Thesis Portfolio

Designing a Lock and Home Security System to Prevent Porch Package Theft

(Technical Report)

How Engineers Should Design IoT Devices for Security

(STS Research Paper)

An Undergraduate Thesis

Presented to 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

Derek Martin
Spring, 2022

Department of Electrical and Computer Engineering

Portfolio Table of Contents

Sociotechnical Synthesis

Derek Martin

For our technical project, my capstone team designed and created an electronic locking system that connects to the Internet to allow for password management. Although not the focus of the project, we have put careful effort into making the device secure and resistant to cyberattacks. My research paper was very closely related as I investigated how to design IoT devices, similar to my capstone project, to be more secure.

The technical portion of my thesis produced a package lock box to combat porch package theft. The system consists of an electronic lock and an external keypad connected to a microcontroller that communicates over the Internet to an AWS database that also communicates with a website. The website is designed for passcode management and allows the owner to generate or delete new passcodes. These passcodes get hashed, and the hashes are stored in the AWS database, which gets read by the microcontroller. What is unique to this system compared with other electronic locking systems is that my technical project allows for single use passcodes with dynamic updates, which allows the system to delete passcodes from the database after they have been entered. This allows the owner to issue a passcode to a delivery driver and ensure that the package box is secure after the package has been delivered. Another unique feature of my technical project is a dual power supply that runs on rechargeable batters and wall power. This allows the device to operate normally and recharge the batteries when power is on and prevents the device from shutting off in the event of a power outage.

In my STS research, I investigated how engineers can design IoT devices for security. In doing so, I developed a set of guidelines for engineers to follow as they design. Engineers must take accountability for problems that may occur by actively restring what the user can do. Engineers must never allow for universal default passwords and instead should assign cryptographically secure pseudorandom passwords or require user-generated passwords to be secure. Engineers must store and distribute passwords encrypted and protect user data in the strongest way available. Engineers must anticipate misuse and poor security practices by users and put in place additional security measures to mitigate harm caused by these actions. Finally, engineers must follow the strictest set of laws and regulations for all their products, regardless of whether the laws apply to all customers or not.

My technical project enriched my STS research by providing me with firsthand experience and exposure to the field of IoT design. I was also faced with many of the challenging tradeoffs between resource management, time management, and system security that I investigated in my research. My research improved upon my technical project by allowing me to evaluate the design decisions made by my group and determine mistakes we made and issues we overlooked. The combination of these two projects allowed me to understand how I can approach design in my own personal projects to increase security, as well as how engineers can better protect their users and consequently raise the bar for cybersecurity across the world.