韓國融合信號處理學會

2023 夏季學術大會

KICSP SUMMER CONFERENCE 2023

일시 2023.06.16(금)~17(토)

장소 부산대학교

주최 : 사단법인 한국융합신호처리학회

주관 : 부산대학교

후원 : 한국로봇융합연구원, KMG거명
㈜경성테크놀러지

Cybersecurity Threats and Countermeasures in Smart Vehicles

코디로브하산보이[1], 이훈재[1], 이영실[1*]
[1]동서대학교 일반대학원 컴퓨터공학과

Cybersecurity Threats and Countermeasures in Smart Vehicles

Kodirov Khasanboy[1], Hoon-Jae Lee[1], YoungSil Lee[1*]
[1]Department of Computer Engineering, Graduate School, Dongseo University

Abstract It has become increasingly common in the automotive industry to incorporate smart technologies into vehicles as they advance rapidly. Smart vehicles rely heavily on the Internet of Things for their automation, the backbone of every system installed. As well as these advances, the cybersecurity landscape has evolved, leading to new threats that pose significant dangers to smart vehicles. In addition to traditional cyber-attacks on vehicle information and operations, there is a new breed of attacks involving ransomware, IoT attacks, DDoS (connected vehicles taken over by botnet armies), and vehicle theft. As part of this paper, a variety of cybersecurity threats that smart vehicles face and the potential consequences of these threats are analyzed, and the countermeasures designed to enhance the security of these vehicles are proposed. Based on a comprehensive literature review, this paper highlights the importance of protecting drivers and passengers from cybersecurity issues in smart vehicles.

• Key Words : Cybersecurity Threats, Smart Vehicles

Ⅰ. Introduction

According to projections, over 400 million connected cars will operate by 2025, up from 237 million in 2021. A revolution in the automotive industry has been brought about by smart vehicles, which are outfitted with advanced communication and computing systems. Many benefits are associated with these vehicles, including improved safety, improved connectivity, and increased convenience. Furthermore, it is essential to note that integrating complex technologies can introduce vulnerabilities that malicious individuals can exploit. Vehicles equipped with smart technology are vulnerable to cybersecurity threats that compromise vehicle safety, privacy, and functionality. Weighing the importance of these factors, this paper identifies and evaluates these threats, their potential implications, and mitigation measures that can be taken.

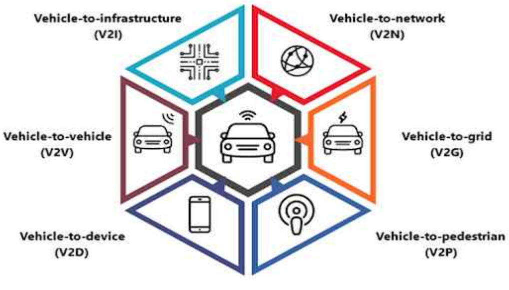

Fig. 1. Communication Architecture of Smart Vehicles

Ⅱ. Cybersecurity threats in Smart Vehicles

In terms of variety, several cyber threats affect smart vehicles, as revealed by the literature review. The data integrity and confidentiality vulnerabilities of vehicle-to-vehicle communications pose the risk of data interception and manipulation, which can lead to accidents and unauthorized access to personal information. Besides that, it is also possible to compromise sensitive data within the infotainment system, including personal information and a history of where the user went. Last but not least, there are numerous privacy concerns raised by inadequate data privacy protection, including data breaches, unauthorized use, identity theft, and targeted attacks.

Considering more technical, it is important to mention that the potential for remote code execution attacks is one of the top cybersecurity threats in smart vehicles. In these attacks, software vulnerabilities and firmware issues are exploited in vehicles' engine control units (ECU) or infotainment systems. Unauthorized access and control over critical vehicle functions can be gained using these vulnerabilities. For example, by injecting malicious code into the ECU, an attacker can control the engine performance, compromising vehicle safety.

In addition, smart vehicles use communication protocols, such as the Controller Area Network (CAN) bus, for inter-component communications. As a result, these protocols are susceptible to attacks like spoofing and replaying due to a lack of authentication and encryption. It may also be possible for an attacker to inject false commands or tamper with sensor data by impersonating trusted components or replaying valid messages.

Furthermore, the increased connectivity of smart vehicles poses a threat of targeted attacks via over-the-air updates. In the absence of secure mechanisms, malicious actors may exploit OTA updates to deliver malware or make unauthorized modifications to the vehicle's systems, compromising the integrity and functionality of the device. Considering these findings, it becomes increasingly important to implement robust countermeasures to effectively mitigate these threats and protect drivers' and passengers' privacy.

Ⅲ. Cybersecurity Countermeasures in Smart Vehicles

Multi-layered cybersecurity approaches that leverage existing cybersecurity frameworks and encourage the industry to adopt best practices to improve vehicle security posture are required to ensure a comprehensive cybersecurity environment.

3.1 Encryption and Authentication

V2V communications and data exchange should be implemented with robust encryption and authentication mechanisms to prevent unauthorized access and data manipulation.

3.2 Intrusion Detection Systems (IDS)

It is possible to detect malicious activity and anomalies in smart vehicles by installing an IDS, which allows for a timely response and mitigation of potential cyberattacks.

3.3 Regular Software Updates

Keeping software up-to-date is crucial for patching vulnerabilities and protecting against emerging threats. Automakers should prioritize releasing security patches, and owners should be encouraged to apply them promptly.

3.4 User Awareness and Education

There is always a need to improve awareness of cybersecurity among vehicle owners. The risk of cyberattacks can be significantly reduced by educating users about potential threats, safe practices, and the importance of strong passwords and secure Wi-Fi networks.

Ⅳ. Conclusion

With the increasing popularity of smart vehicles, it becomes increasingly important to employ robust cybersecurity measures. Throughout this paper, we emphasize the cybersecurity threats that smart vehicles may face and countermeasures. The automotive industry can increase the security of smart vehicles and ensure the future of connected transportation by implementing effective countermeasures, such as encryption, authentication, intrusion detection systems, and user education.

ACKNOWLEDGMENTS

This research was a part of the project titled 'Marine digital AtoN information management and service system development(3/5) (20210650)', funded by the Ministry of Oceans and Fisheries, Korea.

REFERENCES

[1] HyunHo Kim, JongGun Song, "Analysis of IoT Security in Wi-Fi 6," The Korea Institute of Convergence Signal Processing, 22(1), 38-44.

[2] Martin Placek, "Connected cars worldwide," Dec 8, 2021, available from:
https://www.statista.com/topics/1918/connected-cars/

KICSP

KICSP-2023-018호

우수 발표 논문상

Excellent Paper Award

제목 : Cybersecurity Threats and Countermeasures in Smart Vehicles

발표자 : 코디로브하산보이, 이훈재, 이영실(동서대)

상기 논문은 (사) 한국융합신호처리학회가 주최한 2023년 하계학술대회에서 우수한 논문 내용과 뛰어난 발표력으로 세션 좌장들이 추천한 우수 발표논문으로서 학술이사회의 결정에 따라 이 상을 수여합니다.

2023년 6월 17일

(사)한국융합신호처리학회 회장 박 준 모 인

(General chair of KICSP Summer Conference 2023 Jun-Mo Park)