Université Libre de Bruxelles

Security Analysis of Automotive In-Vehicle Networks (CAN and Automotive Ethernet)

Students:
Amanor Deborah
Hassani Mortaza

Supervisor:
Prof. MÜHLBERG Jan Tobias

December 21, 2024

Contents

1 Abstract

Automotive In-Vehicle Networks (IVNs) serve as the backbone for communication between various components and Electronic Control Units (ECUs) inside a vehicle's architecture. These enable seamless integration and/or operation of critical systems, such as powertrain, infotainment, advanced driver-assistance systems (ADAS) and safety mechanisms. However, the protocols used in IVNs, such as Controller Area Network (CAN) and Automotive Ethernet, at first place were designed with a focus on efficiency, reliability, and real-time communication rather than security. As a result, they lack robust mechanisms to protect against modern cyber threats. With the increasing connectivity of vehicles to external networks, such as the internet and mobile devices, the attack surface has expanded significantly, exposing vehicles to potential cyberattacks. This report provides a comprehensive analysis of the security challenges and vulnerabilities associated with CAN and Automotive Ethernet, studying some real-world attack scenarios, and proposes mitigation strategies to enhance the security of modern automotive systems.

Keywords: *Automotive Ethernet, CAN, V2X, Security*

2 Introduction

With the shift towards software-defined vehicles, Autonomous vehicles and vehicle-to-everything (V2X) applications, there is an increasing demand for high bandwidth communication in the automotive domain. Over the years, automotive in-vehicle networks have comprised various protocols, ranging from high bandwidth, fault-tolerant ones supporting safety-critical applications such as Powetrain and braking system, to low bandwidth protocols supporting secondary applications like HVAC and body control module (BCM).

The Controller Area Network (CAN) has been the backbone of IVNs, providing reliable and deterministic communication for critical functions like engine control and braking systems. However, as vehicles become increasingly connected, CAN's limitations in terms of bandwidth and lack of built-in security pose significant challenges.

Automotive Ethernet has emerged as a promising alternative, offering higher bandwidth to support advanced applications like infotainment, telematics, and ADAS. Despite its lower bandwidth, CAN remains a vital component of IVNs, due to its deterministic and reliable timing properties.

Both protocols, however, face unique security challenges. CAN, as a legacy protocol, was not designed with modern security threats in mind, while Automotive Ethernet inherits vulnerabilities from traditional IT Ethernet, exposing vehicles to a broader attack surface. This research focuses on analyzing the security issues in these two critical in-vehicle network protocols.

3 Problem Statement

In-Vehicle Networks (IVNs) are critical for communication between Electronic Control Units (ECUs) and other components within the vehicle's Electrical/Electronic (EE) architecture. They support both onboard communication and external connectivity with offboard services. However, existing protocols, particularly CAN and Automotive Eth-

ernet (AE), exhibit significant security vulnerabilities. Modern intelligent vehicles face increasing threats as adversaries exploit these vulnerabilities to compromise vehicle safety. Emerging technologies such as Vehicle-to-Everything (V2X) communication and over-the-air (OTA) updates further expand the attack surface, introducing new challenges in ensuring the security and privacy of vehicle data. Given the safety-critical nature of the automotive domain, addressing these vulnerabilities is an urgent priority, hence the goal of our research.

3.1 Research Goal

1. Analyze the vehicle EE architecture trend:
    - Explore how future EE systems integrate CAN and AE to meet safety-critical and bandwidth-intensive needs.
2. Assess vulnerabilities in CAN and Automotive Ethernet and the several ways they could be exploited including potential use cases.
3. Propose Security Measures
    - Explore how security zoning and defense-in-depth can mitigate these threats.
    - Discuss Intrusion Detection Systems (IDS) for anomaly detection and their limitations.
4. Investigate emerging trends, such as the use of blockchain for IVN security.

3.2 Scope of Study

The automotive IVN, is made up of several networking protocols, CAN, CAN-FD, Automotive Ethernet, Flexray, LIN and MOST. However, for the scope of this project we will focus on CAN and Automotive Ethernet. This decision is based on the following considerations:

1. **Flexray:** Although it offers higher bandwidth and fault tolerance compared to CAN, its high implementation cost has limited its adoption. Additionally, the growing adoption of Automotive Ethernet is gradually phasing out FlexRay as the preferred high-bandwidth solution.
2. **LIN:** LIN is designed for low-bandwidth, cost-effective applications and is not used for safety-critical systems, making it less relevant to the scope of this project.
3. **MOST:** MOST is primarily used for multimedia and infotainment systems, which do not form part of the project's focus on safety-critical and core operational networks.

4 Methodology

To achieve the goal of this research, a comprehensive literature study was conducted to gain a thorough understanding of the domain, the vehicle EE architecture, and the IVN protocols used, as well as the security vulnerabilities and mitigations currently implemented.

4.1 Literature Study

The study focused on reviewing the following key papers:

1. **Security Issues with In-Vehicle Networks, and Enhanced Countermeasures Based on Blockchain** by Narayan Khatri et al.
    - Compares the security vulnerabilities of the various IVNs and proposes how blockchain can be applied for secure communication.
2. **In-Vehicle Communication Cyber Security: Challenges and Solutions** by Rajkumar Singh Rathore et al
    - Identifies key challenges in CAN and AE, and proposes security solutions such as IDS.
3. **Security Analysis of Ethernet in Cars** by Ammar Talic KTH, Sweden.
    - Focuses on vulnerabilities in Automotive Ethernet.

4.2 Research Questions

To guide the literature review, the following research questions were posed:

- **RQ1:** What is the current vehicle EE architecture and what is the future trend?
- **RQ2:** How are these IVNs (CAN and AE) enablers for the Vehicle EE architecture?
- **RQ3:** What are the key attack surfaces and vulnerabilities of CAN and AE?
- **RQ4:** What trade-offs are associated with implementing security measures?
- **RQ5:** How does fuzzing reveal vulnerabilities in CAN and AE?
- **RQ6:** What security measures are currently in use for CAN and AE?

4.3 Structure of the Report

The report is organized into the following sections

Section 3: Provides the background of the various vehicle EE architectures and their evolution to date, along with a brief description of the IVN protocols used within the vehicle EE architecture.

Section 4: Details the security issues and vulnerabilities found in CAN and AE.

Section 5: Analyzes three use cases of real-world attacks carried out on automotive vehicles and includes threat modeling for all.

Section 6: Discusses security mitigations based on our proposals and recommendations from other researchers.

Section 7: Addresses and answers the research questions posed for the study.

Section 8: Concludes the study with final thoughts and recommendations.

5 Background

This section presents study of available technologies used in vehicle communication.

5.1 The Vehicle E/E architecture

The E/E system architecture of automotive vehicles has evolved over the years from a flat backbone architecture where the backbone networking technology was CAN-based. As the number of ECUs connected to the backbone expanded and additional subnets and sub systems were introduced, data transport on the backbone became a bottleneck and as such the flat backbone architecture evolved to domain distributed and domain centralized architectures and now the future is zonal architecture.

5.1.1 Domain Distributed E/E Architecture

In this architecture, Electronic Control Units (ECUs) with similar functionalities are grouped into functional domains such as Telematics, Powertrain, Body, and Chassis. ECUs in different domains communicate with each other via a central gateway.

5.1.2 Domain Centralized E/E Architecture

Similar to the domain distributed architecture, ECUs are grouped into functional domains. However, in this setup, each domain has a Domain Control Unit (DCU) which manages and coordinates the operations within the domain. For inter-domain communication, Automotive Ethernet or CAN is used as the backbone. Intra-domain communication can occur via different networks, helping to segment and enhance security within the vehicle.

5.1.3 Zonal Architecture

The zonal architecture represents the future of vehicle E/E architecture, introducing high-performance compute nodes. This architecture supports the concept of the software-defined vehicle, where new functionalities are added through over-the-air updates rather than by replacing or adding ECUs. Key components include vehicle servers and zonal gateways, which facilitate efficient and flexible communication across the vehicle.

5.2 In-Vehicle Networking Technologies

The in-vehicle network is an enabler for the vehicle E/E architecture. It facilitates the transport of data among several ECUs within the same domain as well as between different domains. In-vehicle communication protocols in the E/E system are heterogeneous, consisting of CAN, Automotive Ethernet, LIN, Flexray and MOST protocols.

For communication between onboard and offboard services, a combination of both wireless and wired networking technologies is used. Wireless technologies such as Wi-fi, cellular networks and Bluetooth enable connectivity to cloud services this is usually housed in the telematics domain. Whereas classical Ethernet, 100 Base-TX or CAN is used for On-Board Diagnostics (OBD).

5.2.1 CAN

CAN is the most widely used in-vehicle networking protocol. It is a bus-based technology where all ECUs are attached and share the same wiring. CAN is a broadcast technology where every node can transmit and receive frames over the medium. To prevent collisions, the arbitration method is used where the node with the highest priority is allowed to communicate on the bus. The CAN bus consists of two twisted pair wires known as the (CAN High) and (CAN Low) which enhances immunity to EMI. Classical CAN supports data rates up to 1 Mbps and a payload of 8 bytes. However, a better version of CAN exists with improved data rates of 8 Mbps and an extended payload of 64 bytes.

5.2.2 Automotive Ethernet

Automotive Ethernet is a special type of Ethernet that fulfils the stringent requirements of EMC in the automotive environment [3]. It is also designed to ensure reliable and deterministic communication, which is crucial for safety-critical applications and real-time communication through the use of the protocols, AVB and TSN. Automotive Ethernet can currently support data rates of up to 10 Gbps[3], a significant improvement compared to the traditional in-vehicle networking protocols. This high data rate capability coupled with traffic prioritization and shaping (QoS)enables the support of advanced automotive applications such as autonomous driving and V2X . The AE technology is based on swithces which allows efficient data routing and minimizes latency making it suitable for the modern vehicle.

5.2.3 LIN

LIN is a low-cost serial communication protocol. Unlike CAN being a multi master communication protocol, LIN is a single master networking protocol. The data rate is up to 20 kbps making it a useful technology for low-speed, non-safety critical tasks such as comfort clusters, doors and seat

5.2.4 FlexRay

FlexRay evolved as an alternative for more demanding tasks which needed better performance than CAN could provide. It operates at a higher data rate of 10 Mbit/s and is used for applications such as Drive-by-wire, active suspension, and adaptive cruise control. FlexRay is an innovative communication protocol which combines event-driven and deterministic communication with static and dynamic segments. A static segment is reserved for deterministic data, while a dynamic segment is used for priority based event-driven communication

5.2.5 MOST

MOST is a high-speed protocol developed for infotainment and media oriented communication. Its maximum data rate is 24.8 Mbit/s and it can support up to 64 nodes. However because of the adoption of Automotive Ethernet, the use of most is decreasing.

Below is a table showing the various protocols and their bandwidth;

Protocol	Bandwidth
CAN	125 Kbps - 1 Mbps
LIN	1 Kbps - 20 Kbps
Flexray	10 Mbps
MOST	24 Mbps
Automotive Ethernet	100 Mbps - 10 Gbps

Table 1: Table showing In-vehicle networking protocols and their bandwidths

6 Security Issues and Vulnerabilities

Vehicles have relatively long lifecycles, during which attack patterns and vulnerabilities evolve, exposing them to new and emerging threats. This section outlines the major attack surfaces and vulnerabilities associated with the CAN and Automotive Ethernet AE networks

6.1 Attack Surface of CAN and AE

Adversaries target specific entry points to exploit vulnerabilities in CAN and Automotive Ethernet networks. These attack surfaces can be categorized as follows

6.1.1 Remote/offboard attack

These attacks target external communication interfaces and systems, primarily through the telematics unit. The telematics unit is the domain in the vehicle that consists of wireless communication interfaces such as:

1. **Wi-Fi:** Attackers can exploit unsecured or poorly configured vehicle Wi-Fi networks to gain unauthorized access to in-vehicle systems.
2. **Bluetooth:** Vulnerable to pairing exploits or unauthorized connections, allowing attackers to manipulate connected systems.
3. **Wireless Key Fobs:** Replay or spoofing attacks, such as the TeslaX attack, can enable unauthorized access or control of the vehicle. Additionally, the constant power-on state of certain ECUs, like those in keyless comfort entry systems, can be used as an attack vector, even when the vehicle is parked and locked.
4. **Cellular Networks:** Used for vehicle connectivity and over-the-air updates, these networks can be targeted to infiltrate telematics systems.

6.1.2 Physical/Onboard attacks

These require physical access to the vehicle through the following interfaces:

1. **OBD-II Port:** Used for diagnostics, this port can be exploited to inject malicious CAN messages.
2. **USB Ports:** Unsecured USB interfaces can be used to upload malware.

3. **Electric Vehicle (EV) Charging Ports**
4. **Ethernet Switches:** Attackers can target AE switches to intercept, reroute, or block critical data flows within the network.

6.1.3 Hybrid Attacks

Adversaries often combine remote and physical attack vectors. An attacker might exploit a vulnerability in the telematics unit remotely and then gain deeper access during physical interaction with the vehicle for further post exploitation.

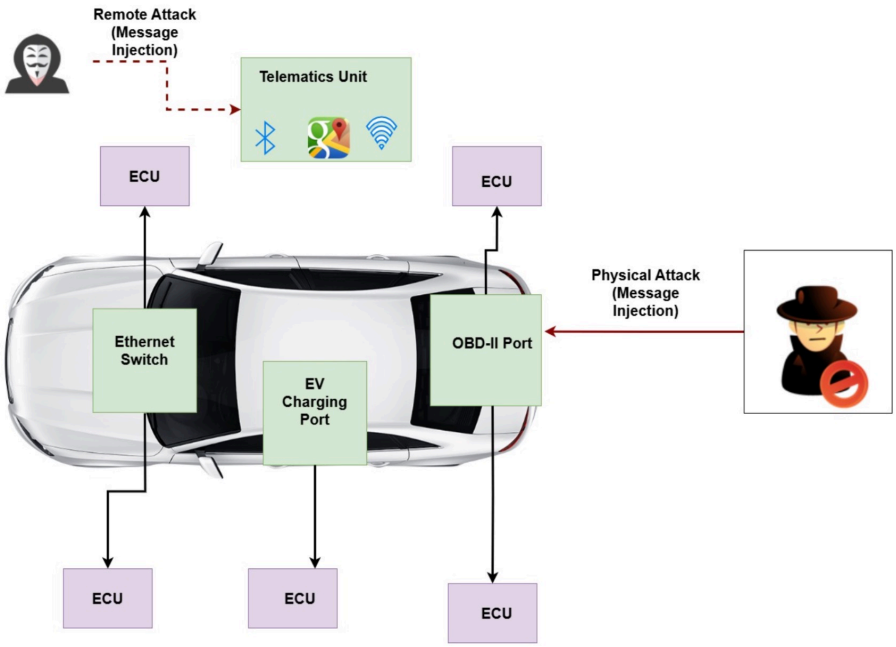

Figure 1: Hybrid Attacks

6.2 Vulnerabilities in CAN

CAN a legacy protocol, was developed without considering modern security threats, making it inherently vulnerable to various attacks. Below are the major vulnerabilities identified in the CAN network:

6.2.1 ID-Based Arbitration

CAN uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) to manage message collisions. Arbitration is based on message IDs where ECUs with lower message ID have higher priority and are allowed to transmit first. Attackers can exploit this mechanism to execute a Denial-of-Service (DoS) attack by injecting high-priority messages that dominate the bus blocking legitimate ECUs to transmit.

6.2.2 Lack of Authenticated Messages

The CAN frame has no field for sender or receiver information to determine a legitimate communicating device. Thus, the authenticity of the message cannot be guaranteed in CAN networks, allowing attackers to inject malicious messages into the network.

6.2.3 Lack of Confidentiality

Since CAN is a broadcast Network, all nodes receive data that is transmitted hence, a malicious ECU has the tendency to eavesdrop and intercept data transmitted on the bus. This is because messages are not encrypted in CAN leading to a lack of confidentiality.

6.3 Common CAN Bus Attacks

Exploiting these vulnerabilities can lead to the execution of the following attacks on the CAN bus:

1. **Denial-of-Service (DoS) attacks:** By exploiting the arbitration mechanism, attackers inject high-priority messages to dominate the bus, preventing legitimate ECUs from communicating. Critical vehicle systems are disrupted, potentially compromising safety.
2. **Fuzzing Attacks:** Attackers send random or malformed CAN messages to test how ECUs respond to unexpected inputs. This can reveal weaknesses in ECU software and hardware, causing crashes or unexpected behavior.
3. **Replay Attacks:** Replay attacks occur when an attacker intercepts legitimate CAN messages and retransmits them at a later time, potentially causing unauthorized actions or disruptions. Since CAN cannot differentiate between original and replayed messages, this can lead to unintended consequences, such as unlocking doors. The wireless key fob functionality is particularly vulnerable to this type of attack, making it a common target for exploitation.
4. **Impersonation or Spoofing attacks:** By pretending to be a legitimate ECU, attackers inject malicious frames into the network. This can manipulate the vehicle system, such as deploying airbags or tampering with engine performance.

6.4 Vulnerabilities in Automotive Ethernet

Automotive ethernet inherits vulnerabilities from traditional IT ethernet. The vulnerabilities are non-exhaustive and only a few are captured in this study. Some of the attack patterns in AE have similar characteristics to the ones in CAN networks, e.g., replay attacks and spoofing, DoS The primary categories of vulnerabilities in Automotive Ethernet Networks include:

6.4.1 Unauthorized Joins

Any device can connect to an unconnected port on the switch. This means that anyone with physical access to the switch can eventually have access to the network and can communicate in several ways such as VLAN hopping where a user may create frames to bypass VLAN segmentation.

6.4.2 Spoofing attacks

- **MAC Spoofing:** Attackers can change their devices MAC address to mimic another device on the network, gaining unauthorized access and potentially disrupting network services.
- **DHCP Spoofing:** Attackers can set up a rogue DHCP server to provide incorrect IP addresses to devices, redirecting traffic to malicious nodes.
- **IP Spoofing:** Attackers can send IP packets from a false (or spoofed) source address, making it appear as though the packets are coming from a trusted source.

6.4.3 Man-in-the-middle attacks

In the Man-in-the-Middle (MitM) attack, the attacker intercepts communication between two ECUs or nodes, eavesdropping or altering the transmitted data without their knowledge. This can lead to the exposure of sensitive information or the injection of malicious data into the communication stream.

6.4.4 MAC Table flooding

Switches maintain a MAC table to map MAC addresses to switch ports. In a MAC table flooding attack, an attacker floods the switch with a large number of frames, each with a different source MAC address. This can overflow the MAC table, causing the switch to broadcast all frames to all ports, effectively turning the switch into a hub and allowing the attacker to sniff all network traffic.

6.4.5 ARP table poisoning

Attackers send fake ARP messages to associate their MAC address with the IP address of a legitimate device. This allows them to intercept, modify, or stop data intended for that device.

7 Use Case Scenarios

In this section, we outline two use cases relevant to our study.

7.1 Tesla X Wireless key fob attack

Brief Description
Researchers in KU leuven previously hacked the keyless entry of the me tesla model s. Although tesla improved the security in the new model, They found additional ways to bypass the tesla model . The same researchers hacked the Tesla Model S keyless entry system and now detail how the security measures implemented in the more recent Tesla Model X can be bypassed. They demonstrate how the battery powered Tesla Model X priced at over $100.000 US can be stolen in a few minutes. The Attack flow is shown below: **Identified issues**
First, the Model X key fobs lack what's known as "code signing" for their firmware updates.

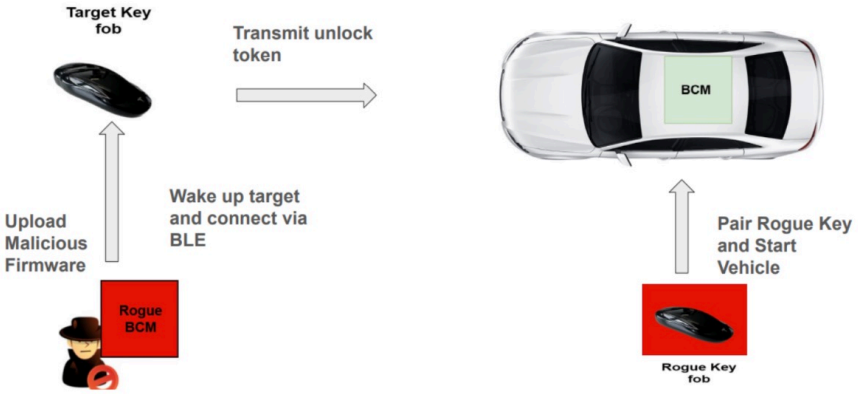

Figure 2: Tesla X Wireless key fob attack

Tesla designed its Model X key fobs to receive over-the-air firmware updates via Bluetooth by wirelessly connecting to the computer inside a Model X.

7.2 2014 Jeep Cherokee Attack

The 2014 Jeep Cherokee attack by researchers Charlie Miller and Chris Valasek highlighted critical vulnerabilities in the CAN bus system and the connected Uconnect infotainment system, exposing how remote access to vehicle systems can lead to severe consequences. **Threat Analysis:**

- **ID-Based Arbitration Exploitation:** Attackers injected high-priority malicious messages, leading to Denial of Service (DoS) and blocking legitimate ECUs from communication.
- **Lack of Authentication:** Allowed unauthorized access to send commands to the CAN bus, leading to unsafe vehicle control (e.g., disabling brakes, manipulating acceleration).
- **Lack of Confidentiality:** Broadcast nature of the CAN bus enabled interception and injection of malicious messages.
- **Remote Entry via Uconnect:** Exploited vulnerabilities in AE to gain access to the CAN network, showcasing a hybrid attack scenario.

8 Security Mitigations and Recommendations

1. **Intrusion Detection Systems (IDS):** IDS play a critical role in monitoring network traffic for abnormal patterns or unauthorized activities. For CAN networks, anomaly-based IDS detect deviations from typical message patterns, such as sudden high-priority messages indicative of Denial-of-Service (DoS) attacks. In AE, signature-based IDS can identify known vulnerabilities, such as MAC spoofing or Man-in-the-Middle (MitM) attacks, ensuring timely detection and response.

2. **Firewalls:** Firewalls act as a barrier between critical in-vehicle networks and external interfaces. For AE, firewalls are deployed at gateways to filter malicious traffic and enforce rules that limit communication to authorized systems. This segmentation reduces the risk of remote exploits spreading across network domains.

3. **Deep Packet Inspection (DPI):** DPI enhances network security by inspecting the content of data packets beyond basic header information. For AE, DPI helps detect malicious payloads, unauthorized data, or malformed packets that could compromise ECUs or vehicle functionality.

4. **MACsec:** Media Access Control Security (MACsec) is an IEEE 802.1AE standard that provides data integrity and encryption for Ethernet networks. In AE, MACsec ensures that communication between switches and devices is both confidential and tamper-proof, protecting against spoofing and MitM attacks.

5. **Security Zones:** Security zoning involves segmenting networks into isolated domains based on their functionality and criticality. For instance, CAN-based safety-critical systems (e.g., braking) can be separated from AE-based infotainment or telematics domains. This minimizes the impact of an attack on one domain from affecting others.

6. **Secure Boot:** Secure Boot ensures that only authorized and verified software can run on vehicle ECUs. By validating digital signatures during the startup process, Secure Boot prevents attackers from deploying malicious firmware, safeguarding both CAN and AE environments.

7. **Port Security:** Port security restricts access to Ethernet switches by allowing only authorized devices to connect. In AE networks, port security can mitigate unauthorized joins or MAC address spoofing, enhancing control over physical access points.

9 Emerging Future Trends For Securing IVNs

9.1 Blockchain Technology

Blockchain offers a decentralized and tamper-proof mechanism for securing in-vehicle communications and data exchanges. By creating immutable logs of network activity, blockchain can help:

- Ensure message integrity by validating data exchanged between ECUs.
- Detect unauthorized changes by maintaining a transparent history of events.
- Facilitate secure over-the-air (OTA) updates through trusted distributed networks. Blockchain's inherent resilience to single points of failure makes it a promising solution for safeguarding critical IVN components like CAN and AE against spoofing, replay, and tampering attacks.

9.2 Zero Trust Architecture (ZTA)

ZTA shifts the security paradigm by assuming that no device or user within a network is inherently trustworthy. In the context of automotive IVNs, ZTA principles can be applied to:

- Authenticate and authorize every interaction within the network, regardless of its origin.
- Limit access to critical systems through micro-segmentation and strict access controls.
- Continuously monitor and assess devices for anomalies, ensuring real-time threat detection. By adopting ZTA, automakers can reduce the risk of lateral movement in attacks and enhance the overall security of both legacy (CAN) and modern (AE) networks.

These technologies hold significant potential to transform the security landscape of in-vehicle networks, addressing evolving threats and ensuring robust protection for next-generation vehicles.

10 Discussion and Analysis

10.1 Research Questions Answers

- **RQ1: What is the current vehicle EE architecture and what is the future trend?**
  - Currently, most automotive OEMs use a domain-based architecture where Electronic Control Units (ECUs) with similar functionalities are grouped into functional domains. Each domain has a domain control unit that acts as a gateway for communication between different domains. This interdomain communication happens through the gateway.
  - With the shift towards Vehicle-to-Everything (V2X) and Software-Defined Vehicles (SDV), the trend is gradually moving towards zonal EE architecture. This is a centralized architecture compared to the distributed nature of the domain-based architecture. It consists of a central compute unit and groups ECUs into zones. This High-Performance Compute Unit (HPCU) facilitates over-the-air updates and cloud communication, effectively supporting V2X applications.
- **RQ2: How are these IVNs (CAN and AE) enablers for the Vehicle EE architecture?**
  - For domain-based architecture, CAN is the main backbone communication protocol; however, due to high bandwidth requirements, in the Zonal EE Architecture, Automotive Ethernet will be used in conjunction with CAN bus for backbone communication. CAN facilitates deterministic, low-latency communication for safety-critical systems and Automotive Ethernet provides the

scalability and bandwidth required for data-intensive applications like ADAS, teleoperations, and infotainment.

- **RQ3: What are the key attack surfaces and vulnerabilities of CAN and AE?** The attack surface can be categorized into two main groups:
  - **Remote/offboard attack:** These attacks target external communication interfaces and systems, primarily through the telematics unit. The telematics unit is the domain in the vehicle that consists of wireless communication interfaces such as:
    1. **Wi-Fi:** Attackers can exploit unsecured or poorly configured vehicle Wi-Fi networks to gain access to in-vehicle systems.
    2. **Bluetooth:** Vulnerable to pairing exploits or unauthorized connections, allowing attackers to manipulate connected systems.
    3. **Wireless Key Fobs:** Susceptible to relay or spoofing attacks, enabling unauthorized access to the vehicle or its systems. (TeslaX attack)
    4. **Cellular Networks:** Used for vehicle connectivity and over-the-air updates, these networks can be targeted to infiltrate telematics systems.
  - **Physical/Onboard attacks:** These require physical access to the vehicle through the following interfaces:
    1. **OBD-II Port:** Used for diagnostics, this port can be exploited to inject malicious CAN messages.
    2. **USB Ports:** Unsecured USB interfaces can be used to upload malware.
    3. **Onboard Wi-Fi:** Internal wireless networks can act as a gateway for attackers.
    4. **Electric Vehicle (EV) Charging Ports**
    5. **Ethernet Switches**
  - Combination of both remote and onboard attacks

- **RQ4: What are the major security issues with CAN and Automotive Ethernet?**
  - **CAN Vulnerabilities**
    1. Lack of authentication and due to ID-Based Arbitration Mechanisms
    2. Lack of confidentiality since it is a bus (Broadcast Network), all nodes receive data.
    3. Broadcast nature exposes all nodes to malicious messages.
    4. Vulnerable to replay and spoofing attacks.
  - **Automotive Ethernet Vulnerabilities**
    1. Adapts traditional Ethernet vulnerabilities e.g., spoofing, ARP poisoning, VLAN hopping, MAC flooding.

- **RQ5: What trade-offs are associated with implementing security measures?**

  - Adding cryptographic measures (e.g., encryption) can increase latency and resource consumption in real-time systems like CAN.
  - Implementing IDS or firewalls may require additional hardware, increasing costs and complexity.

- **RQ6: How does fuzzing reveal vulnerabilities in CAN and AE?**
  - **CAN Fuzzing:** Sends random CAN IDs or malformed packets to identify weaknesses in ECUs. This often reveals how systems handle invalid or unexpected inputs, leading to crashes or misbehavior.
  - **AE Fuzzing:** Targets Ethernet stacks by injecting malformed frames or protocol-specific data (e.g., ARP requests). This helps uncover vulnerabilities like buffer overflows or improper error handling.
- **RQ7: What security measures are currently in use for CAN and AE?**

11 Conclusion

– to be added –