Creation of Multitiered Access System
(Technical Paper)

Vulnerabilities in Internet of Things Devices
(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 for the Degree
Bachelor of Science, School of Engineering

Arthur Given

November 2021

Technical Project Team Members
Derek Martin
John Chrosniak
Jamison Stevens

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 _____ Date_____
Arthur Given

Approved _____ Date_____
Harry Powell, Department of Electrical and Computer Engineering

Approved _____ Date_____
Richard D. Jacques, Department of Engineering and Society

Introduction

In recent years, the term “porch piracy” has become a household name to describe the theft of packages that have been delivered outside of someone’s home. This can occur when packages are delivered during the workday and the homeowner does not have a chance to bring them inside immediately. According to CNBC in 2019, one in three Americans had been the victim of porch piracy at least once (Martino, 2019). This article was written in 2019, and ecommerce has only increased since then. In another article written by CNBC in April 2020, it was noted that ecommerce had increased by 30 percent since the beginning of the coronavirus pandemic (Rattner, 2020**).** In addition, the coronavirus pandemic has increased the use of noncontact deliveries, allowing more opportunities for thieves to steal packages from porches before they can be brought inside.

For my technical project I (along with my capstone group of Derek Martin, John Chrosniak, and Jamison Stevens) will be designing a locking system that allows a homeowner to generate single use codes to give to delivery drivers that will allow them to deliver packages inside a home or to a package box. The general purpose is to give delivery drivers limited access to an area not accessible by the public. In addition, the system will have a camera that records the actions of a delivery driver to ensure that they themselves do not steal the package while they have access to the pack box or home.

Technical Discussion

In this project, my team and I are hoping to develop a system that will greatly reduce the amount of porch piracy by making it significantly harder for a thief (or a malicious driver) to steal a package that was delivered with contactless delivery. My team and I are working under the supervision of Professors Avik Ghosh, Todd Delong, and Harry Powell of the ECE department in a semester long capstone project. Our goal is to have a working prototype by the end of the semester, through computer aided printed circuit board design, embedded C coding on a Raspberry Pi, and the development of python web application.

Currently, there are many products that attempt to solve this problem. These include Ring Doorbell and Amazon Key. Ring Doorbell is a doorbell with a camera that allows a homeowner to view live and recorded footage of their front porch. This allows the homeowner to see when packages are delivered as well as when they are stolen. The main issue with the Ring is that it does not provide any significant barriers that stop potential thieves from taking a package. The thief will be recorded, but if they cover their face, it is hard to identify who took the package. Amazon Key is service very similar to the system we intend to build. It places a smart lock on the front door of a house that an amazon driver can open. However, Amazon Key does not include a camera, so it is up to the homeowner to safeguard against potential malicious delivery drivers. Amazon Key also only works for amazon delivery services. One Washington post journalist expressed their discomfort with the product as a way for Amazon to work its way even more into people’s lives (Fowler, 2019). Our hope is to develop a product that can be integrated with most delivery services, offering protection for the homeowner and a decrease in liability for the delivery services.

The prototype that is being developed is known as the bouncer locking system. The physical pieces of the bouncer include an electric strike that regulates access to a package box, a keypad for password inputs, a video camera, and a Raspberry Pi to analyze user input and operate the peripheral devices. The electric strike can be mounted in many places including a doorjamb, but a package box was selected for our prototype for simplicity. When a user enters a code into the keypad, the Raspberry Pi determines whether or not the code is valid. If that code is valid, the Pi operates the electric strike, allowing the user to open the door of the package box, and turns on the camera, recording the actions of the user. Once the user has closed and relocked the box or the recording has exceeded the allotted time, the Raspberry Pi will upload the camera footage along with the time the lock was opened and which code was used to a cloud service platform. Using a web application, the product owner access to every current valid code as well as the ability to modify or cancel the codes. The owner also has access to the footage from every code that has been used to open the lock.

The locking system will also allow for the creation of codes that are not single use, but are only valid for specific windows of time. This provides another use case for the product in which homeowners may give individuals, such as an Airbnb guest access to a house or any space secured by the locking system. This allows for quick turnaround between guests, ensuring that old guests do not have access after they check out without the need to send someone to reprogram a lock in person or exchange keys.

The central goal of this project is to create a tiered access locking system in which a trusted administrator has full access to the system and can easily control who else has access and for how long they have access. By the end of the semester my team will have a working prototype, which allows an administrator to perform the tasks outlined above.

STS Discussion

Porch piracy is an ongoing phenomenon which can affect every homeowner. The low barriers for theft allow anyone to simply take a package because they want to. In 2020 Americans lost 5.4 billion dollars to porch piracy (Asymkos, 2020). As discussed previously, there are already many products on the market that attempt to solve this problem. Both of the products discussed in addition to the prototype that I hope to develop involve Internet of Things (IoT) devices. In 2018, it was estimated that there would be 20.4 Billion IoT devices connected to the internet by 2020 as compared to the roughly 11 Billion devices at the time (Griffiths, 2019). These IoT devices provide convenience or smart home features for the owners, such as a smart fridge's ability to be controlled from a phone or Ring Doorbell's live camera feed. Amazon Alexa can be connected to a multitude of devices that allow a user to control countless devices in a home such as lights, blinds, and locks. But, these features present a serious risk to security. For my STS research I hope to explore how the vulnerabilities of IoT devices and smart devices affect their users and the outside world as well as how these vulnerabilities can be mitigated.

Many of these smart devices are insecure and can easily have control taken by hackers. Having IoT devices controlled by a malicious user is arguably more dangerous than a traditional

PC because IoT devices are specifically designed to interact with and possibly cause physical change in the world around them opening the door for loss of property and life (Schneier, 2018). There is very little incentive for manufacturers of IoT devices to make their devices secure. Monetary incentives are especially low, since most consumers are unaware of the security risks that these devices create and no federal law currently exists requiring IoT devices for general consumer use to meet any security standards (Schneier, 2018). The IoT Cybersecurity Improvement Act of 2020 does provide some security standards, but only for which devices can be used by government agencies. This does not require manufacturers of home devices to change make their systems more secure, which still leaves many people open to cyber-attack.

The obvious question that emerges from this is "How do we ensure that these smart devices are secure enough?" While, Increasing the regulations placed on microcontroller based smart devices worldwide could lead to improved security for all users (Schneier, 2018), the designers of smart devices should be asking themselves other questions. Designers and manufacturers need to balance their own financial interests with the global need for a more secure IoT. All designers need to recognize that, while an insecure device presents a security risk to the user and their property, it also creates security risks for the entire world. Unsecure IoT devices can be incorporated into large groups of hacked devices called botnets. These botnets are made up of computers that are remotely controlled by a malicious actor and can be used for various malicious purposes. In 2016, the Mirai botnet used approximately 600,000 IoT devices to execute a distributed denial of service attack which took large portions of the US internet offline (Griffiths, 2019). The fact that these botnets can threaten anyone should have designers asking how smart do smart devices need to be? How do we ensure functionality of an IoT device without leaving it vulnerable? Cyber security involves a tradeoff between usability and security. A device that has been disconnected from all computer networks and is stored in a locked room is very secure, but practically unusable. Currently IoT designers are creating very usable devices, but are making very few tradeoffs for security.

Conclusion

The world is still searching for a definitive solution to the problem that is porch piracy, and many of the products on the market that attempt to solve this problem are IoT devices. My capstone team is currently developing our own IoT device that we hope will provide a safe and easy solution to the problem. However, we have been careful throughout development and need to continue to be careful to consider how design decisions affect the security of our system. Especially given that our system is made for security, we have been attempting to use practices and design methodologies that are accepted as secure in both cyber space and physical space. In addition, I hope to much further explore the ethical issues relating to the security of IoT systems and how it can be improved with minimal effects to device usability.

Citations

Asymkos, S. (n.d.). *Americans lost $5.4 billion in stolen packages this year, survey finds*. Yahoo! Retrieved October 16, 2021, from https://www.yahoo.com/now/americans-lose-54-billion-in-stolen-packages-213320756.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAGtsrP5IGD-_ZIVJqFHFmqhFLtnc6wtS-INchgyaa81s2cTyi78ddYhQJt6A4Z1yPrFmt5qL8TMxtAzZG8il3Juc77leTOe2mYb7HFNeuj-IZIUY4706SpBzxdgYetssQxjiZDPOkkX5KMPX9KjVeudfavk3pyaATsOrkYOe8_UR.

Fowler, G. (2019, April 8). *Review | Amazon wants a key to your house. I did it. I regretted it.* The Washington Post. Retrieved October 16, 2021, from https://www.washingtonpost.com/news/the-switch/wp/2017/12/07/amazon-wants-a-key-to-your-house-i-did-it-i-regretted-it/.

Martino, D. (2019, December 13). *Over a third of Americans are victims of 'porch pirates.' how not to become a statistic*. CNBC. Retrieved October 16, 2021, from https://www.cnbc.com/2019/12/13/over-a-third-of-americans-are-porch-pirate-victims-dont-become-one.html.

Rattner, N. (2020, June 10). *As coronavirus restrictions drag on, Americans shift online spending from stockpiling to entertainment*. CNBC. Retrieved October 16, 2021, from https://www.cnbc.com/2020/04/19/coronavirus-what-americans-are-buying-online-while-in-quarantine.html.

Griffiths, J. (2019). *Internet of things: Japan to hack millions of web ... - CNN*. cnn.com. Retrieved November 1, 2021, from https://www.cnn.com/2019/02/01/asia/japan-hacking-cybersecurity-iot-intl/index.html.

Schneier, B. (2018). *We need stronger cybersecurity laws for the internet ... - CNNBruce*. Cnn.com. Retrieved November 1, 2021, from https://www.cnn.com/2018/11/09/opinions/cybersecurity-laws-internet-of-things-schneier/index.html.