Trust and Security of Advanced Logistics Systems with Embedded Smart Devices
(Technical Paper)

Security and Privacy Implications of Public Wi-Fi and Bluetooth Connectivity
(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

Beatrice E. Li
Fall, 2020

Technical Project Team Members
Rahman O. Adekunle
Andrew T. Koch
Mai N. Luu
Chris M. VanYe

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

By 2023, the number of public Wi-Fi hotspots, globally, will increase four times the number in 2018 (*Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper*, 2020). In addition, people, from Generation X to Gen Z, are connected to their devices more than ever before. Technology usage has also seen a surge during the Covid-19 pandemic as people find themselves unable to attend in-person events and stay at home more than normal. The STS research focuses on the increasing risks posed to user privacy and security associated with the internet and Bluetooth connectivity that go unaddressed. Users tend to perceive themselves as safer than they actually are as they connect to open networks without a second thought, which "exposes themselves – knowingly or unknowingly - to security and privacy risks" (Sombatruang et al., 2016). Smart devices have become so integrated with people's lives to the extent to which phones contain almost everything there is to know about a person and perhaps even more. Though people are quick to express their concern over data privacy and security, it is often not supported by the appropriate actions. The concern and respective actions offer the opportunity to assess the public's understanding of open networks and its influence on data privacy and security.

On a similar note of trust and security risk with technology, assessments of the defense supply chain have proved an infiltration of counterfeit electronic components, which poses a critical threat to national security (U. S. Government Accountability Office, 2016). The capstone proposal centers around the growing need to assess the trust and security of embedded hardware and embedded systems within the military and industry supply chains. For Systems Planning and Analysis, Inc. (SPA), this would mean to minimize the risk associated with the deployment of fully functioning hypersonic glide bodies in the acquisition of hypersonic aviation technologies.

Likewise, Fermata LLC needs to realize the potential security and privacy risks in implementing a bidirectional charger network and assess the resilience of a power grid that supports electric vehicle charging. The risk of the systems requires a thorough assessment of success criteria and the risk associated with the systems along with disruptive scenarios. The research team will perform the same analysis for the Commonwealth Center for Advanced Logistics (CCALS) to address Internet of Things (IoT) devices in logistic systems. The final technical deliverable, excel spreadsheets utilizing scenario analysis, will identify and rank the success criteria with respect to the disruptive scenarios and initiatives when proceeding with the respective systems' development and production.

Technical – Trust and Security of Hardware and Embedded Smart Devices

The Center for Hardware and Embedded Systems Security and Trust (CHEST) is an Industry-University Cooperative Research Center (IUCRC) funded by the National Science Foundation (NSF). CHEST strives to address the research challenges that industry and government partners face concerning trust, security, and assurance for electronic hardware and embedded systems through the coordination of university-based research (*CHEST*, 2020). The following projects are part of the efforts to meet the needs of the industry and government sponsors under CHEST. The respective industry sponsors are SPA, Fermata and CCALS, each with their own research and Excel workbooks that apply scenario analysis to the respective topic. The approach to the capstone will be a combination of established resources and publications combined with new ideas from the research group headed by the capstone advisor and Systems Engineering Professor, James Lambert. Contributions are also made by Dr. Zachary A. Collier, Thomas L. Polmateer, Mark C. Manasco, Negin Moghadasi, and Kelsey A. Hollenback. The resulting deliverables will be completed by the end of the Fall 2020 semester with presentations to involved sponsors and documented in a SIEDS paper, in April 2021.

Research and Development Priorities of Hypersonic Glide Bodies

One of the industry sponsors, Systems Planning and Analysis Inc. (SPA), is a defense contracting company that provides acquisition support for the interested parties of the Department of Defense (DOD) concerning the DOD's conventional prompt global strike program (CPGS). The purpose of the CPGS program is to "bolster U.S. efforts to deter and defeat adversaries by allowing the United States to attack high-value targets or 'fleeting targets' at the start of or during a conflict" (Woolf, 2020). As the United States is left further behind in the research and development of hypersonic technologies compared to other countries, such as China and Russia, urgency and support for the CPGS program has been growing (Woolf, 2020). The lack of capabilities places the United States in a position of disadvantage, which could dictate the nature of future international relations. In recent years, the program's efforts have shifted to hypersonic technologies, the ability to fly at speeds that are at least five times the speed of sound – defined as Mach 5. Hypersonic technologies, or weapons, in this case, are divided into two categories – hypersonic glide vehicles and hypersonic cruise missiles. The interest of SPA's acquisition support lies within hypersonic glide vehicles, also known as hypersonic glide bodies (HGB), which are launched to the appropriate altitude with a rocket before gliding to the designated target (Sayler, 2020). Though the term "glide" suggests it to be uncontrollable, it actually refers to the absence of a rocket motor on hypersonic glide bodies; they can maneuver in flight, but that is not without its challenges. When working with such a complex system, there are many scenarios and challenges that have yet to be addressed but crucial to the deployment of the technology. The capstone team will analyze literature that pertains to the subject of hypersonic technology and the challenges related to the system. The team will then produce a scenario analysis of potential conditions that can affect the success of the system, which is the deployment of the hypersonic glide bodies.

With the focus on the deployment of a fully functioning hypersonic glide body, the performance of the HGB is evaluated through a variety of metrics describing it from the moment of deployment to the moment of impact. With the scenario analysis approach, success criteria are not the only aspect to be considered but also initiatives, emergent conditions, and their respective relationships. As this project is partially sponsored by SPA, the team will provide the scenario analysis to guide SPA in understanding which scenarios to focus on and plan for in the deployment of the hypersonic glide bodies.

Research and Development Priorities of the Bidirectional Charger Network

Another industry sponsor, Fermata LLC., is the national leader in proven vehicle to building (V2B) and vehicle to grid (V2G) systems. As electric vehicles (EV) become more popular than conventional vehicles, so does the need for forward-thinking about how the power grid needs to handle the increased stress of powering all the buildings and infrastructures in an area and the growing need for extra electricity in cars. More specifically, the project's primary goals are to find potential risks to the research and development of a bidirectional charger network and to assess the resilience of a power grid that supports electric vehicle charging. Bidirectional charging allows electric vehicle owners to get paid to give power back to the grid during times of grid stress. The means that EV owners can use their cars as extra power banks for the grid while they are not in use and can substantially help out the grid (Almutairi et al., 2018).

Existing literature will guide the previous understanding of work in the topic areas and provide previous success metrics in evaluation of the system. Data like surveys, fault trees, and initiative charts will be essential in giving the group a good idea of where the direction of electric vehicle charging is going (Andrews et al., 2020). A spreadsheet outlining the success criteria for the system, along with initiatives and potential emergent conditions, will be produced for Fermata to better understand potential situations of risk that the company might encounter in the development of a bidirectional charger.

IoT Devices in Logistics Systems

The Commonwealth Center for Advanced Logistic Systems (CCALS) is an applied research center that brings Universities and companies together to perform analysis on rapidly growing technologies in the IoT sphere. The interest of CCALS lies in the trust and security of IoT devices in logistics systems, which is the basis of the research for SPA and Fermata. The generated scenario analysis for SPA and Fermata can be generalized to fit the scenario analysis for CCALS.

STS Topic

Technology has advanced greatly in recent years, but cyber-attacks have also grown increased in frequency without much concern from the general public. Not only do public Wi-Fi networks number to hundreds of millions today, but are projected to grow even more along with the number of Internet of Things (IoT) connections in the coming years (*Cisco Annual Internet Report - Cisco Annual Internet Report (2018–2023) White Paper*, 2020). Internet of Things (IoT) refers to the network of connected devices that communicate with each other through a cloud network while being connected to the internet ("Understanding the Differences," 2020). The most well-known IoT devices include the Amazon Echo and smart locks; however, smartphones are generally not considered as IoT devices since they are expected to connect to the internet. With the development of IoT devices, there is also a growth in privacy and security concerns.

When it comes to day-to-day usage, the trust that consumers place is not only on the internet providers of the network, but also in their devices from smartphones to cars. Under the current conditions of the Covid-19 pandemic, the need for the use of public Wi-Fi has grown more urgent, significantly more so with users that cannot afford it at home (Stewart, 2020). The reduction of public networks could create other problems with a potential scenario being users who cannot do work otherwise. Cyberattacks can allow hackers to steal and utilize users' data for their benefit, which tend to be malicious (Agrafiotis et al., 2018). The concern is not on the attacks necessarily as hackers attack about every 39 seconds based on a study at the University of Maryland (*Study: Hackers Attack Every 39 Seconds*, 2007). Public Wi-Fi networks are not the only open networks that people should be concerned about but rather all open networks, including IoT, due to the numerous unaddressed security risks. Open networks will be defined as any typical connection that involves the internet, which is to say that it is unsecured as most typical connections are.

Given the nature of open networks, Actor-Network Theory (ANT) will be used in addressing the topic as it aids in understanding complex relationships. The theory is especially useful in its application to open networks compared to other sociotechnical approaches as it considers both human and non-human actors equally (Cressman, 2009). The consideration of non-human actors is valuable, but that is also the basis of several criticisms in that non-human actors should not be considered of equal importance to human actors as it also may not always be the case. ANT focuses on the study of the associations between actors by also working to define the actors within the system without assuming the size of the network (Cressman, 2009). In the study of associations, or relationships, between actors, networks can be assessed in how they can become more robust and which associations add power to the network. However, there is a flaw in that there is no boundary or stopping point of when to stop adding actors to the network. There are more advantages than disadvantages in the application of ANT as the associations between actors can reveal the impact of user knowledge in open networks.

The primary stakeholders are the users, that are divided into many categories, such as students, workers, or leisure users. Users utilize many services and protocols to protect their data and privacy, where it is up to the users to take measures to implement them. Aside from the users, it is essential to recognize that day-to-day IoT devices such as cars to smart-home hubs and smartphones are within this system and should be considered. Open networks between devices offer increased efficiency, and the extent of the efficiency depends on the users' needs or desires. The users' understanding of open networks can be influenced by the engineers behind the devices and brand marketing; thus, the people behind the devices should be considered as stakeholders. The research can contribute significantly to security and data protection in today's age, where data is everything, and people live on open connections.

Methodologies

Research Question: How does the public understanding of open networks contribute to the safety and security of those networks?

In order to answer this research question, the concept of open networks needs to be defined and provided. The definition of open networks and the research question will be answered through a literature review that will also include policy analysis. The compilation of secondary sources will be based on the following list of keywords: Internet of Things (IoT), cybersecurity, Wi-Fi, security, user awareness, data protection, and risk. The list of keywords is used as they are closely associated with the topic of the question. The literature will include research into user behavior and the security risk associated with the different open networks. The use of the literature review will provide context and clarity of the technical concepts. The compilation of literature bridges gaps that may be present in some of the research. Policy analysis will fall under the literature review as the sources will include discussion of legislation, especially those related to consumers' data privacy. The methods utilized will address the complexities of open networks and the impact of public understanding in the pursuance of the research question.

Conclusion

This paper explores the sociotechnical impacts of unsecured connections between devices, specifically exploring the security and privacy implications of using unsecured connections. Despite the increase of connections, most of which are unsecured, the average user does not implement any methods to ensure security and privacy. The proposed STS research examines how public understanding of open networks impacts the safety and security of those networks. The STS deliverable will lend itself to understand how more user knowledge and preparedness will contribute to the safety and security of open networks.

On a related note of safety and security, the three industry sponsors, SPA, Fermata and CCALS, are interested in the trust and security of their respective systems. The technical deliverables will be Excel workbooks, implementing scenario analysis for SPA, Fermata, and CCALS to identify each system's research and development priorities. The technical deliverables will advance knowledge of trust, security, and trust for electronic hardware and embedded systems while identifying risk reduction countermeasures. It is imperative for concerns related to not just national security, but individual security as well, to be addressed especially with the progression of technology.

References

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *0*(0), 15.

Almutairi, A., Thorisson, H., Wheeler, J. P., Slutzky, D. L., & Lambert, J. H. (2018). Scenario-Based Preferences in Development of Advanced Mobile Grid Services and a Bidirectional Charger Network. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering*, *4*(2), 04018017. https://doi.org/10.1061/AJRUA6.0000962

Andrews, D. J., Polmateer, T. L., Wheeler, J. P., Slutzky, D. L., & Lambert, J. H. (2020). Enterprise Risk and Resilience of Electric-Vehicle Charging Infrastructure and the Future Mobile Power Grid. *Current Sustainable/Renewable Energy Reports*, *7*(1), 9–15. https://doi.org/10.1007/s40518-020-00144-6

Center for Hardware and Embedded Systems Security and Trust. (2020). Center for Hardware and Embedded Systems Security and Trust. http://nsfchest.org/

Cisco Annual Internet Report—Cisco Annual Internet Report (2018–2023) White Paper. (2020, March 9). Cisco. https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Cressman, D. (2009). *A Brief Overview of Actor-Network Theory: Punctualization, Heterogeneous Engineering & Translation*. https://collab.its.virginia.edu/access/content/group/6ac8ef1f-6b15-4912-a488-d8c7468046db/Readings/Cressman%20-%20Overview%20of%20ANT.pdf

Sayler, K. M. (2020). *Hypersonic Weapons: Background and Issues for Congress*. 26.

Sombatruang, N., Sasse, A., & Baddeley, M. (2016). *Why Do People Use Unsecure Public Wi-Fi? An Investigation of Behaviour and Factors Driving Decisions*. 72. https://doi.org/10.1145/3046055.3046058

Stewart, E. (2020, September 10). *Give everybody the internet*. Vox. https://www.vox.com/recode/2020/9/10/21426810/internet-access-covid-19-chattanooga-municipal-broadband-fcc

Study: Hackers Attack Every 39 Seconds. (2007, February 9). https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

U. S. Government Accountability Office. (2016). *Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk. GAO-16-236*. https://www.gao.gov/products/GAO-16-236

Understanding the Differences: M2M vs. IoT. (2020, May 7). *IoT For All*. https://www.iotforall.com/m2m-vs-iot-understanding-the-differences

Woolf, A. F. (2020). *Conventional Prompt Global Strike and Long Range Ballistic Missiles: Background and Issues*. 54.