ISSN: 2583-9888
DOI: doi.org/10.51219/JAIMLD/suresh-sureddi/371

URF PUBLISHERS
connect with research world

Journal of Artificial Intelligence, Machine Learning and Data Science

https://urfpublishers.com/journal/artificial-intelligence

Vol: 2 & Iss: 3

Research Article

Mitigating Escalating Cybersecurity Threats in advanced Automotive Systems

Suresh Sureddi*

Citation: Sureddi S. Mitigating Escalating Cybersecurity Threats in advanced Automotive Systems. J Artif Intell *Mach Learn & Data Sci 2024*, 2(3), 1665-1668. DOI: doi.org/10.51219/JAIMLD/suresh-sureddi/371

Received: 03 September, 2024; **Accepted:** 28 September, 2024; **Published:** 30 September, 2024

***Corresponding author:** Suresh Sureddi, USA, E-mail: ssureddi@gmail.com

ABSTRACT

With the rise of connected cars and their integration with various networks and systems, there is a higher risk of cyberattack targeting these vehicles. Hackers can exploit vulnerabilities in the car's software or network to gain unauthorized access and control over critical functions. This scholarly article explores into the escalating challenges, vulnerabilities and defense measures essential for safeguarding intelligent connected vehicles against cyber threats.

Keywords: Connected Vehicles, Cybersecurity, Connectivity, CAN (Controller Area Network), Autonomous, V2X, Artificial Intelligence.

1. Introduction

Vehicle OEMs and their suppliers are integrating increased connectivity features to provide enhanced safety and user experience for their customers. Many advanced technologies, such as artificial intelligence, V2X (Vehicle-to-Everything), OTA(Over-the-air) updates, cloud computing, online subscription features and ADAS (Advanced Driver Assistance Systems), are widely used in cars. These technologies make connected vehicles more intelligent and provide comfortable services for people, but at the same time, the risk of cyber-attacks has become a growing concern.

Factors contributing to increased Cybersecurity risks in automotive and their countermeasures:

1.1 Cyber vulnerabilities overview:

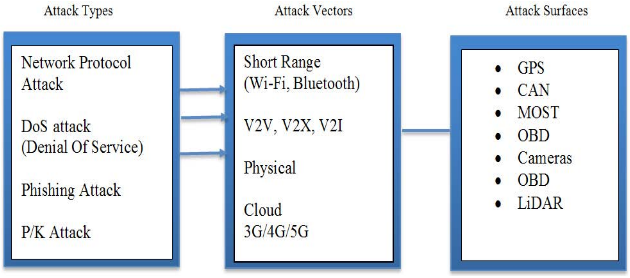

Figure 1: Overview of cyber-attack types, attack vectors and attack surfaces

- **Vehicle Networking Protocols**
- **MOST (Media Oriented System Transport):** This network is used for media and infotainment and is less harmful as it is not directly connected to critical systems like Power train or engine related sensors. However, two types of attacks are possible on MOST, synchronization disruption and jamming. In synchronization attacks, hackers can send fake timing frames continuously and tamper with the synchronization of MOST. Whereas in jamming, hackers can send misleading messages and interrupt low-priority legitimate messages[1].
- **Counter Measures:** To address the above threats, source code authentication, encryption of exchanged messages and strict enforcement of firewalls can be considered.

CAN (Controller Area Network) and Flex ray:

- Most of the vehicle's ECUs (Electronic Controller Units) are connected to the vehicle CAN and Flex Ray networks. These network protocols lack the design of an information security mechanism at the beginning of their design, which makes them vulnerable to sniffing, replay or forgery of messages. The CAN message has poor confidentiality, the bus data is easy to capture and analyze and the availability and integrity cannot be guaranteed. There is no original address information in the CAN message, making it easy for the attacker to tamper with the message by injecting false information. Also, the arbitration mechanism is given priority in the CAN bus protocol, which can make attackers replay or flood the vehicle bus using sniffing.

- The OBD (On Board Diagnostics) port is used for vehicle diagnostics and ECU software updates. In this case, the diagnostic tool can gain access to the vehicle network over the CAN bus. This can be hacked by installing malware through a direct connection.

Countermeasures: Researchers have explored Security enhancement technologies for vehicle networks, which include,

Vehicle network data encryption technology[2]: The CAN bus's security solution can be divided into encryption, authentication and redesign of the protocol stack.

Cryptography-based methods focus on protecting the CAN bus from malicious messages, while the intrusion detection system (IDS) detects malicious messages.

Firewalls and intrusion prevention systems (IPS) can be considered for external interfaces to prevent access to the bus.

1.2. Vehicle Network Message Authentication Technology

Various lightweight message authentication protocols can be considered to protect vehicles from camouflage attacks.

Vehicle network Intrusion Detection Technology is more suitable for vehicle networks with limited resources and costs. This detection technology is further categorized into detection methods based on feature observation, information theory, statistical analysis and machine learning[2], etc.

- **Vulnerabilities in Smart key systems:** These systems eliminate the need for a physical key by depending on wireless communication between the vehicle and the key fob but may become vulnerable to cyber-enabled replay attacks (Signal replication by malicious actors leading to vehicle theft).
- **Countermeasure:** Tesla tried to overcome the issue by replacing the traditional RKE (Remote less Key Entry) design with a Bluetooth Low Energy (BLE) enabled key; however, this design, too, was vulnerable to relay attack and cost issues defeated it. The other countermeasures considered are rolling code[3] and separating the door control and engine unlock functions to avoid the problem of simply opening the door to drive the vehicle away.
- **Connected and Autonomous Vehicles (CAV)**
- V2X communications involves communication between Vehicle-to-Vehicle(V2V), Vehicle-to-Infrastructure(V2I), Vehicle-to-Pedestrian(V2P) and V2R (vehicle-to-roadside units). This communication is facilitated by VANET technology (Vehicular ad hoc networks). The cyber-attacks and countermeasures in V2X communication are categorized into,

Attacks on authentication: Authentication defines the ability to verify the legitimate sender of the message. The absence of a strong authentication mechanism has led to threats such as GPS spoofing and masquerading attacks. Researchers have suggested potential prevention and mitigation techniques, which include encryption, location algorithms, cryptography and artificial intelligence.

Attacks on availability: Availability defines that the authorized users shall have all the time access to network resources. Common attacks on availability include denial of service (DOS) attacks, jamming attacks and black-and-grey hole attacks. Studies on these attacks provided mitigation and detection mechanisms such as monitoring, packet detection and machine learning methods[4].

Attacks on integrity: Integrity confirms that the message has not been modified along the communication channel. Attacks on integrity include replay and false injection. Suggested prevention algorithms for these kinds of attacks include cryptography, timestamp verification, message verification and machine learning.

Attacks on non-repudiation: Non-repudiation means accountability. Any action performed on the network must be accounted for. In a repudiation attack, it is impossible to identify the sender of a message on the network. The authors use digital signatures, mutual authentication and certificate authorization techniques to address this concern. More studies have been performed to ensure accountability while maintaining privacy.

Attack of Confidentiality: Confidentiality protects the content of messages from unauthorized access by users. This kind of attack includes eavesdropping and man-in-the-middle attacks. Researchers have suggested Kalman filtering and deep reinforcement learning techniques to address this attack.

Attacks on Privacy: This includes protecting data such as the user's identity and position details of the sender. To address this security attack, studies suggested tree-based risk assessment, cryptography, location cloaking and encryption pseudonyms.

The above-discussed countermeasures, such as cryptography and Intrusion Detection Systems (IDS), are highly effective for preventing and detecting external attackers but less effective in internal attack situations. Also, these techniques are computationally expensive and limited to known attacks. To address these challenges, the focus of the research is turned towards evaluating the credibility of the sender and message through trust. Numerous studies such as Fuzzy logic, game theory, blockchain, RSU-based, cloud and edge-assisted frameworks have been done to improve the internal security of connected and autonomous vehicles using trust-based security solutions. However, there are some drawbacks that require further research to enhance security in connected and autonomous vehicles.

- **Cloud-based services:** OEMs and suppliers offering functionalities such as remote command execution and vehicle status monitoring to vehicles represent another potential weak point in the automotive data ecosystem.

Also, vehicles now regularly communicate with OEM and third-party cloud services for over-the-air updates and subscriptions. This expanded connectivity significantly increases the vulnerability to cyber-attacks.

In 2022, a vulnerability was identified in the MQTT broker of the HQT-401 telematics unit, which lacked the required authentication mechanisms. This flaw allowed attackers to manipulate the telemetry data[5]. In another instance, the lookout for vehicle data leaked via MQTT revealed several open brokers that lacked both authentication and password protection. Many unsecure MQTT servers accept write instructions from any subscriber, which opens the potential for attacks.

Over-the-air technology helps automakers and users avoid physical visits to the dealership by updating the software in the vehicle from remote over-the-cloud servers[6]. However, this technology introduces potential vulnerabilities regarding the authenticity and integrity of the updates.

Cloud-based Subscription management has transformed revenue models for OEMs and suppliers. However, this has also helped attackers generate revenue by jailbreaking features and avoiding the subscription fee.

Countermeasures: A cloud API is the main character of the whole network architecture and provides variable functions.

More secure API should be developed considering good practices, (1) Address AuthN, (2) Following the least privilege model, (3) Adopt data minimization, (4) Avoid incremental IDs, (5) Enforce rate limiting (6) Sanitize inputs and reject anything suspicious (7) implement proper security headers (8) Configure CORS to reduce attack surface (9) Don't reveal useful info in error messages (10) Use versioning and deprecate old APIs. Also, Cybersecurity cannot be one-time testing; it shall be part of the active SDLC (Software development life cycle) and security design and implementation shall run in parallel with the software development lifecycle.

AI-driven driver assistance and autonomous driving systems: Autonomous vehicles are susceptible to malicious interference. AI and ADAS (Advanced Driver Assistance Systems) depend on several sensors, cameras and algorithms to interpret the environment and make decisions. Generally, ADAS systems use sensors to capture the inputs, interpret the input data using AI models and then use actuators to drive the outputs. Sensor data, especially camera inputs, are vulnerable to attacks; for instance, when the camera sensors direct IR (Infrared) light, it can be misinterpreted as a red signal, causing the vehicle to perform unintentional breaking, called ghost breaking[7].

AI provides plenty of opportunities to address cyber security threats, which include,

AI-supported Intrusion Prevention Systems analyze large amounts of data from various sources in real-time to identify emerging threats, analyze attack methodologies and provide real-time threat intelligence reports. This allows cybersecurity experts to become more proactive and strengthen security measures before attacks happen.

AI-supported IDS (Intrusion Detection Systems): IDS can analyze large amounts of data in real-time, (1) identify suspicious activities, (2) Analyze network traffic and (3) Provide timely warnings to security teams. This helps it continuously learn from new threat patterns and update its algorithms.

AI can prevent attacks by analyzing messages through natural language processing to detect phishing attempts by recognizing (1) Suspicious patterns, (2) misleading information and (3) malicious URLs.

On the flip side, however, AI systems can become hackers' targets. Adversarial attacks, where small manipulations in data can cause AI systems to make incorrect decisions, present a significant risk. For instance, researchers demonstrated how slightly altered stop signs could cause Tesla's Autopilot system to misinterpret them, showing how vulnerable AI can be to carefully crafted attacks.

Also, AI can help attackers by gathering information about the target, educating the attacker on needed equipment and how to perform certain attack actions and help writing malicious code. It benefits from a reduction in attack times and easily provides needed expertise. AI can help attackers search for data easily to enhance attacks, create phishing emails and create deep fakes. AI (specifically chatbots) can also create polymorphic malware, which is very hard to detect.

Countermeasures will be needed to control the rising threat of AI-generated or enhanced attacks. AI systems are expected to become more adept at predicting and preventing attacks through continuous learning and adaptation. Companies are exploring the integration of quantum computing, which will strengthen AI capabilities by building unbreakable encryption methods and rapid detection of threats. Collaborative efforts of the auto industry are needed to establish standards and protocols. AI shall continuously monitor and ensure regulatory compliance in the automotive industry.

2. Conclusion

This article explores the several security breaches that can happen at any interface of the vehicle architecture; it can happen anywhere between the vehicle communication bus protocol level to the application level, which includes interfaces to the cloud, other vehicles and external infrastructure. Initially, automotive protocols are designed without considering security threats, but current scenarios require advanced security measures for these protocols to counter malicious attacks. Researchers are exploring Vehicle network Intrusion Detection Technology, which is suitable for vehicle networks with limited resources and cost. Also, in the case of CAV (Connected and autonomous vehicles), the researchers are exploring trust-based frameworks to address internal-type attacks as IDS helps address external-type attacks. Also, the cloud-based attacks were discussed and the factors to be considered while developing APIs were mentioned. Connected vehicle technology will rapidly change with the rapid transformation of AI. Vehicles connecting to the external world (Cloud, other vehicles and infrastructure) are changing rapidly. To maintain safety and security while increasing the number of connected vehicle functions, the automotive industry, academia and government bodies need to be aligned, especially in terms of safety standards. Safety standards and regulations should be reviewed and updated as technology advances as appropriate.

Design, implementation and testing of security methods should be an active part of the SDLC (Software development lifecycle) and should run in parallel with the software development lifecycle instead of giving emphasis to security at the later stage of the development cycle.

3. References

1. Rathore RS, Hewage C, Kaiwartya O, Lloret J. In-Vehicle Communication Cyber Security: Challenges and Solutions. Sensors, 2022;22:6679.

2. Guan T, Han Y, Kang N, Tang N, Chen X, Wang S. An Overview of Vehicular Cybersecurity for Intelligent Connected Vehicles. Sustainability, 2022;14:5211.

3. h t tps://vicone.com/files/rpt-automotive-cybersecurity-in-2022.pdf

4. Mwanje MD, Kaiwartya O, Aljaidi M, Cao Y, Kumar S, Jha DN, Naser A, Lloret J. Cyber security analysis of connected vehicles. IET Intell. Transp. Syst, 2024;18:1175-1195.

5. https://nvd.nist.gov/vuln/detail/CVE-2023-3028

6. N umaan Huq, M.Sc, Automotive Cyber Security - Emerging Risks and New Case Study Insights: ATZ Electronics, 2024;07-08.

7. h ttps://www.reddit.com/r/SelfDrivingCars/comments/10gngs6/ghost_braking_incidents_threaten_usefulness_of/