PhD Thesis Summary

Cybersecurity for future interconnected and smart vehicles

by Franco Oberti
Department of Your Department
Politecnico di Torino

April 9, 2024

Abstract

he continual technological advancements mark the modern world, and the automotive industry is no exception. As vehicles rely more heavily on technology and connectivity, cybersecurity has become a pressing concern to ensure safe and reliable transportation. This PhD dissertation extensively explores the intricate relationship between cybersecurity measures and their significant role in the automotive industry. It highlights the importance of strong security protocols in effectively reducing cyber threats and ensuring the integrity of operations and the safety of passengers. Regulatory bodies globally have introduced new Cybersecurity Approval frameworks in response to the growing need for cybersecurity measures in the automotive sector. These frameworks, including the United Nations Regulation No. 155 (UNR155) and strict guidelines from the National Highway Traffic Safety Administration (NHTSA) in the United States, highlight the urgent need for enhanced cybersecurity measures.

The dissertation comprises several chapters meticulously crafted to examine various aspects of automotive cybersecurity. The dissertation summarizes automotive technology's evolution, setting the stage for understanding the importance of cybersecurity in the industry. It then delves into legislative norms and historical and potential cyberattacks, identifies risks, and evaluates economic effects. Subsequent chapters scrutinize the electrical architecture of vehicles, communication protocols, and security techniques and introduce innovative research projects focusing on hardware authentication, advanced vehicle communication networks, and the authentication of CAN data frames to ensure communication integrity. One of the pivotal contributions of this thesis is the development of novel network architectures that balance high-security standards with the operational demands of real-time automotive systems.

The dissertation critically examines the vulnerabilities in current cybersecurity standards within the automotive sector. It proposes enhanced solutions to bolster defenses against cyber threats in an increasingly interconnected and automated ecosystem. Through in-depth analysis and the proposition of innovative security mechanisms adapted to automotive communication protocols, this dissertation aims to fortify the automotive industry's resilience against the continuously evolving cyber threat landscape. The research addresses current challenges and anticipates future developments, striving to significantly contribute to automotive cybersecurity and ensure the sector's security in the digital age.

In the dynamic and ever-changing terrain of contemporary technological advancements, the critical importance of cybersecurity in maintaining the operational integrity and safety of passenger cars has become a matter of paramount concern. This dissertation delves deep into the nuanced relationship between cybersecurity measures and their crucial role within the automotive industry, emphasizing the urgent need to implement robust security protocols to thwart cyber threats effectively. The impetus for this research is significantly reinforced by the introduction of new Cybersecurity Approval mandates required across all significant nations, notably including adherence to the United Nations Regulation No. 155, along with the stringent guidelines promulgated by the National Highway Traffic Safety Administration in the United States. These regulatory frameworks underscore the acute

necessity for bolstered cybersecurity measures within the automotive sector, particularly in the context of the burgeoning connectivity and the increasing dependency on embedded systems that characterize contemporary vehicles.

Cyber intrusions still pose a significant security threat to areas such as embedded systems, particularly those responsible for critical safety functions. The deployment of conventional Information Technology cybersecurity strategies offers limited protection within these specialized embedded environments, thus highlighting the urgent need for dedicated research to develop security measures specifically crafted for these contexts. The architectural design of this thesis meticulously demystifies the complex landscape of automotive cybersecurity. Beginning with an introduction in Chapter 1 lays a solid foundation for a deep dive into the evolution of automotive technologies. This exploration is critical for grasping cybersecurity's importance in ensuring road vehicles' safety and integrity. Chapter 2 provides an extensive overview of the legislative norms, standards, and guidelines shaping the realm of automotive cybersecurity, thereby preparing the ground for subsequent analyses. Chapter 3 delves into the intricate details of historical and potential automotive cyberattacks, identifying likely attack surfaces, assessing associated risks, and evaluating the economic repercussions of such security breaches. Following this, chapter 4 meticulously examines the electrical architecture of vehicles, communication protocols, and prevailing security techniques within the automotive industry. The dissertation concludes with a discussion of the research's main findings and contributions, along with recommendations for future research in automotive cybersecurity.