Thesis Project Portfolio

ALTAIR: Automatic Light Tailoring Apparatus Instructing Radiance

(Technical Report)

The Ethical Question of New Technology in Vehicles: Is It Worth the Trade-Off?

(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

Steven Peng

Spring, 2022

Department of Electrical and Computer Engineering

Table of Contents

Sociotechnical Synthesis

The technical project focuses on an implementation of Internet of Things (IoT) technology to improve the users' quality of life while providing health benefits, while the Science, Technology, and Society (STS) paper focuses on privacy and safety issues that come with the implementation of new technology in automotive vehicles. A connection can be made from both projects in that the concerns raised in the STS topic are common concerns found with many IoT devices today, in that they are often not hardened enough to deter malicious entities from hacking into the device and stealing the users data and infringing on their privacy. Together, these two projects aim to bring light to data privacy issues that are introduced with new technologies.

The technical project focuses on improving the quality of life of individuals working at home with a system called the Automatic Light Tailoring Apparatus Instructing Radiance, or ALTAIR. ALTAIR is a system that automatically controls the ambient light levels of a room to help reduce eye strain and improve the user's overall health. ALTAIR has two nodes: a wirelessly accessible remote node, which contains the user interface and the interior light sensor, and the window node, which controls the servo on the blinds and transmit the exterior light sensor back to the remote node. The system is controlled by the user through a web interface and has features such as "night mode" which can turn off the smart lights and close the blinds for privacy. The interior light is measured at the remote node, which would increase or decrease light output at every source as the day progresses to ensure the light level stays within the users desired setting.

The STS paper focused on how new vehicles are getting "smarter" with new features such as autonomous driving and driver awareness features, which introduces an increase concern of cybersecurity and privacy risks regarding the consumer's safety and personal data. The paper focused on answering the following question: what security and privacy tradeoffs do automotive manufacturers make when implementing new technology into their vehicles, and how do these

decisions impact the general public? The risk analysis framework and the technological fix framework guided the analysis as it relates to Science, Technology, and Society. It was found that an abundance of cybersecurity risks does exist throughout the manufacturing and design process that stem from a lack of proper procedures to mitigate such risks, and that the privacy of the consumer's data can potentially be abused unknowingly. From this research, the automotive industry should emphasize the importance of securing the software and hardware vehicle during every step of the process, from the design stage to manufacturing stage and ultimately to the delivery stage and beyond. Along with that, the value and importance of preserving the consumer's data from third parties should be a high priority for manufacturers, as there is a direct correlation to the manufacturer's reputation on how they handle the consumers data. Some issues that are better off solved by implementing new policies or through societal changes in lieu of new technological features was also discussed within the paper.

By working on both projects simultaneously, I gained a deeper understanding of the issues that manufacturers face when trying to create a product that is secured from start to finish. Without having a defined process in place before designing the system, it is harder to secure a product from the top down rather than from the bottom up, with security being one of the driving design factors. For example, to secure an IoT product both the hardware and software need to be designed in a manner that would protect against both a hardware and software-based attack as much as possible, although if the malicious entity does have physical access to the device, then the entire system would likely be compromised already. I also learned that any data leaked from internet connected devices could be useful to attackers. For example, simply knowing either the vehicle's location or the status of the light bulbs and shades within a house could indicate whether the owner is at home or not, which could allow a malicious entity to then rob the house without fearing that anyone is

around. Specifically, from the technical project, I learned that an easy-to-use user interface is critical to a successful product, as if the user cannot use the product easily then they would have never bought the product to begin with. To tie that into the STS paper, if the user can share their personal usage data to allow the manufacturer to update and design a more effective and easier-to-use interface, then that is an acceptable use of their data. Overall, I learned a great deal on the cybersecurity aspects of both the automotive industry and with IoT devices, and I anticipate that my work will help guide more informed design decisions for both myself and to those in either industry.