Designing an Effective IoT Security Course

(Technical Report)

The Struggle over Data Collection from IoT Devices in American Households

(STS Research Paper)

An Undergraduate Thesis Portfolio
Presented to the Faculty of the
School of Engineering and Applied Science
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Major

by

Eric Sakmyster

May 7, 2021

Preface

IoT devices pose a user privacy risk from hackers and tech companies. Because IoT is in early development, it lacks standards that would protect users. These projects seek to build trust between the public and tech companies that data privacy is of foremost importance.

Given their popularity, Internet of Things (IoT) devices and their safety have been at the forefront of technology research. It is imperative to educate developers of IoT devices that security should be a priority in the development and production stage. Studies have shown that consumers expect manufacturers to put in proper protections to ensure their devices are safe, but newer devices continue to be more susceptible to exploits. Keeping the current mindset of producing devices without focusing on the security of the user will make homes more vulnerable to hackers over time. To address privacy concerns associated with IoT, universities can develop an IoT security course. Developing this course would entail discussing topics related to the various hardware aspects of IoT devices and how to exploit vulnerabilities within these systems. A lab section would cover devices and hardware; a student would be prepared to replicate previous exploits on old IoT devices. Through this course, future employees of IoT companies will adopt a security mindset in their development and the overall security of home IoT systems will be improved.

Despite calls for restriction from the public, tech companies creating IoT devices for households have had almost unlimited access to user data. This raises major privacy concerns, especially when more data collection contributes to more revenue. Tech companies have achieved this by reframing the data argument to be about security, being deceptive and not transparent, and taking advantage of users who lack knowledge of their devices. Ambiguous user consent with IoT device data collection enables tech companies to have power over the

consumer. Because unimpeded access to user data is the ultimate good for tech companies, case studies of common home IoT devices show they will not clearly inform consumers about their privacy policies. Regulation has avoided involvement with IoT privacy issues, and tech companies are always exploiting loopholes in existing laws. New regulation must be precise in defining key IoT terms and lawmakers must be active in their approach towards IoT, otherwise privacy issues will continue.

List of Contents