Firmware Security in Connected Electric Vehicles: Challenges and Solutions

Omkar Manohar Ghag

M. S Telecommunication, University of Pittsburgh, PA
Email: *ghag.omkar28[at]gmail.com*

Abstract: ***The adoption of autonomous electric vehicles is one of the most significant milestones in the sustainability endeavor that the automotive industry has achieved. These autonomous vehicles are characteristically well - optimized, thus reducing traffic congestion, minimizing accidents, and significantly reducing environmental pollution. The design of an autonomous vehicle entails the mechanical parts, which are the moving and body sections, and the computerized systems consisting of software that performs the processing of the programmed autonomous driving as it receives timely updates from the surroundings using several sensors attached to it. A middle layer called firmware between these systems is used to translate the software instructions into a machine - understandable state, which is the actual action leading to autonomous driving. This firmware is essential; hence, there is a high concern for its security. The firmware could be vulnerable to interceptions when communicating with other remote systems that provide over - the - air updates and sensor communications. Furthermore, it could be compromised by physical manipulation if an attacker gains access. There have been recent attacks on the firmware showing its vulnerabilities and challenges. This paper discusses these cases and explores some strategies that can be used to enhance firmware security, such as defense - in - depth frameworks and security - by - design approaches.***

Keywords: Autonomous Driving, Firmware security, Electric vehicles

1. Introduction

One of the most significant advancements in the automotive industry is the development of electric vehicles. An even further evolution in the field is through the design and production of autonomous vehicles. Autonomous vehicles are expected to mitigate issues associated with accidents and human inefficiencies, thus ensuring road safety and optimizing productivity [4]. Furthermore, using electric vehicles immensely benefits environmental sustainability and eases traffic congestion. Considerably, electric vehicles, particularly autonomous ones, are still in the immature stages of development as their adoption has yet to be highly successful in most parts of the world [1]. One of the leading concerns in autonomous vehicles is the security of its components. Considering that these autonomous vehicles are highly computerized and rely on the technological components that are sometimes interconnected over the internet to enable over - the - air updates of its systems and timely assessment of efficiency issues such as traffic status on different roads, it implies that the communication of the autonomous vehicles faces the same risks as all information systems on the internets—getting hacked [1]. This paper focuses on the firmware component of autonomous vehicle systems. Considering its crucial role in communication and contribution towards autonomous driving, the paper will examine its security concerns. The paper will specifically examine the potential vulnerabilities of recent security breaches. Then, it will provide recommendations on possible strategies and technologies that can be used to enhance the security of the autonomous vehicle’s firmware.

The development of autonomous driving functionality requires a harmonious integration of computerized systems with the mechanical parts of the vehicles. The computerized systems comprise the software components and hardware hosting the former. Firmware, in its conventional form, is used to bridge the software and hardware components of these computerized systems of autonomous driving. Thus, the architecture of computerized systems used in autonomous driving, especially communication, is detailed as the abstract layer of software, a firmware translating these functionalities into a machine - understandable state, and the lower layer of hardware taking instructions from the middle firmware section [1]. Hence, the firmware is pivotally dependable to realize autonomous vehicles' autonomous driving aspect and communication.

Autonomous driving vehicles have several sensors that constantly collect data from the surroundings, perform real - time analysis, and make immediate adjustments. These sensors include cameras, ultrasonics, radar, Light Detection and Ranging—LIDAR, and onboard chips [7]. These sensors are all necessary to detect objects around the vehicles, the status of the road, and navigation capabilities. Additionally, the firmware is used in implementing communication protocols that enable data transmission from the sensors to the control systems for processing before performing the same function when interacting with the driving components [7]. The accuracy of firmware in transmitting information between the computerized parts and the driving components of the vehicle is the central determinant of efficiency in realizing a safe, well - functioning autonomous automotive.

Moreover, the vehicle control units themselves are managed entirely by the firmware component. These vehicle control units are, in turn, used to ensure functionalities of almost all aspects that lead towards the vehicle's movement in the context of autonomous driving. Such aspects include suspension, braking, propulsion, and steering [4]. These aspects are realized through the command interpretation action of the firmware as received from higher - level software, and then the machine instructions lead to the physical execution. This process is very critical, considering that the decisions made are required within a very short time. In some instances, they determine the safety of those in the vehicle and individuals sharing the road, such as pedestrians on pavement and other cars on the same and other lanes. The

Paper ID: SR24302010944 DOI: https://dx.doi.org/10.21275/SR24302010944

firmware also manages all communication with other vehicles in real - time. Additionally, the firmware translates communication processes such as alarms, instructions from traffic, and updates.

2. Potential Vulnerabilities of the Firmware Used in Vehicle Communication and Autonomous Driving

Considering that the firmware acts as a gateway to the hardware components of the computerized systems that act in the autonomous driving process, its vulnerability puts the entire system at risk. The over - the - air - updates are the leading vulnerability in the firmware used in autonomous vehicles [4]. This implies that the firmware configuration could be replicated on an attacker's computer and then manipulated and delivered as an update [2]. Considering the communication capabilities of the firmware over the internet, the attackers could manipulate the update codes and compromise the vehicle's safety. This attack could even be more straightforward if the hacker initially understood the vehicle and the firmware used to control the autonomous driving aspect.

An attacker could also perform malware injection to the firmware, creating backdoors that can later be used to perform other malicious activities, including gaining complete control of the vehicle and leading it to undesired places [3]. Some companies or insider attackers could install rootkits earlier to collect consumer data after delivering the autonomous vehicles. These rootkits could be used further in collecting sensitive data about the users of the vehicles and other aspects that can be used in more sophisticated attacks. For instance, using the data collected and gaining further access to the software components of the autonomous car system, the attacker could use the information to conduct brute - force password hacks into other computer systems and execute a distributed denial of service attack [5]. Alternatively, an attacker could intercept communication of the autonomous vehicle functionality of the firmware and execute a man - in - the - middle attack.

While solid access control mechanisms could have been implemented on higher - level software used in the autonomous vehicle, the firmware could be weakly authenticated. In some worse instances, a completely or inefficient encryption mechanism could have been utilized in securing the firmware. A more difficult - to - detect vulnerability would be errors in communication protocols used during the configuration and establishment of information exchange sessions. Vulnerability of protocols can lead to interception of communication between the firmware and remote servers or computer systems issuing commands. The firmware is also vulnerable to physical manipulation if accessible. The vehicle could be left unguarded and unlocked, and then the attacker could gain access and manipulate the firmware, enabling them to remote control it. Considering the first advancement of autonomous vehicles and related technologies when autonomous vehicle adoption is still immature, complexities could arise in integrating firmware in older vehicles [4]. There could also be vulnerability due to the use of legacy firmware in modern electric - connected cars. This could expose cars to unprecedented vulnerabilities, leading to calculation errors, machine errors, and outright integration challenges that could be highly dangerous. Human errors in configuring and updating firmware are also significant vulnerabilities that could lead to exploitable flaws and failures.

3. Recent Security Breaches

In 2019, an attack targeting the autonomous vehicle’s normal behavior was conducted and successfully executed by locking the radio in the car so that those inside it could not turn on, thus compromising communication [8]. In 2020, a breach was executed in an autonomous car to distract the driver [9]. This attack was done by forcibly turning in the in - vehicle radio and tuning its volume [9]. This was risky, considering the confusion of the driver. One of the historic data breaches in autonomous cars occurred remotely on the Jeep Cherokee in 2015 as a research test showing the vulnerability of self - driving cars [6]. This breach led to the recalling of 1.4 million cars by Fiat Chrysler as they strove to fix vulnerabilities in the vehicles [6]. After getting fixes, the researchers showed that the Tesla key for vulnerability could be breached by cloning its firmware and using it to gain unauthorized access to the control system of the entire vehicle [10].

4. Strategies For Enhancing Firmware Security

Effective frameworks should be used in the development of the firmware. For instance, security by design could be used to ensure that the security of the systems is established as part of the architecture, thus preventing potential development flaws [5]. A defense - in - depth framework that ensures multiple layers of security are utilized could also ensure maximum security of the framework [5]. A zero - trust framework can be employed by assuming anyone accessing or using the firmware cannot be trusted; thus, authentication should always be checked. Security of data transmitted remotely could be enhanced by using more robust encryption standards and multifactor authentication methods to store sections of this crucial information [5]. Technologies such as intrusion detection and prevention systems should be installed on the autonomous vehicle to detect potential data breaches of the firmware [5]. Strict, comprehensive checks should be established to ensure vendors of these firmware are examined to ensure no flaws occur along the supply chain that could lead to vulnerability.

5. Conclusion

The firmware is one of the most crucial components of autonomous driving. It bridges the interaction between the higher - level software components and lower - level hardware ones. This firmware is, however, likely to have vulnerabilities that could be destructive to the security of the autonomous vehicle, considering that it can be physically or remotely manipulated. This paper explored the significance of the firmware in detail as utilized in autonomous electric cars, including how it is used in communication and bridging the interaction between the software components and the mechanical aspect of the vehicles. Firmware security issues discussed herein include interception risks when obtaining over - the - air updates, denial of service attacks, and physical manipulation if an attacker can access the firmware. This paper has also discussed possible security implementations that can be employed to protect the firmware from potential attackers, such as using a security - by - design framework when creating it, employing defense - in - depth or zero - trust implementations, and improving the physical security of the firmware.

References

[1] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud, and M. Abdallah, "Blockchain - based Firmware Update Scheme Tailored for Autonomous Vehicles, " *arXiv (Cornell University)*, Apr.2019, doi: https: //doi. org/10.1109/wcnc.2019.8885769.

[2] M. Channon and J. Marson, "The Liability for Cybersecurity Breaches of Connected and Autonomous Vehicles, " *Computer Law & Security Review*, vol.43, p.105628, Nov.2021, doi: https: //doi. org/10.1016/j. clsr.2021.105628.

[3] M. Dibaei *et al.*, "Attacks and defenses on intelligent connected vehicles: a survey, " *Digital Communications and Networks*, May 2020, doi: https: //doi. org/10.1016/j. dcan.2020.04.007.

[4] C. Gao, G. Wang, W. Shi, Z. Wang, and Y. Chen, "Autonomous Driving Security: State of the Art and Challenges, " *IEEE Internet of Things Journal*, pp.1–1, 2021, doi: https: //doi. org/10.1109/jiot.2021.3130054.

[5] Giannaros *et al.*, "Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions, " *Journal of Cybersecurity and Privacy*, vol.3, no.3, pp.493–543, Aug.2023, doi: https: //doi. org/10.3390/jcp3030025.

[6] Kagubare, "Increasingly Autonomous Cars Raise Cybersecurity Fears, " *The Hill*, Jun.08, 2022. https: //thehill. com/driving - into - the - future/3514634 - increasingly - autonomous - cars - raise - cybersecurity - fears/

[7] Nobles, D. N. Burrell, S. L. Burton, and T. Waller, "Driving into Cybersecurity Trouble with Autonomous Vehicles, " pp.255–273, Mar.2023, doi: https: //doi. org/10.4018/978 - 1 - 6684 - 7207 - 1. ch013.

[8] H. Olufowobi and G. Bloom, "Connected Cars: Automotive Cybersecurity and Privacy for Smart Cities, " *Smart Cities Cybersecurity and Privacy*, pp.227–240, 2019, doi: https: //doi. org/10.1016/b978 - 0 - 12 - 815032 - 0.00016 - 0.

[9] S. Ornes, "How to Hack a self - driving Car, " *Physics World*, vol.33, no.8, pp.37–41, Aug.2020, doi: https: //doi. org/10.1088/2058 - 7058/33/8/25.

[10] D. Winder, "Tesla Has Facepalm Moment as Hackers Defeat 'Fixed' Model S Security, " *Forbes*, Aug.30, 2019. https: //www.forbes. com/sites/daveywinder/2019/08/30/tesla - has - facepalm - moment - as - hackers - defeat - fixed - model - s - security/?sh=39f1d5884135.