Autonomous Vehicles: Addressing Security Concerns and Remedies

Liana Davis
Old Dominion University
Norfolk, Virginia, USA

Ldavi029@odu.edu

***Abstract*— As autonomous vehicles venture to revolutionize transportation by eliminating the need for human operation, they also come with significant cybersecurity risks. These vehicles are highly reliant on built-in systems, making them vulnerable to hacking, control disruptions, and incapacitation. This paper discusses current security risks facing self-driving cars, highlights real-world hacking incidents, and explores emerging threats from technologies like AI and smart city integration. It also examines possible solutions and emphasizes the need for proactive cybersecurity measures from manufacturers, developers, and regulators to ensure the safe future of autonomous travel.**

I. Introduction

Autonomous vehicles have gone from science fiction to real life machines cruising down highways. They use sensors and software to navigate without human input. Although the technology promises safer roadways and more convenient travel, it opens up a whole new world of cybersecurity risks. These vehicles are particularly vulnerable to attacks as they depend heavily on complicated systems that constantly share data with each other, surrounding infrastructure, and cloud services.

As autonomous cars are connected to a number of external networks including cloud services, traffic control, and navigation satellites, eachadded link represents an additional point of entry for the attacker. While this connectivity is necessary for optimizing operations, it significantly expands the attack surface upon which malicious actors can exploit.

Autonomous vehicles are particularly vulnerable to cyberattacks through various entry points because they utilize sensors along with control units and communication protocols and AI decision-making units. Both the internal network of the car and its wireless interfaces like Bluetooth and GPS and cellular connections create possible vulnerabilities throughout the system. The vulnerable areas can be used by hackers to hijack steering systems and brake functions and to completely immobilize the car. The absence of standardized cybersecurity protocols among manufacturers lays bare the problem because different systems have varying degrees of exposure and protection. A small security flaw could have fatal or dangerous implications. [1]

Among the more disturbing emerging vulnerabilities is one involving vehicle-to-everything (V2X) communications, where cars exchange information with traffic lights, road sensors, and other vehicles. If those communications are hacked or spoofed, attackers can confuse a self-driving car about road conditions, causing accidents. Similarly, LIDAR sensors can be tricked by broadcasting fake signals, causing a car to think there are objects in the roadway when there are not.

Autonomous vehicles have been demonstrated through multiple high-profile hacking incidents and real-world examples. In 2015, two security researchers gained remote control of a Jeep Cherokee by exploiting a vulnerability in its infotainment system, which allowed them to manipulate the brakes, steering, and transmission. The hack was done over the internet and it exposed how dangerous even non-critical systems can become when they're connected to core vehicle functions. Another case involving Tesla vehicles showed researchers being able to trick the system by using fake road signs and GPS spoofing, showing that even advanced AI can be manipulated. These incidents highlight the real, tangible risks that exist today, proving the fact that as tech evolves, so do the threats. [2]

Other researchers have demonstrated attacks through over-the-air (OTA) software updates, a feature utilized by many modern vehicles to patch vulnerabilities. If attackers can intercept or mimic an OTA update, they could install malware right into the vehicle's systems. In addition, key fob replay attacks allow hackers to unlock and ignite cars by capturing the wireless communication between a vehicle and its key fob, just to demonstrate how easy it is to bypass conventional defenses

Autonomous Vehicles possess a range of devices, protocols, and applications that offer multiple lines of attack. Its weakest link is the CAN BUS that manages all the communications between different components of the automobile such as the brakes, steering, and engine

management. It was originally designed with minimal thought for cybersecurity, and
therefore, it is fairly simple to take advantage of if attackers have remote or physical access. Wireless technologies like Bluetooth and Wi-Fi also present risks, especially if they are not adequately secured or patched. Even attacks aim at over-the-air update systems that deliver software patches to cars directly. Components like navigation, entertainment systems, and driver assist technologies can all be means for more critical intrusions if vulnerabilities are not identified or dealt with early on. Each stage of connectivity brings convenience but increases the risk of a system being compromised. [3]

Another issue on the increase is zero-day exploitation — previously unknown faults in car software that have yet to be remediated by the manufacturers. Those first discovering the vulnerabilities are the attackers who are able to exploit them before any defense measurescan be rolled out, gaining quiet access to critical systems without alerting anyone. Because cars increasingly are being upgraded digitally rather than physically, the threat of bulk zero-day exploitation is much more pronounced than for older vehicles.

As autonomous vehicles get more sophisticated, their cybersecurity risks are expected to get even more complex. Future models will likely depend even more on artificial intelligence, machine learning, 5G networks, and vehicle-to-everything communications, which will introduce new vulnerabilities. For example, intrusions into AI decision-making systems can cause a car to misinterpret traffic patterns or ignore important safety signals. [4] Future cars will also be more integrated into smart city infrastructure, offering even more ways for hackers to get in. As more elements of transportation become automated and remotely controlled, a single breach could have a cascading impact beyond one vehicle, with the potential to bring down entire networks of cars or citywide traffic grids.[4] Guarding against these threats in the future will require cybersecurity to be integrated into every phase of vehicle design, and not just added on later as an afterthought.

Even further down the line, cybersecurity experts are warning that advances in quantum computing could render today's encryption techniques obsolete. Once quantum computers are powerful enough, they'll be able to penetrate the secure channels protecting vehicle communications, leaving even the most secure systems open to attack. Future autonomous vehicles will need quantum-resistant security protections to be safe in a threat landscape that will only become more advanced.

The solution to these growing security concerns lies within manufacturers and developers, who must be held to a standard that prioritizes a proactive approach to cybersecurity. This means designing vehicles with security in mind from the beginning, rather than trying to patch problems after they've been discovered. A few recommended methods involve implementing an end-to-end encryption and secure authentication systems for all vehicle communications. Regular software updates delivered through secure channels can help prevent tampering. Intrusion detection systems can be integrated into vehicle networks to monitor suspicious behavior in real time. Beyond technical fixes, there also needs to be a collaboration between automakers, cyber experts, and regulatory bodies to establish and enforce standards across the entire industry. The more coordinated the defense, the harder it becomes for attackers to find weaknesses. [5]

Organizations like the International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) have created new cybersecurity standards, such as ISO/SAE 21434, that are tailored to protect vehicles from cyber threats. The standards provide frameworks that manufacturers can implement to build security into every stage of a vehicle's life cycle, from design to end-of-life, to provide a minimum baseline of attack resistance.

II. Conclusion

While autonomous vehicles are quickly developing and determining the way transportation will be in the future, they also remain grave cybersecurity risks that cannot be eliminated or avoided. The effects of security breaches will only get worse as the technology continues to mature and seep into the market. It is critical that manufacturers, coders, and policymaking bodies recognize these risks and take measures early before disastrous happenings start occurring. Incorporating strong cybersecurity into every element of a vehicle's design is a flat-out necessity. Confronting weaknesses early, promoting standards across the industry, and staying ahead of new attack methods keep the dream of safer, smarter transportation in sight. The future of autonomous vehicles is not only dependent upon innovation, but also the security and trust that envelops it.

References

[1] H. H. Chen, *Automotive Cyber Security: Introduction, Challenges, and Standardization*, 1st ed. Springer, 2020.

[2] A. Youssef et al., "Autonomous Vehicle Security: A Deep Dive into Threat Modeling," *arXiv preprint arXiv:2412.15348*, 2024.

[3] M. Pham and K. Xiong, "A Survey on Security Attacks and Defense Techniques for Connected and Autonomous Vehicles," *arXiv preprint arXiv:2007.08041*, 2020.

[4] Y. Liu et al., "On the Criteria for Cybersecurity and Risk Assessment Based on ISO/SAE 21434 for the Application of Autonomous Vehicle," in *Proc. 2022 Int. Conf. on Computer Science, Information Engineering and Digital Economy (CSIEDE 2022)*, Atlantis Press, 2022, pp. 134–143.

[5] S. Iqbal et al., "Simulating Malicious Attacks on VANETs for Connected and Autonomous Vehicle Cybersecurity: A

Machine Learning Dataset," *arXiv preprint arXiv:2202.07704*, 2022.

[6] "Autonomous Cars & Cyber Risks," HTTPCS Blog. [Online]. Available: https://blog.httpcs.com/en/autonomous-cars-cyber-risks/

[7] "Vehicle Cybersecurity," National Highway Traffic Safety Administration (NHTSA). [Online]. Available: https://www.nhtsa.gov/research/vehicle-cybersecurity