Thesis Project Portfolio

Trust and Security of Embedded Smart Devices in Advanced Logistics Systems

(Technical Report)

Empowerment of Users: Privacy and Security Implications of Smart Devices

(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

Beatrice E. Li

Spring, 2021

Department of Engineering Systems and Environment

Table of Contents

Sociotechnical Synthesis

Technology has progressively advanced in what appears to be a self-governing manner with a disregard for the interests of users. As technology better caters to users' needs and desires, users have become increasingly suspicious, yet their behaviors are constrained by the very technologies they use. The power imbalance becomes apparent as the safety of people at the individual and national level is increasingly dependent on the reliability of technology. Control and power for the people are not unattainable but only need the right tools.

The technical component utilized a scenario-based risk analysis to assess the security and risk of hardware and embedded smart devices in three applications: (1) defense, (2) bidirectional charging, (3) advanced logistics systems. The risk analysis is performed through a literature review and consultations with industry experts from each of the three sponsors (1) Systems Planning and Analysis Inc., (2) Fermata LLC, (3) Commonwealth Center for Advanced Logistics Systems, respectively. The key findings for enterprise resilience to emergent and future conditions were identifying potential scenarios and its respective score that signifies its level of disruptiveness to the success of the system. A scenario was selected from each testbed for discussion and recommended actions. For the more general application of advanced logistic systems, the selected scenario was the proprietary information leak. The recommended action was to establish strategies that would secure proprietary information, such as data encryption.

The STS component explored various strategies that would empower users in their interactions with smart devices with a focus on user privacy and security. A type of gap analysis is performed to locate opportunities for intervention. The examination of the relationship between smart devices and users was central to the gap analysis as the dynamics of the relationship will help understand which strategy may be the most effective. The result was a

proposed data transparency scorecard that would help users understand the different facets of privacy policies related to a device, from how the data is collected to what is the data being used for – empowering users.

The technical and STS components yielded very relevant results as society progresses towards a more digitized form. Trust, security, and privacy are values that will always remain important to people, which prompts further research. With respect to the technical projects, the scenario-based risk analysis could be extended to additional stakeholder perspectives within each testbed, which would make the results more robust. With respect to the STS research, the feasibility and projected impacts of a proposed data transparency scorecard can be investigated. The two components centered around taking back the reins in controlling privacy and security in a world that is becoming increasingly technological. I want to thank my team, especially Chris VanYe, for being a supportive friend and a brilliant teammate. I would like to also thank David Barnes, our point of contact for the hypersonics analysis, for providing a wealth of information that has saved time and made this research possible.