https://doi.org/10.24867/FUTURE-BME-2024-119 Review paper

CYBERSECURITY RISKS WHILE DRIVING CAR

Miloš Stanojević[1] [0000-0001-8100-9864], *Mladen Babić*[2] [0000-0002-8398-7044], *Srđan Tegeltija*[3] [0000-0002-9307-445X], *Gordana Ostojić*[4][0000-0002-5558-677X]

Abstract

In recent years, the automotive industry has experienced a significant transformation through the application of new technologies that enable the car to communicate with the outside world. This technological revolution has brought numerous advantages in terms of the safety of road users, comfort, and efficiency. Still, at the same time it has opened the door to new challenges in the field of cyber security. Also, newer vehicles increasingly rely on the use of a number of sophisticated technologies that include sensors, cameras, GPS, radar, LiDAR, and advanced computer systems. All the mentioned systems can be susceptible to cyber-attacks, which must not be allowed in order to avoid unwanted consequences. This paper explores current threats and vulnerabilities affecting vehicle cyber security, including attacks on network systems, unauthorized access to control modules, data security as well as software manipulation.

Key words: *autonomous vehicles, driving, cyber-attacks, network, unauthorized access*

1. Introduction

Autonomous vehicles are a set of advanced technologies that aim to revolutionize and improve road safety. These vehicles use multiple sensors and artificial intelligence to sense the environment and make independent decisions. AVs represent a significant advance in transportation, as they promise to reduce human error on the road, bring greater road safety, and provide mobility for people who are unable to drive traditional vehicles. However, AVs still face a number of challenges, including resistance to different weather conditions, foolproof cybersecurity and public acceptance of the use of such vehicles in everyday life.

[1] University of Novi Sad, Faculty of Technical Sciences, Serbia, stanojevicmilos@uns.ac.rs
[2] University of Novi Sad, Faculty of Technical Sciences, Serbia, mladen.babic@uns.ac.rs
[3] University of Novi Sad, Faculty of Technical Sciences, Serbia, srkit@uns.ac.rs
[4] University of Novi Sad, Faculty of Technical Sciences, Serbia, goca@uns.ac.rs

2. Autonomous Vehicles Levels and Vulnerabilities

The process of automation in vehicles involves several different levels, with each level of automation representing a different degree of autonomy. The National Highway Traffic Safety Administration (NHTSA) has proposed the following six-level categorisation of autonomous vehicles (NHTSA, 2024):

- No automation (level 0): The vehicle is fully controlled by the driver, who controls all functions such as steering, acceleration, and braking.
- Driver assistance (level 1): The vehicle is still under the control of the driver but has built-in driving aids such as automatic braking or lane departure warning.
- Partial automation (level 2): At this level, the vehicle is equipped with more advanced systems that can control the acceleration, deceleration, and steering of the vehicle, but the driver must be present and actively controlling the vehicle to be able to take control if necessary. .
- Conditional automation (level 3): The vehicle is capable of controlling all key driving elements under some controlled conditions. However, the driver must be present and ready to take control of the vehicle if requested by the system.
- High level of automation (level 4): A vehicle at this level can independently perform all necessary driving tasks in all conditions. The driver still has the option to take control of the vehicle, but this is not mandatory.
- Full automation (level 5): The highest level of automation. Such vehicles are capable of performing all necessary driving functions throughout the journey without human intervention.

As more advanced technologies are incorporated into autonomous vehicles, these vehicles become increasingly vulnerable to cyber threats (Harris, 2024). Potential hackers can exploit these cyber vulnerabilities, posing a threat to both road safety and user data security, whether motivated by simple curiosity or malicious intent. The following are examples of prominent attack vectors for autonomous vehicles that can compromise security:

- Key hacking: The key fob technology used in almost all vehicles today can be a target for attack. By using a device to amplify the signal, hackers can gain unauthorised access to the vehicle and even the ability to remotely start the vehicle (Algarni & Thayananthan, 2022).
- CAN bus attacks: Because the CAN bus lacks encryption and protection mechanisms in its basic design and is used as the current standard vehicle networking protocol, it can be a target for hackers. By exploiting vulnerabilities in the CAN bus, hackers can take over some of the vehicle's basic functions.
- Hacking the in-car entertainment system: As the in-car entertainment system uses technologies such as Bluetooth, OBD-II, Wi-Fi, and other

similar technologies, it can easily become a target for hackers and allow hackers to gain access to all other parts of the autonomous vehicle system.

- Theft of user information: Given the large amount of user data stored in autonomous vehicles, these vehicles are becoming prime targets for cybercriminals. By hacking into a vehicle's system, hackers could steal private information about both the vehicle and its owner and driver.
- Attacks from the sensor layer: Autonomous vehicles rely heavily on systems that use a range of advanced sensors, such as lidar, millimetre radar, cameras, and GPS. While these systems improve the safety and efficiency of vehicles, they also introduce new vulnerabilities that can have serious implications for road safety.

The wide range of potential attack vectors shows that one of the imperatives in the development of autonomous vehicles is to improve cybersecurity measures. A compromised vehicle poses a significant threat to all road users, which is why this part of the research related to autonomous vehicles is very important. This chapter presents the vulnerabilities of autonomous vehicles related to the On-Board Diagnostic (OBD) port, then to the Global Positioning System (GPS), as well as the vulnerabilities of sensor systems such as LIDAR and cameras.

2.1 Onboard Diagnostic Port (OBD) Vulnerability

The OBD port in both traditional and autonomous vehicles is a key component that provides access to gather diagnostic information. By connecting an external device to an OBD port, it is possible to send and receive data from the vehicle's ECU. Such an open connection can be used for malicious attacks on the vehicle system. One of the potential problems is unauthorised access to the vehicle; if an attacker had physical access to the OBD port, they would be able to connect external devices to extract data or even reprogram the vehicle's systems, which could lead to unauthorised control of the vehicle. As some vehicles have OBD ports that support wireless communications (Wi-Fi or Bluetooth), attackers can access the vehicle remotely without the need for physical access. One of the main problems is the lack of encryption, which means that data can be intercepted and manipulated. This can be a major problem if the intercepted data includes commands to critical systems such as steering, braking, or acceleration. In addition, the OBD port could give attackers access to a wide range of in-car information, such as the vehicle's location, speed, and even the personal details of the driver and passengers. Finally, the OBD port could be used to introduce malicious software that could alter the behaviour of the autonomous vehicle, posing a significant risk to road safety.

2.2 Global Positioning System (GPS) Vulnerability

The Global Positioning System (GPS) enables autonomous vehicles to accurately track their location and navigate routes, which is very important for their functioning. However, this dependence creates a potential vulnerability that can be exploited by malicious individuals. If the security of the GPS system were compromised, hackers could potentially manipulate the signals, provide inaccurate information about the exact location of the vehicle, and even cause vehicle collisions, posing a serious threat to road safety (Kumar et al., 2018).

Attacks on the GPS system of autonomous vehicles take two forms: jamming and spoofing. A jamming attack is the emission of a stronger signal on the same frequency as GPS, causing temporary interference (Hu & Wei, 2009). A spoofing attack is a more subtle form of attack where the attacker emits fake GPS signals designed to mimic authentic ones. This type of attack causes the receiver to inadvertently accept false data as genuine. A spoofing attack would typically involve first jamming GPS signals to block the real ones, and then broadcasting spoofed signals to fool the system (Ahmad et al., 2019).

A well-executed attack on an autonomous vehicle's GPS system can seamlessly change the vehicle's location by transmitting a strong, false signal. Various defences, such as tracking identification codes, satellite signals and time intervals, can be used to counter such attacks. As the signal strength is around 163 decibel watts, blocking all higher frequency signals could also be one of the solutions to attack the GPS system (Yang et al., 2019). In their research, the authors developed an antenna-based method that combines anti-jamming and antispoofing techniques for GPS receivers. Currently, there is no fully reliable and practical solution to these attacks on the GPS system of autonomous vehicles. The only solution that can fully guarantee the security of the GPS system is the use of military-grade cryptography.

2.3 LiDAR System Vulnerability

One of the key components of any autonomous vehicle is the LiDAR system, which measures distance. By emitting pulses of light and measuring the time it takes for these pulses to reflect off distant surfaces, they create a three-dimensional map of the vehicle's surroundings. The LiDAR system's laser pulses, which are generated hundreds of times per second, are typically reflected off a rotating mirror to create a scan. If the vehicle can produce additional pulses, also known as echo signals, it can detect objects in different weather conditions.

As the LiDAR system is responsible for creating a three-dimensional image of the vehicle's surroundings, i.e. detecting obstacles around the vehicle, the safety of this system is crucial to maintaining road safety. One of the possible threats to this system is real signal attacks, which are a version of replay attacks that aim to change the actual positions of existing obstacles by broadcasting a new original signal from a changed location. To carry out such an attack, only two transmitters and one receiver are needed, as shown in (Petit et al., 2015).

Another possible threat is the spoofing signal attack, which is an extension of the real signal attack. The aim of such an attack is to create phantom objects by transmitting a signal at the same frequency as the scanner. A LiDAR system typically waits for incoming reflections for at least 1.33 microseconds, meaning that if an attacker could inject a signal into this time window, they would be able to successfully inject false signals into the LiDAR and create false objects in the space around vehicles.

Attacks on the LiDAR system of autonomous vehicles can be very dangerous, with some attacks potentially leading to fatal accidents, especially on highways. For these reasons, the security of this system is one of the most important things to work on. One possible solution could be the use of unpredictable LiDAR. Such a LiDAR would skip pulses but continue to listen for incoming pulses. Another solution would be to reduce the duration of the LiDAR pulse, thus reducing the attack window in the sensor, although reducing the time would result in a reduction in the working range of the sensor (Petit et al., 2015). Another possible solution would be to encode the LiDAR pulses to mitigate these attacks.

2.4 Vulnerability of Camera in Autonomous Vehicle

Cameras in autonomous vehicles are used as optical eyes, providing digital video of the external environment. They are used in various autonomous vehicle functions such as lane tracking, traffic sign recognition, and headlight detection (Bahlmann et.al, 2005; Cheng et.al 2006).

One of the major vulnerabilities of camera systems is the possibility of being temporarily or permanently blinded by targeted light jamming. Such an attack could pose a significant risk to occupant safety, particularly in situations where the vehicle's ability to detect key traffic signs is compromised (Petit et al., 2015).

A similar form of attack exploits the recovery time required by cameras after exposure to high intensity light. During this time, autonomous vehicles may be more vulnerable to undetected obstacles. This type of attack could be carried out from any direction, front, rear, or even from an old vehicle, by switching a strong light source on and off (Petit et al., 2015).

One of the solutions to the problems described above would be to use a configuration consisting of a large number of cameras, with each camera recording the same field of view. In this situation, the attacker would have to confuse all the cameras at the same time, which would certainly make his job more difficult. Also, the use of a removable near-infrared filter could allow selective filtering of near-infrared light, increasing the camera's resistance to light-based attacks. And another way to protect would be to use photochromic lenses, which have the unique ability to change colour and block certain wavelengths of light (Petit et al., 2015).

2.5 Vulnerability of Ad Hoc Network in Autonomous Vehicle

The Ad Hoc network of autonomous vehicles consists of two main communication channels, namely vehicle-to-vehicle (V2V) communication and vehicle-to-infrastructure (V2I) communication. V2V communication is based on the use of peer-to-peer networking principles, allowing vehicles to establish connections with each other. The V2V communication system is based on the IEEE 802.11p protocol and is built on the principle that vehicles within a certain radio range can automatically form an ad hoc network. Vehicles are network nodes that can exchange key information such as coordinate positions, directions, metric speeds, and many other data. V2I communication allows vehicles to connect to embedded electronic devices in the wider transport infrastructure system, such as traffic lights, information boards, and other similar devices. The information exchanged between vehicles and infrastructure can be used for a variety of applications, including improving traffic management, optimising traffic flow, promoting fuel efficiency, and reducing environmental impact.

V2V and V2I communication systems have significantly advanced the development and efficiency of autonomous vehicles, but these vehicle-to-vehicle communications are also vulnerable to various cyber threats. Ensuring system availability is a key aspect of the security framework for autonomous vehicles. One of the potential threats is denial of service (DoS) attacks, which can drain network resources and disrupt vehicle operations. Effective countermeasures include authentication measures, anomaly detection systems, and cryptographic solutions. It is also possible to infiltrate the vehicle system through V2V and V2I communications and install malicious software, such as a computer virus, to compromise the software infrastructure of autonomous vehicles. The use of firewall technology and anti-malware systems is recommended to protect against such threats (Pathre, 2013).

3. Discussion

Considering that AV vulnerabilities are numerous, and they are not limited to those already mentioned since they are only limitations related to cybersecurity, quantifying the exact percentage of each vulnerability is analysed. This is challenging due to the dynamic nature of the technology and varying degrees of exposure depending on the vehicle's architecture, the manufacturer’s cybersecurity measures, and evolving threat landscapes. However, based on general industry assessments and the prominence of certain risks, here’s a breakdown with approximate estimations:

1. OBD vulnerability 5-10%, since requires physical access to the vehicle, which reduces its exposure compared to remote vulnerabilities. However, in cases where an attacker gains physical access, they could use the OBD to exploit the vehicle’s systems.
2. GPS vulnerability 10-15%, significant, but the use of multiple navigation systems in AVs can somewhat mitigate the risks. Therefore, it is placed in the 10-15% range, reflecting the importance of GPS while acknowledging the presence of complementary systems that reduce sole dependency on it.
3. LiDAR System vulnerability 20-25%, reflects the importance of LiDAR to overall system function and the potential dangers posed by spoofing, jamming, and environmental factors.
4. Camera vulnerability 15-20%, due to their importance and susceptibility to adversarial and environmental interference. This reflects the medium-

to-high risk posed by compromised camera systems, tempered by the use of redundant sensors like LiDAR and radar.

5. Ad Hoc network vulnerability 15-20%, is significant due to its decentralized nature, lack of strong control mechanisms, and susceptibility to attacks where an attacker floods the network with unnecessary data, overwhelming the system and preventing legitimate communications between vehicles and infrastructure. This could disrupt real-time decision-making and safety-critical information exchanges.

These percentages are estimations and can vary depending on the specific architecture of the AV system, the cybersecurity measures in place, and the evolving landscape of both AV technology and cyber threats.

4. Conclusions

Autonomous vehicles are complex systems that rely on a variety of technologies, including sensors, machine learning algorithms, communication systems, and control mechanisms. Despite their promise to improve road safety and reduce human error, AVs have several vulnerabilities that could be exploited by malicious actors or could lead to failures in operation. In this paper, several vulnerabilities were analysed, and estimations of vulnerability percentages are given. After thorough analysis, mitigation strategies should be proposed. Possible mitigation strategies can be end-to-end encryption, ensuring that communications between AVs, infrastructure, and cloud servers are encrypted can reduce the risk of man-in-the-middle attacks; regular auditing and patching since continuous monitoring for vulnerabilities in both hardware and software, coupled with timely patching, is crucial for minimizing risk, and implementation of fail-safe mechanisms, where a robust fail-safe system will be built that ensures that even when attacks or failures occur, AVs can safely bring themselves to a halt.

Acknowledgments

This research has been supported by the Provincial Secretariat for Higher Education and Scientific Research (Contract No. 000659162 2024 09418 003 000 000 0001/2) through project (Cybersecurity System for Monitoring the Health Status of Drivers of Semi-Autonomous Cars Supported by Artificial Intelligence) and Ministry of Science, Technological Development and Innovation (Contract No. 451-03-65/2024-03/200156) and the Faculty of Technical Sciences, University of Novi Sad through project “Scientific and Artistic Research Work of Researchers in Teaching and Associate Positions at the Faculty of Technical Sciences, University of Novi Sad” (No. 01-3394/1).

REFERENCES

[1] Ahmad, M., Farid, M. A., Ahmed, S., Saeed, K., Asharf, M., & Akhtar, U. (2019, January). Impact and detection of GPS spoofing and countermeasures against spoofing. In *2019 2nd International Conference on Computing, Mathematics and Engineering Technologies* (iCoMET) (pp. 1–8). IEEE. ISBN 978-1-5386-9509-8.

[2] Algarni, A., & Thayananthan, V. (2022). Autonomous vehicles: The cybersecurity vulnerabilities and countermeasures for big data communication. *Symmetry*, *14*(12), 2494. https://doi.org/10.3390/sym14122494

[3] Bahlmann, C., Zhu, Y., Ramesh, V., Pellkofer, M., & Koehler, T. (2005, June). A system for traffic sign detection, tracking, and recognition using color, shape, and motion information. In *IEEE Proceedings. Intelligent Vehicles Symposium, 2005* (pp. 255–260). IEEE. https://doi.org/10.1109/IVS.2005.1505111

[4] Cheng, H. Y., Jeng, B. S., Tseng, P. T., & Fan, K. C. (2006). Lane detection with moving vehicles in the traffic scenes. *IEEE Transactions on intelligent transportation systems*, *7*(4), 571–582. https://doi.org/10.1109/TITS.2006.883940

[5] Hu, H., & Wei, N. (2009, December). A study of GPS jamming and anti-jamming. In *2009 2nd international conference on power electronics and intelligent transportation system (PEITS)* (Vol. 1, pp. 388–391). IEEE. https://doi.org/10.1109/PEITS.2009.5406988

[6] Harris, J. R. (2024, September 01). Can Driverless Vehicles Be Hacked? Harris Lowry Manton. https://www.hlmlawfirm.com/blog/can-driverless-vehicles-be-hacked/

[7] Kumar, A. D., Chebrolu, K. N. R., & KP, S. (2018). A brief survey on autonomous vehicle possible attacks, exploits and vulnerabilities. arXiv preprint arXiv:1810.04144. https://doi.org/10.48550/arXiv.1810.04144

[8] NHTSA. (2024, September 03). Automated Vehicles for Safety. NHTSA. www.nhtsa.gov/technology-innovation/automated-vehicles-safety

[9] Pathre, A. (2013). Identification of malicious vehicle in vanet environment from ddos attack. *Journal of Global Research in Computer Science*, *4*(6), 30–34. https://www.rroij.com/open-access/identification-of-malicious-vehicle-in-vanet-environment-from-ddos-attack-30-34.pdf

[10] Petit, J., Stottelaar, B., Feiri, M., & Kargl, F. (2015). Remote attacks on automated vehicles sensors: Experiments on camera and lidar. *Black Hat Europe*, *11*(2015), 995. https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf

[11] Yang, Q., Zhang, Y., Tang, C., & Lian, J. (2019). A combined antijamming and antispoofing algorithm for GPS arrays. *International journal of Antennas and propagation*, *2019*(1), 8012569. http://doi.org/10.1155/2019/8012569