, N. A., & Ishaq, K. (2022). Cyber threats: Taxonomy, impact, policies, and way forward. *KSII Transactions on Internet and Information Systems, 16*(7). doi:10.3837/tiis.2022.07.017

Maybury, M. (2015). Toward the assured cyberspace advantage: Air force cyber vision 2025. *IEEE Security & Privacy, 13*(1), 49-56. doi:10.1109/msp.2013.135

Rahman, M. A., Al-Saggaf, Y., & Zia, T. (2020). A data mining framework to predict cyber attack for cyber security. *2020 15th IEEE Conference on Industrial Electronics and Applications (ICIEA)*. doi:10.1109/iciea48937.2020.9248225

Serwin, A., Meshulam, D., & Javanshir, L. (2022, March 14). US Senate unanimously passes the strengthening American Cybersecurity Act: Insights: DLA piper global law firm. Retrieved September 25, 2022, from https://www.dlapiper.com/en/us/insights/publications/2022/03/us-senate-unanimously-passes-the-strengthening-american-cybersecurity-act/gi

Slayton, R. (2018). Certifying "ethical hackers". *ACM SIGCAS Computers and Society, 47*(4), 145-150. doi:10.1145/3243141.3243156

Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in Cyber Security: Framework, standards and recommendations. *Future Generation Computer Systems, 92*, 178-188. doi:10.1016/j.future.2018.09.063