Designing a IoT Device Security Course

(Technical Topic)

Developing a Universal Standard to Create Safe IoT Devices

(STS Topic)

A Thesis Project Prospectus Submitted to the

Faculty of the School of Engineering and Applied Science

University of Virginia * Charlottesville, VA

In Partial Fulfillment of the Requirements of the Degree

Bachelor of Science, School of Engineering

Ryan Lenfant

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

Signature: Ryan Lenfant

I. Introduction

Given the recent boom in popularity of Internet of Things (IoT) devices, it is extremely important to develop devices that are safe for consumers to use. These devices are so popular that "there were an estimated 12.5 billion IoT devices, almost twice as much as the world's population of 6.8 billion" (Sirvaraman et al. 2018). Due to the sheer variety and vast amount of IoT devices, it is imperative to invest in more security, so a user's valuable information is not stolen. As Zheng et al. (2018) claims, consumers do not understand the security risks of owning IoT devices and expect manufacturers to put the proper protections in place to ensure their devices are safe. This emphasizes the importance of making security a priority when developing any technological device. If we keep our current mindset of producing devices without focusing on the security of the user, our homes will become more vulnerable to hackers as time goes on. As Oka et al. 2014 claims, new technology coming out is extremely susceptible to exploits as the technology is so new, emphasizing why it is so important to focus on safety in the development stage. To improve the climate of trying to focus on profits to the ethically safe IoT devices, a system of "cyber hygiene" must be taught to those that develop and use these devices (Oravec 2017). This would include educating a user on the security features of the devices they use, constantly updating devices to have the most secure software, and forcing the user to change their password regularly. Although cyber hygiene will help ensure a user's safety, it is of utmost importance to establish ethical standards for creating IoT devices to maintain this safety. Having ethical standards will allow all devices to be on the same strong level of security, preventing networks from being exploited by one vulnerable device.

II. Designing a IoT Device Security Course

One effective way to establish the importance of security in IoT devices and teach people how to defend against vulnerabilities is to create a course focusing on the defense of IoT devices. This course would be a combination of the Computer Architecture course and the Intro to Cybersecurity course. As it combines two fundamental courses regarding device hardware and software security, the new course would teach students about the hardware in an IoT device that can be exploited leading to a device being hacked, the fundamentals of how IoT devices connect and communicate with each other, and case studies to learn about previous exploits and how to prevent them. This would give students a foundation in how these systems work as well as prepare them for real world scenarios.

There are endless amounts of ways a hacker can exploit a vulnerable device, so it is important for students to understand the scope of a vulnerability to address the vulnerability the correct way. For example, one form of communication between IoT systems that is commonly used is Bluetooth. Although Bluetooth has been around for a while, it is not always a protected feature (Oka et al. 2014). Hackers can utilize Bluetooth to connect and gain control of a particular device without prompting the user. As something so commonly used such as Bluetooth can be taken advantage of, it is important to comprehend how vulnerable the device is using the Common Vulnerability Scoring System (CVSS) created by Mell et al. (2006). This standard gives cybersecurity researchers the ability to quantify the amount of security in a device, allowing them and students to understand what makes a device vulnerable.

A major problem in most computer sciences curriculums is the lack of IoT security courses at most colleges, giving students less of a chance to learn about the dangers associated with owning an IoT device. Due to this lack of classes, most colleges do not require students to take any course associated with cybersecurity. As students lack the requirement of taking a cybersecurity

course, they are not able to develop a security mindset. Developing this security mindset helps students develop products that are safe to users and think about the impact of their device on society and their coding ability (Bratus et al. 2010). This further emphasizing the importance of developing an effective IoT security course, as students can become better programmers and put security first when working on a project.

By failing to address the importance of device security through an effective IoT course, manufacturers will have a continued focus on developing the most profitable IoT devices instead of focusing on the security of the device. Users will continue to perceive that the developers oversee all security issues and fail to check if the device is safe and secure (Zheng et al. 2018). Devices will continue to include security features that the user must manually set up instead of focusing on automatically setting up safety features. Without the information conveyed in an effective course, people will continue to unintentionally allow hackers access to their important personal information which could cost them a lot of money.

In developing an effective course, I will be combining my knowledge of cybersecurity and computer architecture to teach students the ethical standards one should think about when developing an IoT device. The course will have a syllabus modeled after the one created by Gal-Ezer & Harel (1999) and a lab section where students can apply the tools they learn in class. The course will teach three main topics to give students a good foundation of cybersecurity. Firstly, in the labs, students will hack into vulnerable IoT devices and explore how to prevent these using different protections taught in the course. Secondly, students will learn how IoT devices communicate with each other to grasp the different pieces of technology within a device and how they work. Finally, the course will also take a deep dive into previous exploits so students can understand how the security of technology is constantly changing and understand how to prevent

these events from happening again. Developing a course on IoT Device Security will allow students to learn a security mindset to protect against future attacks.

III. Developing a Universal Standard to Create Safe IoT Devices

Establishing new standards allows society to grow and develop around issues that are happening in the present. Given the importance of standards, there exist many universal systems for classifying vulnerabilities and scoring the danger of vulnerabilities but not for developing safe and secure IoT devices (Mell et al. 2006). As this technology is so commonly used, society must develop new ethical standards to address the rapid growth of IoT devices that are not secure. This will force device manufacturers to have a security mindset when designing and producing new technology while also ensuring a consumer's safety. Producing standards to address cybersecurity concerns allows researchers and developers to have a common focus when addressing concerns with IoT.

Addressing the issue of vulnerable IoT issues is exceedingly difficult since each IoT device is different in terms of how it is created, how it communicates with other devices, and with which devices it communicates. Although these may make it hard to make a standard of security for each device, there are still some basic ethical standards that can be put in place to protect a user. Emphasizing the importance of enforcing security, Meneghello et al. (2019) suggest that security is an integral part to developing IoT devices and should not be ignored by developers.

As stated in the technical topic section, users perceive that developers oversee all security issues and do not often check to see if the device is secure (Zheng 2018). Devices often include security features for users to set up, however these are can be hidden/complicated for the user when they purchase the device causing them to not set up these secure features. This poses a

problem as user's devices are not the most secure when they come out of the box. Owning one device of these devices that lacks basic security in a network is extremely harmful to device owners as it can lead to more secure devices becoming exploited. As we can see from Figure 1 below, each IoT device is connected to each other in some from or another making them inherently more vulnerable if a device in the network is more vulnerable. This is due to a lack of cyber hygiene in device owners who use the same login/password for their devices making it easy for a hacker who gets into one device to get into more secure devices within the network (Oravec 2017). Creating ethical standards which reflect on how to implement cyber hygiene into IoT allows manufacturers to create safer devices and consumers to feel/be safe and secure.

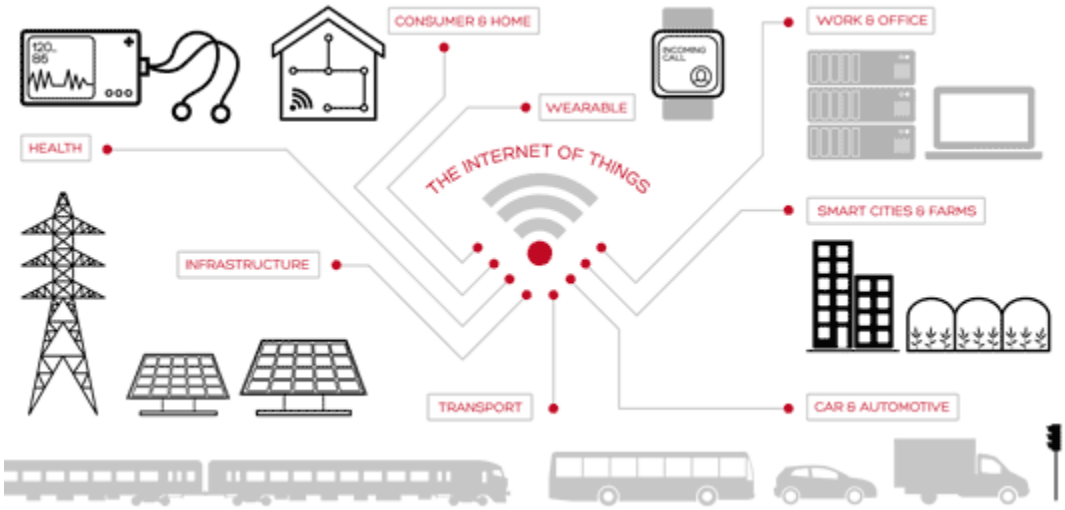

Figure 1. IoT devices are all connected making it extremely important to establish safe devices to make all other devices are protected (*Internet of Things*, 2019)

How can we establish safer IoT devices while also giving consumers the best possible experience in terms of setting up and easily using their device? By looking at the work of Meneghello et al. we can understand how a network of devices can be impacted by one weak link and come to the conclusion that there must be some sort of ethical standard to ensure

network safety. Using the Actor Network Theory, we can see what actors, or devices in this case, impact the integrity of a user's home network and define strict standards to manufacturers which they can incorporate into their devices. A lot of research must be conducted on different home networks and devices to come up with the general factors that make a device secure. If there is no intensive prior research done before establishing ethical standards, the devices produced could become more vulnerable, causing harm to the people who own and manufacture the devices. Setting the precedence of ensuring device security will allow society to become safer from hackers while also increasing the trust between manufacturers and consumers.

IV. Overall Conclusion

Although IoT devices are becoming more mainstream, proper security practices surrounding the devices are still widely ignored or unknown to by users. To combat this lack of knowledge and make IoT devices generally safer, I am planning on creating lectures which will have examples of previous exploits and explain different terminology that students must know before they are able to understand the exploits. There will be labs which involve students performing progressively harder IoT devices so they can understand the different ways a hacker can attack a device. These deliverables will push to establish some sort of ethical standards for developing secure IoT devices and lead to the creation of a new course at UVA that will teach students how to hack and the ethics of hacking IoT devices.

References

Bratus, S., Shubina, A., & Locasto, M. E. (2010, March). Teaching the principles of the hacker curriculum to undergraduates. In *Proceedings of the 41st ACM technical symposium on Computer science education* (pp. 122-126).

Gal-Ezer, J., & Harel, D. (1999). Curriculum and course syllabi for a high-school CS program. *Computer Science Education*, *9*(2), 114-147.

Internet of Things. (2019). Retrieved November 02, 2020, from https://www.nccgroup.com/uk/your-sectors/internet-of-things/

Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy*, *4*(6), 85-89.

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, *6*(5), 8182-8201.

Oka, D. K., Furue, T., Langenhop, L., & Nishimura, T. (2014, November). Survey of vehicle IoT bluetooth devices. In *2014 IEEE 7th international conference on service-oriented computing and applications* (pp. 260-264). IEEE.

Oravec, J. A. (2017, July). Emerging "cyber hygiene" practices for the Internet of Things (IoT): professional issues in consulting clients and educating users on IoT privacy and security. In *2017 IEEE International Professional Communication Conference (ProComm)* (pp. 1-5). IEEE.

Payne, J., Budhraja, K., & Kundu, A. (2019, July). How secure is your iot network?. In *2019 IEEE*

Sivaraman, V., Gharakheili, H. H., Fernandes, C., Clark, N., & Karliychuk, T. (2018). Smart IoT devices in the home: Security and privacy implications. *IEEE Technology and Society Magazine*, *37*(2), 71-79.

Sivaraman, V., Gharakheili, H. H., Vishwanath, A., Boreli, R., & Mehani, O. (2015, October). Network-level security and privacy control for smart-home IoT devices. In *2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob)* (pp. 163-167). IEEE.

Vlajic, N., & Zhou, D. (2018). IoT as a land of opportunity for DDoS hackers. *Computer*, *51*(7), 26-34.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-20.