Interval Scheduling Maximization in Mobile Ordering
(Technical Paper)

Cybersecurity Infrastructure Status in the United States
(STS Paper)

A Thesis 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

Peng Zhang
Fall, 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

Introduction

The United States is the most targeted country for cyberattacks, experiencing 156 "significant" cyberattacks between May 2006 and June 2020, followed by 47 in the United Kingdom ("The Countries Experiencing," 2020). In the United States, there are 16 critical infrastructure sectors whose assets, systems, and networks are essential to such a severe degree that the loss of these sectors would be catastrophic to security, economic security, and public health or safety on a national scale ("Critical Infrastructure Sectors," n.d.). This list consists of the following: chemical sector, commercial facilities sector, communications sector, critical manufacturing sector, dams sector, defense industrial base sector, emergency services sector, energy sector, financial services sector, food and agriculture sector, government facilities sector, healthcare and public health sector, information technology sector, nuclear reactors, materials, and waste sector, transportation systems sector, and the water/wastewater systems sector. With the digitization of society on a global scale, the cybersecurity industry continues to grow in prominence and has already established itself as a necessity to maintain privacy and security. The first proposed project will examine cybersecurity systems within the critical infrastructure sectors of the United States in order to analyze cybersecurity infrastructure within the nation as a whole.

The second proposed project will utilize computer science to address problems that have appeared in the restaurant and food retail service industry during the COVID-19 pandemic. COVID-19 has drastically changed the way society functions, causing many businesses to transition to remote operations to maintain safety. Many restaurants have been detrimentally impacted by the regulations, as there have been over 1,500 chain restaurant locations that have been permanently closed and 12 restaurant chains that have filed for bankruptcy (Jiang & Stone,

2020). Fast food chains have experienced different results, as consumer trends have shown that customers are purchasing more quantities per order, and that both drive-throughs and digital sales are thriving (Valinsky, 2020). Additionally, 48.5% of restaurant consumer spending was off-premises, through carry-out, delivery, and drive-through (Paril, 2020). However, the surge of mobile ordering has produced increased wait times, which can be addressed by proper time estimation and algorithmic scheduling.

Technical Topic

Many businesses experienced the worst financial impact of COVID during March of 2020, whereas drive-through visits increased by 43% (Davityan, 2020). Studies show that the average waiting time to receive a fast food order increased from 2019 by nearly 30 seconds to 356.8 seconds, and that "knowing when an order will be ready" is an important factor for the customer experience (Davityan, 2020). Frustrations with mobile ordering are evident in the local Charlottesville area, as recent reviews of fast food restaurants such as Chipotle have observed waiting times that have ranged from 30-90 minutes past estimated times.

The hypothetical deliverable attempts to alleviate these frustrations by introducing algorithmic scheduling to mobile ordering. Interval scheduling is a way to algorithmically consider the time it takes to complete tasks and determine a schedule to execute as many tasks as possible. Maximizing the tasks completed through interval scheduling can be classified as a "greedy algorithm," because it attempts to find the optimal solution by selecting the locally optimal choice during each iteration (Moore, Khim, Ross, n.d.). In the technical deliverable each task will represent a fast food order, and the tasks will be programmatically represented by the time interval that is the estimated time to complete all items in the order added to the time that

the order was received. Schedules will be created by picking tasks with the earliest finishing time and overlapping tasks will be updated to reflect the current schedule. Following the schedule that is created to fulfill orders will algorithmically decrease average waiting time for fast food orders, while also addressing the customer pain of not knowing an accurate estimate for when their order will be ready.

STS Topic

When COVID-19 began to spread globally cybercriminal attacks preyed on the public desire for more information. COVID-themed cyber attacks rapidly surged as nations attempted to restrict the physical spread of the virus ("Exploiting a crisis," 2020). During the 2016 presidential election, the computer network of the Democratic National Committee was breached by Russian cyberespionage groups, leading to the leakage of stolen information (Lipton, Sanger, Shane, 2016). Leading up to the 2020 presidential election, Microsoft has observed cyberattacks targeting both people and organizations involved with the opposing campaigns, by groups from Russia, China, and Iran (Burt, 2020). It is clear from cyberattacks against both the public and political organizations that a national cybersecurity infrastructure is essential to maintain societal security.

The healthcare and public health sector has been directly impacted by the COVID-19 pandemic both physically and virtually. Hospitals across the nation are experiencing numerous shortages, including personal protective equipment, drugs, and staffing (McLernon). This pressure also increases the impact of virtual vulnerabilities, as shown by the cyberattack against Universal Health Services, which compromised its computer systems (Collier, 2020). As a major hospital chain, this attack forced hospitals to file patient information by hand, immensely

slowing down operations. Cyberattacks like this also disable essential hardware, directly putting lives at risk.

The state of national security and safety is maintained by the relationships between government agencies, industry businesses, and citizens, as well as the health and data of all these entities. Due to the complexity involving each critical infrastructure sector and the network that they maintain with the public, the STS theory for analysis is the Actor-Network Theory (ANT).

ANT focuses on the interaction of actors to effect social processes. An important distinction is that actors are a "source of action regardless of its status as a human or non-human," which explores the agency of inanimate objects (Cresswell, 2010). Examination of actors is conducted through the consideration of networks, which consists of actors acting in combination with each other. ANT allows the scale of each actor and network to be contextually based, and it emphasizes the development of these networks. The importance of each actor within a network parallels the importance of critical infrastructure sectors in the United States. ANT assumes that if any actor is added or removed, that the whole network will be affected (Cresswell, 2010). Similarly, if any critical infrastructure sector experiences a change, there could be drastic effects to the state of the nation as a whole.

The concept of generalized symmetry is used in ANT to associate equally important roles to human and non-human components in these networks. Generalized symmetry provokes one criticism of ANT, that the theory does not incorporate pre-existing factors such as power imbalances into its networks. Furthermore, ANT has been criticized for the implication that all actors hold equal importance in the network (Criticism, 2010). ANT has also been criticized to be amoral. However, it has been argued that morality and political views can be applied, but the context of the network must be defined first (Criticism, 2010). The STS deliverable will combat

these criticisms by clearly defining the role and importance of actors within respective networks, in addition to emphasizing the context of morality in sectors such as the healthcare and public health sector.

Research Question

The research question being investigated is: What is the state of existing cybersecurity infrastructure in the United States? Data collection for this investigation involves gauging existing cybersecurity infrastructure, in addition to recent cybercriminal activity. Analysis will be done by examining existing implementations of cybersecurity infrastructure and procedural plans in critical infrastructure sectors. Analysis will then be conducted on cybercriminal activity in recent events, specifically with regards to targeted attacks against individuals or organizations within specific critical infrastructure sectors. By looking at current infrastructure for vulnerabilities and combining this with analysis of cyberattack trends in recent months, conclusions can be made on the state of cybersecurity infrastructure within the United States.

Conclusion

Coinciding with the technological development of numerous industries is the necessity to reinforce these technologies with cybersecurity foundations. With the sudden arrival of the COVID-19 virus and the radical changes it has made to societal and industrial practices, the technical deliverable of this project presents a solution to ameliorate customer frustrations that have grown in the food retail service industry. The STS deliverable will provide a thorough analysis of current United States cybersecurity infrastructure. Analysis of existing infrastructure

and practices in response to recent cybercriminal events will reveal current vulnerabilities and areas of improvement for cybersecurity infrastructure.

References

Burt, T. (2020, September 10). New cyberattacks targeting U.S. elections. *Microsoft on the Issues*. https://blogs.microsoft.com/on-the-issues/2020/09/10/cyberattacks-us-elections-trump-biden/

Collier, K. (2020, September 11). *Cyberattack hits major hospital system, possibly one of the largest in U.S. history*. NBC News. https://www.nbcnews.com/tech/security/cyberattack-hits-major-u-s-hospital-system-n1241254

Cresswell, K. M., Worth, A., & Sheikh, A. (2010). Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare. BMC Medical Informatics and Decision Making, 10(1), 67. https://doi.org/10.1186/1472-6947-10-67

Critical Infrastructure Sectors. (n.d.). Retrieved November 2, 2020, from https://www.cisa.gov/critical-infrastructure-sectors

Criticism of Actor-Network Theory. (2010, January 1). https://island94.org/2010/01/Criticism-of-Actor-Network-Theory.html

Davityan, E. (2020, November 6). Is mobile solving the wait-time problem for restaurant brands? Www.Pizzamarketplace.Com. https://www.pizzamarketplace.com/blogs/is-mobile-solving-the-wait-time-problem-for-restaurant-brands/

Davityan, E. (2020, March). Responding to COVID-19: Fast Food Focuses on Drive Thru, Pickup. QSR Magazine. https://www.qsrmagazine.com/outside-insights/responding-covid-19-fast-food-focuses-drive-thru-pickup

Exploiting a crisis: How cybercriminals behaved during the outbreak—Microsoft Security. (2020, June 16). https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/

Jiang, I., & Stone, M. (n.d.). 12 restaurant chains have filed for bankruptcy in 2020 in the wake of the pandemic. See the full list. Business Insider. Retrieved December 2, 2020, from https://www.businessinsider.com/8-restaurant-chains-that-have-filed-for-bankruptcy-during-pandemic-2020-9

Lipton, E., Sanger, D., & Shane, S. (n.d.). *The Perfect Weapon: How Russian Cyberpower Invaded the U.S. - The New York Times*. Retrieved November 2, 2020, from https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html

McLernon, L. (n.d.). COVID-related nursing shortages hit hospitals nationwide. CIDRAP. Retrieved December 2, 2020, from https://www.cidrap.umn.edu/news-perspective/2020/11/covid-related-nursing-shortages-hit-hospitals-nationwide

Moore, K., Khim, J., & Ross, E. (n.d.). Greedy Algorithms | Brilliant Math & Science Wiki. Retrieved December 2, 2020, from https://brilliant.org/wiki/greedy-algorithm/

Paril, B. (2020, July 14). 2020 Trends: QSR During COVID-19. Digital Remedy. https://www.digitalremedy.com/2020-trends-qsr-during-covid-19/

The countries experiencing the most 'significant' cyber-attacks. (2020, July 9). https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/

Valinsky, J. (n.d.). 5 ways the coronavirus changed how we eat fast food. CNN. Retrieved December 2, 2020, from https://www.cnn.com/2020/08/01/business/fast-food-coronavirus-habits/index.html