ISSN: 2641-2039
DOI: 10.33552/GJES.2021.09.000701
Global Journal of Engineering Sciences
Iris Publishers

Mini Review

Cyber-Security Threats of Connected and Automated Vehicles

Xhoendi Collaku* and Azeem Hafeez

CECS Department University of Michigan - Dearborn, USA

***Corresponding author:** Xhoendi Collaku, CECS Department University of Michigan - Dearborn, USA.

Received Date: November 16, 2021

Published Date: December 03, 2021

Abstract

With the evolution of Connected and Automated Vehicles (CAVs), the number of functions that in-vehicle systems must perform has grown in order to facilitate real-time data transmission across the in-vehicle network (IVN) for critical timing automated tasks. Additionally, CAVs functionalities have been further expanded to vehicle-to everything (V2X) technology including inter-communication between (i) vehicle-to-vehicle (V2V), (ii) vehicle-to-infrastructure (V2I), and (iii) vehicle-to- network (V2N). These additional components have all enhanced the vulnerability of inter-vehicle communication to cyber-attacks, which has been a major concern since the widespread adoption of CAVs. As a result, several security researchers are looking into cyber-attack scenarios that might threaten autonomous vehicles. The primary objective of this study is to identify the most prevalent attackable surfaces that can be exploited by intruders to gain access to the IVN of in-vehicle systems by analyzing the CAVs system components that have increased the exposure to cyber-attacks. The analysis of these cyber-trends and incidents would benefit a wide range of industries, including insurance firms and the Automotive Cybersecurity Market, and would have a significant impact on the US economy as a whole.

Keywords: Connected and automated vehicles (CAVs); In-vehicle network (IVN); Cyber-security threats; Vehicle-to- everything (V2X)

Introduction

Connected and Automated Vehicles (CAVs) have been con- tinuously advanced to support both (i) real-time automation, as well as to (ii) expand the connectivity of the vehicle systems beyond the in-vehicle network. Different intra-vehicle interconnection technologies including Controller Area Net- work (CAN), FlexRay, Automotive Ethernet, Media Oriented Systems Transport (MOST), have been utilized in autonomous driving to support the increasing functionalities of electronic control units (ECUs) inside CAVs. Nonetheless, all of these networks have been subject to the same problem, which is related to the growing number of cyber-attack scenarios within the CAVs system. Autonomous vehicles are highly susceptible to attacks since they are mostly governed by ECUs incorporated in the system, which are all prone to malware and cyber-attacks. Various cyber-attack scenarios have been recently reported from well-known automobile manufacturers.

In 2020, a Mercedes-Benz E-Class car was revealed to have 19 vulnerabilities, allowing hackers to remotely operate the vehicle, including unlocking doors and starting the engine [1]. OEMs such as Tesla, General Motors, Ford, FCA, Daim- ler, and others launched bug-bounty programs on sites like BugCrowd, HackerOne, and their own websites in 2020 [1]. Section II addresses the state of art of in-vehicle cyber- security, as well as overviews some of the cyber-attacks scenarios and how they relate to the CAVs architecture.

Cyber-Attack Vectors

Many studies have surveyed the attackable surface of the CAVs networks, and how they have increased the exposure of automobiles to cyber-threats, resulting in an increase of cyber-incidents. Figure 1 shows the distribution of the attack vectors utilized during the last ten years 2010-2020 [1]. As seen in Figure 1, (i) servers, (ii) keyless entry systems, and (iii) mobile apps were the three most prevalent attack vectors. (i) Vehicle connection to an external server or database has made it easier for attackers to gain remote control on the entire connected vehicle fleet by hacking the command-and- control server, one of the most recent incidents reported

by Tesla [1]. (ii) Keyless entry attacks have also made it feasible for hackers to remotely and wirelessly open the vehicles and start the engine leading to hackers stealing these vehicles by exploiting the vulnerability of the embedded software, the reason why this category accounts for 26.62% of the cyber- attacks scenarios, as seen in (Figure 1). (iii) Mobile apps have also been exploited by attackers, ranging from the retrieval of GPS locations to the control and manipulation of a variety of operating functions or devices within the vehicle. Many software flaws or preconfigured credentials encoded in the mobile app code, as well as weakness in the mobile app's backend server, are all factors that have made mobile apps the top third most common attack vector [1].

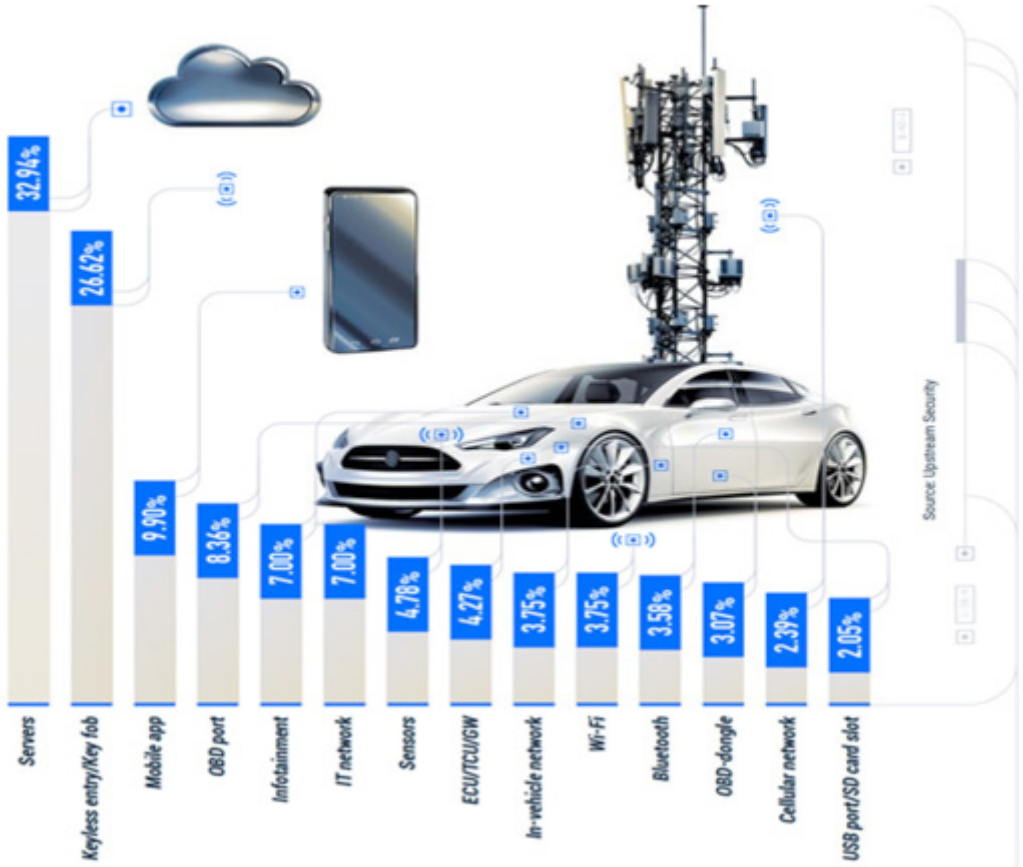

Figure1: Breakdown of most common Cyber - Attack vectors used 2010 - 2020 [1].

Other sources have overviewed some of the previously conducted cyber-attack scenarios by analyzing the CAVs system architecture. According to [2], the key elements of autonomous driving that make CAVs more exposable to cyber- attacks can be divided into three categories (i) Automatic control system, (ii) Autonomous-Driving-System components, (iii) V2X communication technology, as seen in (Figure 2).

The automatic control system is strongly connected to the safety of the driver as it includes elements such as (i) ABS control, (ii) suspension control, (iii) vehicle dynamic control, (iv) Airbag-systems [3]. Automatic control system attacks are further divided into (i) ECU attacks and (ii) In-Vehicle network attacks, and (iii) Automotive-Key-Related attacks [2]. One ex- ample of the ECU attacks is using the fuzzing method where a targeted ECU receives random inputs in the form of a network packet that threatens the security of the driver, by changing parameters that are critical to the operation of the vehicle and might lead to a critical crash [4]. In-vehicle network attacks are based on the vulnerability of the bus topology being utilized. Attackers can inject arbitrary commands into the IVN in the form of payloads, and the target vehicle will execute the commands as intended by the attacker [4]. The second category of Autonomous Driving System includes (i) sensor attacks and (ii) mobile app attacks. Some of the sensors utilized in CAVs are LIDAR sensors, wireless access, autopilots and navigators, sensors, and actuator controls [3]. Sensor security is essential in autonomous vehicles since ECUs rely on sensor data to determine each subsequent action. For example, as shown in [5], a study was conducted on Ultrasonic Sensor Vulnerability, which demonstrated the inaccuracy of employing ultrasonic sensors installed on a vehicle to detect an obstacle when they are interfered with by another ultrasonic sensor nearby. The third category, V2X communication technology, which has essentially increased traffic safety and efficiency, has also increased the exposure of the in-vehicle network to the exter-

nal networks and infrastructures. A paper by Bariah et al. [6] surveys the state-of-the-art on security threats by addressing potential VANET attacks during vehicle communication. One example is GPS spoofing, which occurs when an attacker sends out a powerful signal that is stronger than the GPS signal, leading to the disruption of communication known as jamming [6].

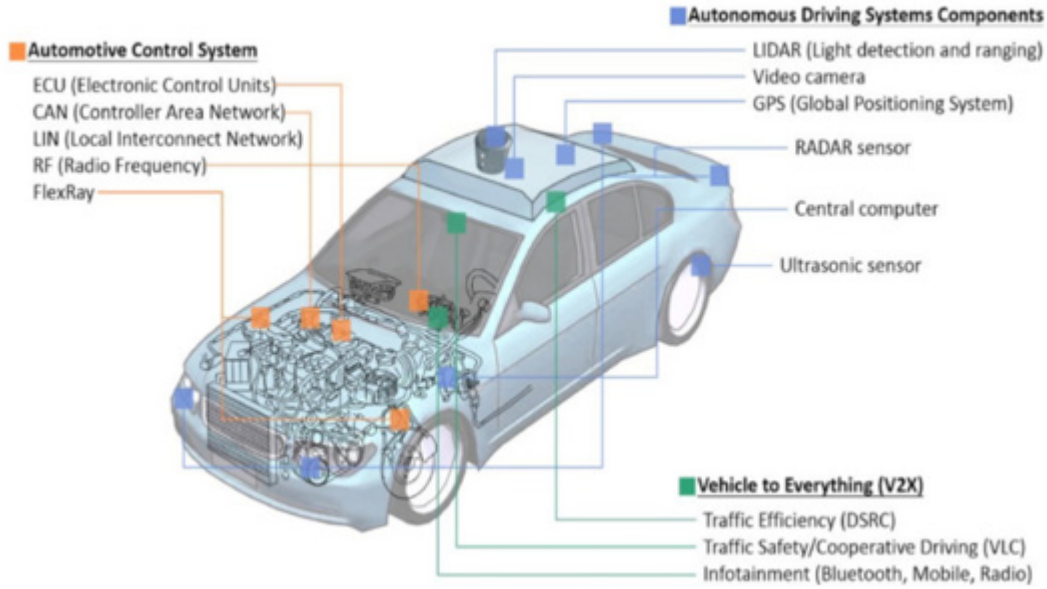

Figure 2: CAV s system components that impact the level of security [2].

Conclusion

This paper is intended to provide a thorough analysis on the current state of art of CAVs security. Based on this study the majority of hackers aim to get access to the car network remotely rather than physically, making it more difficult to identify and halt the attack. Most of the attack scenarios are related with the system architecture of CAVs where the system components that have facilitated the exposure to attacks include (i) Automatic control system, (ii) Autonomous-Driving- System, (iii) V2X communication technology. The identification of the system components and attackable surfaces is crucial in concentrating the further literature studies on the mitigation of the most problematic attack vectors. Despite the fact that numerous defenses and mitigation methods have been given in the literature, the security concerns continue to grow as CAVs' functionalities are advancing rapidly.

Acknowledgement

None.

Conflict of Interest

No conflict of interest.

References

1. Global automotive cybersecurity report.
2. K Kim, JS Kim, S Jeong, JH Park, HK Kim (2021) Cybersecurity for autonomous vehicles: Review of attacks and defense, Computers & Security, pp. 102150.
3. U Kiencke and L Nielsen (2000) Automotive control systems: for engine, driveline, and vehicle.
4. S Jeong, B Jeon, B Chung, HK Kim (2021) Convolutional neural network-based intrusion detection system for avtp streams in automotive ethernet-based networks. Vehicular Communications 29: 100338.
5. BS Lim, SL Keoh, VL Thing (2018) Autonomous vehicle ultrasonic sensor vulnerability and impact assessment. in 2018 IEEE 4th World Forum on Internet of Things (WF-IoT). IEEE pp. 231-236.
6. L Bariah, D Shehada, E Salahat, C Y Yeun (2015) Recent advances in vanet security: a survey. in 2015 IEEE 82nd vehicular technology conference (VTC2015-fall). IEEE pp. 1-7.