Thesis Portfolio

Robotany: An Environmentally-Aware, Autonomous Plant Hybrid
(Technical Report)

Teetime: Timing-Based Approach for Determining Secure World Behavior in ARM TrustZone
(Technical Report)

The Rise of Open Source Hardware: A Sociotechnical Perspective
(STS Research Paper)

An Undergraduate Thesis

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Jason Ashley
Spring, 2021

Department of Computer Science and Department of Computer Engineering

Table of Contents

Sociotechnical Synthesis

The following capstone projects and STS research paper discuss the development and processes behind hardware-based projects. The first capstone to be discussed, “Robotany,” focuses on the development of an autonomous plant potter robot. This project is used to dive deep into the development processes on microcontrollers while exploring the small signals produced by plants, all with the attempt to maximize sunlight for the plant and provide information on the plant’s development to its owner. The second discussion, “TEE,” is a capstone project exploring the use of trusted execution environments, how they secure sensitive information from malicious actors who compromise a device, and how they may not do so by attempting to exploit one design. Finally, the STS thesis is focused on how open source hardware projects, particularly in relation to projects that incorporate microcontrollers, are growing in popularity and commonality, representing a shift away from prior hardware development processes focused on providing very limited access to hardware and design tools. These projects each explore the possibilities of low cost hardware, how they may be used, and what concerns might arise around them.

The Robotany is an environmentally-aware, autonomous plant-hybrid system based on expansions to open systems. This system reports details and statistics related to the growth and health of a plant within some contained vehicle, allowing a user to view the growth progress of the plant. It is based on low cost microcontrollers and hobbyist robot design kits. Much of the software and hardware designs are based on open source projects, allowing the project to explore how this design paradigm allows for previous ideas to be incorporated into new projects. Further, there is a discussion of concerns about the information collected from the system’s sensors, with a further discussion on how these risks are mitigated.

An analysis of Trusted Execution Environments (TEEs) on certain processors was performed to understand what security vulnerabilities exist within these systems and how they can be mitigated. Many CPUs (including microcontrollers) utilize a TEE to run code that handles privileged details. With the rise of inexpensive, accessible hardware, devices are now deployed everywhere, many of which contain sensitive information protected by TEEs. However, TEEs currently on devices have been shown to exhibit security vulnerabilities that leak sensitive information. Thus, it is important to secure these environments. Through this project, a look into a particular type of attack is performed and attempted on low cost, semi-open hardware. This attack vector is important to consider when designing a project and knowledge of these details can inform how hardware is designed in the future.

Low cost and accessible microcontrollers are used in an increasing number of projects thanks to open source development practices for hardware making their use possible. The rise of the use of open source principles in project development was analyzed in the STS thesis to discover why this usage increase is occurring, who it benefits, and how it may be modeled, with several projects analyzed to this end. However, there are some concerns with such projects, such as their security and commercial viability, that are discussed.

In all of the works described, the use of microcontrollers in different situations was analyzed. The Robotany was a simple demonstration in using plants coupled with microcontrollers to provide meaningful information, an idea that could be expanded on in the future with the project being made publicly available and using widely available hardware. Trusted Execution Environments show that elements of microcontrollers still need improvements to handle sensitive information without the potential for leaking information. However, this has not slowed the open source hardware movement and the communities forming around them,

utilizing this technology to generate new projects. Overall, these projects provided a much better understanding of open hardware development, where it is now, and where it may be headed in the future.