Autonomous Vehicles: Addressing Security Concerns and Remedies

Rami Abu Ismail
Department of Computer Science
Old Dominion University
Norfolk, VA, USA
rabu001@odu.edu

Abstract

Autonomous vehicles have become the one of the most preferred vehicle types in today's age. These vehicles use AI and advanced sensors to drive without human control. They also have advanced sensors that overlook all vehicle operations. While these new vehicles bring many convenience options they also bring many risks. One of the biggest risks includes cyber security risk. With these vehicles depending on technology, hackers can target the vehicles software and communication systems. In this paper, I'll explain the main problems with autonomous vehicles, give real world examples of these issues, and explain how these issues affect everyday transportation. I will also include solutions to these issues like government rules, detection systems and secure design solutions.

Index Terms

Autonomous Vehicles, Cybersecurity, IDS, V2X Communication, Secure OTA Updates.

I. Introduction

Autonomous vehicles are one of the favorites when it comes to vehicle choices in today's world. They have many different technologies to operate them. These technologies consist of high tech cameras, LiDAR, GPS systems, and the best computer systems. These all work together to understand the vehicle's surroundings and make driving decisions without needing human control. Even though these vehicles make decisions faster than humans which ultimately save many accidents, they also leave a large margin for cyber attacks.

Because these vehicles rely so heavy on sensors, software, and networks, this gives many hackers access points to gain control or cause disruptions in the vehicle. Gasoline based cars rely more on mechanical systems so they don't deal with many cyber attacks. Autonomous vehicles are just like computers who can drive, this makes them a very high risk in the cyber field.

II. Security Vulnerabilities in Autonomous Vehicles

These vehicles face many different cyber threats. Some of these threats include attacks on the vehicles sensors, perception systems, communication systems, and software. Each of these different types of attacks bring a different type of threat.

1. Attacks on Sensors and Perception Systems:

AVs use sensors like LiDAR, cameras, and radar to understand the environment.

Hackers can:
- Trick LiDAR into seeing fake objects.
- Use bright lights to blind the cameras.
- Modify road signs slightly so the AI misreads them.

2. Communication System Exploits:

AVs talk to other vehicles and road systems using communication. Problems include:
- Man-in-the-Middle (MitM) attacks that change messages.
- Replay attacks using old data.
- Denial-of-Service (DoS) attacks that block real-time information.

3. Software and Firmware Weaknesses:

Like any software, AV systems can have bugs or flaws.

Some problems are:
- Buffer overflows that let hackers take control.
- Weak passwords or authentication systems.
- Old software that hasn't been updated.

III. Real-World Incidents and Examples

1. Jeep Cherokee Hack (2015): Researchers remotely accessed a Jeep and took control of its steering and brakes by breaking into the infotainment system.

2. Tesla Model S Hack (2016): A team of Chinese hackers accessed the vehicle's control system remotely and could manipulate doors and brakes.

3. Kia Hack (2024): Security experts found that the car's mobile app allowed unauthorized users to unlock or start the car due to poor API security.

IV. Impact on Current and Future Transportation

These attacks have serious effects:
- Safety: If hackers control AVs, they can cause crashes.
- Trust: People may not feel safe using AVs.
- Legal and Financial: Companies could face lawsuits and high costs from recalls.
- Regulation: Governments may slow down AV deployment until security improves.

V. Solutions and Remedies

1. Security by Design:
Designing vehicles with security from the beginning helps reduce risks. Use threat modeling, secure coding, and regular testing.

2. Intrusion Detection Systems (IDS):
IDS tools monitor the vehicle's system for unusual behavior. They help spot attacks early.

3. Over-the-Air (OTA) Updates:
Manufacturers should send regular, secure software updates to fix bugs. These updates must be encrypted and verified.

4. Stronger Laws and Regulations:
Governments can require companies to meet certain cybersecurity standards and share data about threats.

VI. Conclusion

Although autonomous cars may revolutionize transportation, cybersecurity has to be given first importance. Targeting several facets of the system, hackers pose major concerns. Better security, smart tool use like IDS, and regulatory cooperation help us create safer and more trustworthy autonomous systems by developing AVs.

References

[1] C. Miller and C. Valasek, 'Remote Exploitation of an Unaltered Passenger Vehicle,' Black Hat USA, 2015.

[2] K. Koscher et al., 'Experimental Security Analysis of a Modern Automobile,' IEEE Symposium on Security and Privacy, 2010.

[3] S. Checkoway et al., 'Comprehensive Experimental Analyses of Automotive Attack Surfaces,' USENIX Security Symposium, 2011.

[4] KPMG, 'The Autonomous Vehicle Readiness Index,' 2020. [Online]. Available: https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/06/avri.pdf

[5] J. Petit and S. E. Shladover, 'Potential Cyberattacks on Automated Vehicles,' IEEE Transactions on Intelligent Transportation Systems, vol. 16, no. 2, pp. 546–556, 2015.

[6] D. Lin, 'Secure OTA Updates for Vehicles: Challenges and Directions,' ACM Conference on Embedded Networked Sensor Systems, 2022.

[7] B. Ghena et al., 'Green Lights Forever: Analyzing the Security of Traffic Infrastructure,' USENIX Security Symposium, 2014.