Cybersecurity in Autonomous On-Road Motor Vehicles focusing on connectivity and perception systems

Intelligent Systems Engineering

Alberto Paganelli

Alma Mater Studiorum - University of Bologna

January 19, 2025

Table of Contents

Introduction

This review provides a comprehensive overview of the current state of research on security in autonomous vehicles, with a particular focus on autonomous cars, a rapidly evolving sector. Key points:

1. Cybersecurity threats
2. Cybersecurity by design and standards
3. Actual solutions
4. Future directions

The ethical implications of the technology or the comparison between human-driven and autonomous vehicles in terms of accidents and fatalities is not be covered, same for social implications that are not deepened.

Table of Contents

Methodology I

Selection Criteria

1. Relevance: focus on cybersecurity.
2. Quality: reputable journals, conference proceedings, or books.
3. Recency: five years limit.
4. Diversity: not limited to only cybersecurity aspects.
5. Accessibility: online accessibility.

Search Strategy - main databases

1. Google Scholar.
2. IEEE Xplore and others.

Some principal queries can be found on the document, in the corresponding section.

Methodology II

Phases

1. General search: helps to understand the current state, main threats and some general aspects of the AVs.
2. Specific search: deep cybersecurity aspects in AVs, such as threats, standards, industry practices, techniques, and future trends.

Methodology III

Limitations

1. As mentioned ethical, legal, and social implications.
2. Only major threats are considered.
3. The interdisciplinary nature of the topic.
4. Advanced machine learning algorithms may not be covered comprehensively.
5. Limited access to publications was mitigated through academic databases.

Motivations

In many ways, the current state of AV security mirrors the early days of the web, where vulnerabilities were abundant, and solutions were still emerging. My interest lies in exploring the intersection between modern vehicles and cybersecurity, combining two of my passions.

The goal is to understand the state of the art and conclude with a thoughtful (technical) reflection on the future of secure autonomous systems.

Research Questions

1. *What are the most significant* ***cybersecurity threats*** *facing autonomous vehicles, and how these threats evolve with advancements in communications and other emerging technologies?*
2. *What existing* ***standards and regulatory frameworks*** *govern cybersecurity by design in autonomous vehicles, and how effectively do they address current and future security challenges?*
3. *What cybersecurity* ***solutions and practices*** *have been implemented by autonomous vehicle manufacturers, and how do they align with best practices in secure software development and system resilience?*
4. *What* ***future trends and emerging technologies****, such as artificial intelligence and blockchain, are being explored to enhance the cybersecurity of autonomous vehicles, and what challenges do they pose in real-world applications?*

.

Table of Contents

Communication

1. Vehicle-to-Vehicle (V2V)
2. Vehicle to Infrastructure (V2I)
3. Vehicle to Everything (V2X)

.
Multiple classifications can be done but this review focuses on this one, as it highlights concerns related to technological separations.

Tampering

What emerge from literature is that nearly 79.6% of all automotive attacks have been remote attacks[KTP22].

Table of Contents

Main Sensors

1. Cameras
2. LiDAR (Light Detection and Ranging)
3. Radar (Radio Detection and Ranging)
4. Etc.

.

Tampering

The more sensors there are, the more the attack surface increases. It's not a news, that's normal. What is more dangerous for me is the ease of temperament of these sensors.

Table of Contents

Cybersecurity-by-design standards

1. **ISO/SAE 21434**: is a joint standard developed by the ISO and the SAE to address the cybersecurity of road vehicles. New concept of Cybersecurity Assurance Levels, which categorize the severity of cybersecurity threats and the corresponding measures to mitigate them.
2. **UNECE WP.29 R155**: It is a mandatory regulation by July 2024. It outlines requirements for original equipment manufacturers and tier suppliers to implement cybersecurity measures in new vehicles.

.

Correlations

Their complementary nature allows manufacturers to leverage each other's documentation and processes to meet each other's requirements, promoting cybersecurity in road vehicles.
The problem remains the huge gap between legislation and IT.

Table of Contents

Actual solutions

1. **Secure Software Development Life-Cycle**: systematic and structured approach to developing software that prioritizes security at every stage of the development process.
2. **Intrusion Detection and Prevention Systems**: helps to detect and prevent unauthorized access to the vehicle's network, monitor the behavior of connected devices, and identify anomalous activities that may indicate a cyberattack.
3. **Secure Over-the-Air Updates**: to address security vulnerabilities and bugs when they are discovered.

.

Table of Contents

Future directions

1. **Artificial Intelligence**: used to recognize threats, deploy adaptive security systems, mitigate risks, identify anomalies, and, in some instances, automatically isolate potentially compromised components or reroute communication paths to counterthreats.[Dur+22]
2. **Blockchain**: can be used to secure communications, support data integrity or identity management. Also for transparent and secure storage of data, reputation and trust management, and forensics applications.
3. **Quantum Computing**: quantum key distribution, moving to quantum-resistant cryptography.
4. **Digital Twins**: can be used to create a virtual model that mirrors the vehicle's operations and interactions where attack surface, vulnerabilities and penetration tests can be analyzed.

.

Table of Contents

Conclusions

Existing defenses like intrusion detection, updates, and current standards offer **some protection** but are inadequate against evolving threats.

Key challenges include a **lack of unified security standards**, latency, scalability, and resource limitations. To secure AVs, data integrity, secure communication, and sensor resilience must be prioritized.

Collaboration, **knowledge sharing**, and joint research are vital to address emerging vulnerabilities.

Future AV cybersecurity will focus on adaptive, resilient systems, leveraging AI, machine learning, digital twins, and blockchain to improve threat detection and secure communications, while ensuring proper regulation to maintain **public trust**.

[Dur+22] Irmina Durlik et al. "Cybersecurity in Autonomous Vehicles—Are We Ready for the Challenge?" In: *Electronics* 13.13 (2022), p. 2654. DOI: 10.3390/electronics13132654. URL: https://doi.org/10.3390/electronics13132654.

[KTP22] Vipin Kumar Kukkala, Sooryaa Vignesh Thiruloga, and Sudeep Pasricha. "Roadmap for Cybersecurity in Autonomous Vehicles". In: *IEEE Consumer Electronics Magazine* 11.6 (2022), pp. 13–23. DOI: 10.1109/MCE.2022.3154346. URL: https://doi.org/10.1109/MCE.2022.3154346.