**METHODOLOGIES**

**The CAN Protocol Vulnerability Assessment**

The Controller Area Network (CAN) protocol, while widely used for its efficiency and reliability, presents significant security challenges. The analysis of vulnerabilities of the CAN protocol are across three key security aspects: confidentiality, integrity, and availability. The analysis will examine how the lack of inherent cryptographic mechanisms, message authentication, and robust error management contributes to these vulnerabilities.

1. **Confidentiality Concerns:** The CAN protocol lacks cryptographic methods to ensure confidentiality, allowing intruders to access sensitive user data and invade privacy [31]. Each message transmitted on the CAN bus is sent to every node, making it easy for a malicious node to listen and read message content, consequently leading to a lack of confidentiality [32]. Furthermore, the absence of suitable security support within the CAN protocol renders it vulnerable to attacks such as CAN bus Denial of Service (DoS) and bus injection attacks, which pose significant threats to confidentiality [33]. The broadcast nature of CAN messages combined with the lack of encryption further worsens the vulnerability, making the protocol susceptible to traffic analysis. This vulnerability enables attackers to passively monitor and collect detailed metrics about CAN traffic, thereby compromising confidentiality [34].
2. **Integrity Concerns:** The CAN protocol's lack of built-in authentication mechanisms creates significant integrity concerns. This vulnerability opens the door to message injection and tampering attacks by unauthorized actors. Furthermore, the absence of secure key management allows these malicious entities to manipulate or forge messages entirely. Replay attacks pose an additional threat, where intercepted valid messages can be retransmitted, leading to unauthorized actions or data corruption. Compounding these issues, the lack of message source authentication makes the CAN protocol susceptible to impersonation attacks. In such scenarios, attackers can masquerade as legitimate nodes and inject malicious messages. Finally, the CAN protocol's limited error management capabilities can also impact integrity. Errors caused by external disturbances or hardware faults can lead to the transmission of erroneous messages, further compromising data integrity [35], [36].
3. **Availability Concerns:** The CAN protocol's reliance on a priority-based messaging system has availability concerns. When a high-priority message is transmitted, it can effectively block lower-priority nodes from accessing the network, hindering their ability to send critical messages. This directly violates the principle of availability. Furthermore, the lack of comprehensive integrity checks within the CAN protocol exacerbates availability issues. The protocol's current Cyclic Redundancy Check (CRC) is insufficient to prevent malicious data injection. When attackers exploit this weakness, the accuracy and validity of data are compromised, potentially leading to disruptions in system operation and reduced availability [31].

Attacks such as CAN bus Denial of Service (DoS) can disrupt the availability of the CAN bus by overwhelming it with high priority messages, preventing the transmission of messages from other Electronic Control Units (ECUs).

Finally, The absence of fault-tolerant mechanisms in the CAN protocol can lead to availability issues in safety-critical applications. System failures caused by external factors or hardware malfunctions can disrupt communication and lead to potentially severe consequences [33].

**Automotive Attack Surface Expansion**

The expanding complexity of modern vehicles opens the door to a wider range of security threats. There are two primary attack categories: physical and remote. Physical attacks focus on exploiting the Controller Area Network (CAN bus), the vehicle's internal network, often through the On-Board Diagnostic (OBD) port. The analysis will explore how attackers can manipulate brakes, engines, and even disrupt the network entirely. Remote attacks target the vehicle's wireless interfaces like Bluetooth and cellular networks. This section will investigate how attackers can exploit these interfaces for unauthorized access, including compromising in-vehicle systems and manipulating software updates [31].

1. **Physical Access Attacks**  
     
   Physical access attacks on automobile systems need direct communication with the network systems of the car, frequently by installing unauthorized devices within the car's network architecture or by using exposed ports. Among these assaults are:  
     
   **On-Board Diagnostics (OBD) Ports Attack:** The OBD port is a main target for attackers since it provides a direct path to the vehicle's network. Attackers have the ability to manipulate a number of vehicle modules, including crucial ones like engine and brake control, by taking advantage of the OBD port. They have the ability to alter engine parameters, release brakes, stop brake activation, manipulate instrument clusters, and even turn off the engine while the car is moving.  
     
   **Selective Denial-of-Service (DoS) Attacks:** These attacks attempt to interrupt the network without transmitting whole messages. They can be executed by overwriting specific bits of transmitted data, causing transmission problems and abusing the CAN standard's vulnerabilities. Research in this arena has been essential in exploiting these vulnerabilities, which led to government alerts and raised awareness of the susceptibility of cars to such attacks.  
     
   **Indirect Physical Access Attacks**: In contrast to direct attacks, these do not require access to the vehicle's network. For example, hacking a car service's IT system can provide them indirect access to the CAN network. Furthermore, attacking via multimedia devices like as CDs, USBs, or MP3 players, while not directly breaching the CAN, can cause the driver to display warnings on the screen or play alarm signals.   
     
   The interpretation of these attacks underscores the critical need for robust cybersecurity measures within automotive systems to safeguard against unauthorized access and manipulation of vehicle networks [37].
2. **Remote Access Attacks**  
     
   The integration of numerous wireless interfaces into modern vehicle systems, such as anti-theft measures, Tire Pressure Monitoring Systems (TPMS), Bluetooth, and telematics units, has increased the vulnerability to remote access cyber-attacks. The vulnerabilities highlighted are:   
     
   **Wireless Interface Exploitation**: These interfaces, which connect to the Controller Area Network (CAN) via gateway Electronic Control Units (ECUs), present substantial security threats. Hackers have exploited such weaknesses to gain unauthorized access and remotely modify numerous vehicle functions, including door unlocking.

**OTA Update Vulnerabilities:** The ease and cost-effectiveness of Over-the-Air (OTA) software upgrades adds another layer of susceptibility. Malicious actors may intercept these updates, corrupting the vehicle's communication network and resulting in ransomware attacks or other cyber-sabotage activities.  
  
**V2V and V2I Communication Risks**: The rise of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, which are critical for vehicular ad hoc networks (VANETs), has revealed new vulnerabilities. These systems, which are intended to optimize traffic and prevent collisions, could be endangered by faked communications, causing in-vehicle communication networks to malfunction.

This thorough investigation emphasizes the increasing risk posed by the incorporation of wireless connections into current automobiles, identifying potential channels for illegal access and control by malevolent actors. The referenced journal paper provides an in-depth assessment of these vulnerabilities as well as ideas for strengthening cybersecurity in automobile systems using cutting-edge approaches [38].

**In-Vehicle Network Classification by Attack Entry Point**

In-vehicle network system attacks can be categorized based on their entry points: sensor-initiated, infotainment-initiated, telematics-initiated, and direct interface-initiated [33].

* Sensor-initiated attacks exploit vulnerabilities in vehicle sensors, manipulating data to cause malfunctions or false readings.
* Infotainment-initiated attacks target the infotainment system, aiming for unauthorized access and control of its functionalities.
* Telematics-initiated attacks focus on exploiting vulnerabilities in the telematics system (communication and navigation) to gain unauthorized access or manipulate data.
* Direct interface-initiated attacks exploit vulnerabilities in communication interfaces (e.g., OBD-II port) to access internal networks and compromise Electronic Control Units (ECUs) [35].

A diagram of a car

Description automatically generated

Figure: Four attack vectors for data manipulation in connected cars: Telematics, Infotainment, Direct Interfaces, Sensors. [3]

Attackers leverage various methods to gain access, including wireless and physical access, exploiting software bugs, remote keys, and other vulnerabilities in ECUs [3].

These vulnerabilities in communication protocols like CAN bus and Automotive Ethernet (AE) create openings for a range of attacks. The CAN bus is susceptible to bus-off, denial-of-service (DoS), masquerading, injection, eavesdropping, and replay attacks [5]. Similarly, attackers can launch traffic integrity, confidentiality, access, and DoS attacks against Automotive Ethernet [3].

**References:**

[1] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, “Evaluation of CAN Bus Security Challenges,” *Sensors*, vol. 20, no. 8, Art. no. 8, Jan. 2020, doi: 10.3390/s20082364.

[2] F. Fakhfakh, M. Tounsi, and M. Mosbah, “Cybersecurity attacks on CAN bus based vehicles: a review and open challenges,” *Libr. Hi Tech*, vol. 40, no. 5, pp. 1179–1203, Jan. 2021, doi: 10.1108/LHT-01-2021-0013.

[3] E. Aliwa, O. Rana, C. Perera, and P. Burnap, “Cyberattacks and Countermeasures for In-Vehicle Networks,” *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–37, Jan. 2022, doi: 10.1145/3431233.

[4] V. Tanksale, “Controller Area Network Security Requirements,” in *2020 International Conference on Computational Science and Computational Intelligence (CSCI)*, Dec. 2020, pp. 157–162. doi: 10.1109/CSCI51800.2020.00034.

[5] R. S. Rathore, C. Hewage, O. Kaiwartya, and J. Lloret, “In-Vehicle Communication Cyber Security: Challenges and Solutions,” *Sensors*, vol. 22, no. 17, Art. no. 17, Jan. 2022, doi: 10.3390/s22176679.

[6] S. Hounsinou, M. Stidd, U. Ezeobi, H. Olufowobi, M. Nasri, and G. Bloom, “Vulnerability of Controller Area Network to Schedule-Based Attacks,” in *2021 IEEE Real-Time Systems Symposium (RTSS)*, Dortmund, DE: IEEE, Dec. 2021, pp. 495–507. doi: 10.1109/RTSS52674.2021.00051.

[7] V. Renganathan, E. Yurtsever, Q. Ahmed, and A. Yener, “Valet attack on privacy: a cybersecurity threat in automotive Bluetooth infotainment systems,” *Cybersecurity*, vol. 5, no. 1, p. 30, Oct. 2022, doi: 10.1186/s42400-022-00132-x.

[8] S. H. Oh, J. Kim, J. H. Nah, and J. Park, “Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity,” *Electronics*, vol. 13, no. 3, Art. no. 3, Jan. 2024, doi: 10.3390/electronics13030555.