Cybersecurity Threats in Autonomous Vehicle Technologies: Perceptions and Preparedness, A Case Study

***Methusela Sulle, Judith Mwakalonge, Gurcan Comert, Saidi Siuhi**
Graduate Student, South Carolina State University, Professor, South Carolina State University, Associate Professor, Benedict College, Assistant Professor, South Carolina State University

Keywords: *Autonomous Vehicle, Cybersecurity.*

ABSTRACT

Integrating Autonomous Vehicle (AV) technologies into modern transportation systems has introduced a new frontier of cybersecurity challenges, necessitating a comprehensive understanding of the associated risks and the measures required to mitigate them. This study explores the diverse spectrum of cybersecurity threats specific to AV technologies, focusing on elucidating perceptions and assessing preparedness within the SC State University community. Through a comprehensive survey instrument, this study endeavors to unveil the intricate web of cybersecurity vulnerabilities inherent in AV systems. These vulnerabilities encompass a wide range of potential risks, including malicious hacking attempts targeting vehicle control systems, manipulation of sensor data, and breaches in communication networks. By capturing the perceptions of students, faculty, and staff regarding these threats, alongside evaluating existing institutional mechanisms for cybersecurity readiness, this study aims to provide valuable insights into the evolving cybersecurity landscape within the context of AV technologies. Furthermore, the findings of this study will contribute to broader discussions surrounding the development of robust cybersecurity frameworks and proactive strategies essential for safeguarding the integrity, safety, and security of autonomous vehicle technologies. Ultimately, the outcomes of this research will inform policymakers, industry stakeholders, and academic institutions about the critical imperative of prioritizing cybersecurity in the deployment and operation of AV systems, ensuring the resilience of future transportation ecosystems.

Transportation Cybersecurity Vulnerabilities, Threat Models, and Mitigation Strategies

***Ostonya Thomas, Jean Michel Tine, and Mashrur Chowdhury**
Ph.D. Student, Clemson University, Ph.D. Student, Clemson University,
Professor, Clemson University

Keywords: cybersecurity, cyber-resiliency, transportation infrastructure security

Abstract

The transportation industry is experiencing a vast digitization as a wide array of technologies are implemented to improve transportation efficiency, functionality, and safety. Although technological advancements bring a plethora of benefits to transportation, the expansion of cyberspace to various sectors of transportation has introduced new threats. In the past, it was assumed that digital infrastructure was secured since its vulnerabilities were not known to adversaries. Since the expansion of cyberspace, however, this assumption stands far from valid. With the rapid advancement of wireless technology connecting transportation to everything and expansion of cyberspace in transportation, threats and vulnerabilities continue to increase. In this work, past cybersecurity failure events in various sectors of transportation are analyzed. These events are studied to discover different threat models and how these threats will significantly increase cyber-vulnerabilities in transportation systems. This research also proposes strategies for mitigating emerging cybersecurity threats, such as the development of standards, testing and certification strategies and adaptive security measures.

Threats of Trojan Incursion in Transportation Hardware

[*]Sefatun-Noor Puspa, Jean Michel Tine, Reek Majumdar, Gurcan Comert, Mashrur Chowdhury, and Yingjie Lao
[*]Ph.D. student, Glenn Department of Civil Engineering, Clemson University, Associate Professor, Dept. Computer Science, Benedict College, Professor, Glenn Department of Civil Engineering, Clemson University

Keywords: Intelligent Transportation System, Hardware Security, Hardware Trojan, Electronic Toll Collection System, Security Measures

Abstract

Today's intelligent transportation systems (ITS) blend new technologies with old-school legacy transportation systems, improving getting around and managing traffic. However, this integration has also introduced new security challenges, particularly in protecting the systems that manage traffic signals and toll collections. While considerable focus has been on safeguarding the software aspect of these systems, the hardware components are critical for ensuring public safety and economic stability.

This study addresses a crucial security concern within ITS: the risk posed by hardware Trojans. These are malicious modifications embedded within the physical components of transportation systems, which become particularly problematic due to the globalized nature of manufacturing of the embedded systems. Components from various suppliers worldwide create many opportunities for malicious actors to insert Trojans. These Trojans are designed to evade standard security measures by remaining dormant until triggered under specific conditions, making their detection and mitigation a complex challenge.

Our research focuses on electronic toll collectors, employing an experimental setup to illustrate the tangible threat posed by hardware Trojans. By incorporating a Field-Programmable Gate Array (FPGA) board into our experiment, we could mimic the operational dynamics of toll collection systems and introduce a Trojan that could be activated under certain conditions. This setup not only revealed the potential for manipulating toll rates and undermining traffic safety but also underscored the critical need for enhanced security measures in the hardware of transportation systems.

The study underscores the importance of adopting secure design and manufacturing practices for ITS hardware, which asks for teamwork among designers, manufacturers, and security experts. Their collaborative effort should ensure that all parts are safe from the beginning of the hardware lifecycle. This effort is crucial to keep threats at bay early on. It also protects the components before they become part of the system.

Moreover, the study points out that we need more research to find better ways to detect hardware Trojan. It is crucial to understand how these security weak spots can affect the safety and reliability of our transportation. A clear picture of these risks will promote extensive arguments on solid security measures. Exploring legal and regulatory aspects related to hardware security in transportation is also crucial, emphasizing gaps identification in security laws, policies, and regulations to enhance the sector's security posture.

In conclusion, this research brings to light an often-neglected aspect of ITS security: the vulnerabilities inherent in hardware components. The study focuses on the dangers posed by hardware Trojans and suggests ways to prevent them. It aims to make ITS both safer and more dependable. This effort is crucial for public safety, national security, and maintaining the integrity of essential transportation networks, thus defending against advanced cyber threats.