**Introduction**

CAN is used by an ECU to send its frames over a bus. Every frame has a distinct 11-bit identification code, called the "arbitration ID" or "CAN ID," that determines its priority and function. The priority resolves transmission conflicts and moves from 0x000 (highest) to 0x7FF (lowest). Data in frames can be up to 8 bytes long. Even though a single ECU is capable of broadcasting multiple CAN IDs, no two ECUs are allowed to send data frames with the same ID. Every ECU on the bus receives a transmitted frame and uses the CAN ID to determine whether to accept and process the message.

The CAN protocol is widely used bus protocol in in-vehicle networks. Communication between different ECUs is possible through wired CAN bus. It can several intrinsic vulnerabilities such as broadcast transmission, no authentication, no encryption, ID-based priority scheme and available interfaces. These vulnerabilities make in-vehicle networks expose to malicious attacks by the adversaries.

**Broadcast Transmission:** CAN frames are broadcasted to all nodes on the CAN bus, allowing every ECU to receive them. However, this also enables malicious nodes to intercept frames easily.

**No Authentication:** CAN frames lack authentication fields, making it difficult for receivers to distinguish between valid and fake frames. Malicious nodes can exploit this by sending fake frames to take control of vehicle components.

**No Encryption:** CAN frames are not encrypted, making it easy for adversaries to analyze historically recorded frames.

**ID-Based Priority Scheme:** The identifier of a CAN frame determines both its target node and its priority. Frames with lower identifiers have higher priority, which can lead to denial of service (DoS) attacks if exploited by malicious nodes.

**Available Interfaces:** Adversaries can access in-vehicle networks through interfaces like the OBD port, CD player, USB port, and telematics systems. They can access the target through these functionalities and implement various attacks such as DoS attack, replay attack, frame sniffing and frame injection. The OBD port is commonly targeted for experimental attacks due to its ability to access the CAN bus and receive messages from other nodes.

**In-Vehicle Network Attacks based on the above vulnerabilities:**

**Frame Sniffing:** Adversaries can observe the traffic on the CAN bus by accessing the in-vehicle network through available interfaces and capture many valid frames and analyze them through which details of CAN frame can be known. By testing CAN frames adversaries can find out many functions of selected ECUs

**Frame Falsifying:** Adversaries can design and send fake frame data to in-vehicle network that mislead corresponding authentic ECUs. They can falsify the fuel level and speedometer reading by falsifying frame data.

**Frame Injection:** Adversariescan usemalicious nodes to inject fake frames onto the CAN bus, exploiting the broadcast characteristic of CAN communication. A laptop connected to the OBD port, a reprogrammed ECU, or a malware-infected telematics system could all be the malicious node.

**Replay Attack:** Adversaries will instruct the malicious nodes to send the valid frames to the CAN bus at particular time. ECUs cannot find whether the source of the frames received are authentic or not as there is no authentication scheme. Adversaries are successful in opening the car door, start the engine, turn on the lights and drive the car by injecting the proper data frame.

**Dos Attack:** Adversaries instruct malicious nodes to send frames with high-priority, which will prevent other nodes from sending messages and disrupting communication.

**Fuzzing Attack:**  By sending messages with randomized CAN IDs and payload values and observing the responses, the attacker executes the attacks and will know about the architecture and behaviour of the vehicle and it’s ECUs.

**Diagnostic Attack**: Adversaries can send a diagnostic message to open a diagnostic session on an ECU. Firmware updates or information queries on the ECU, these are the tasks performed by the attacker once session got initiated. This vulnerability makes use of the ECU's built-in diagnostic mode to make maintenance operations easier. An attacker gains access to the internal functionalities of the ECU through this exploitation, through which attacker will gain unauthorized access or manipulation of the vehicle's systems.

**Attack Mechanism:**

This attack involves injecting 10 packets with CAN IDs greater than 0X700 at random positions in the files. This approach probably intends to flood the ECU with many diagnostic messages, which could disrupt it or allow attackers to hide their malicious activity under the deluge of messages. It's important to consider, that the specific vulnerabilities in the targeted vehicle's systems, the attacker's capabilities, and the countermeasures put in place by the vehicle manufacturer could all affect how effective and detailed this attack method represents.

An attacker uses the diagnostic mode of an ECU to open a session by gaining OBD port access to the CAN bus network of a car. Internal function access is made possible by this, allowing the lock to firmware manipulation and safety system compromise. They can tamper with vital systems like engine control by injecting false diagnostic messages. For detection and mitigation, secure coding techniques and strong intrusion detection are essential. This emphasizes how strict cybersecurity controls are necessary in cars to prevent access and possible safety risks.

**Suspension Attack:** Adversaries cause the ECU to stop emitting its frames which disrupt the normal communication and functioning of the ECUs within the CAN network. This kind of attack can occur in ways such as exploiting vulnerabilities in the ECU’s firmware or sending malicious messages to ECU to cause a malfunction or shutdown.

**Intrusion Detection for different message injection attacks:**

Vehicle security has become more crucial as conventional cars have evolved into computerized systems with network connectivity. To guarantee the security of both drivers and passengers, it is essential to protect cars from attacks. Many research efforts have concentrated on identifying and preventing attacks directed towards automobiles.

To detect anomalies some methods for in-vehicle intrusion detection includes usage of entropy-based anomaly detection techniques, defining attack detection based on protocol and ECU behavior, utilizing a structured approach with multiple sensors, and analyzing message rates. However, due to the limited computing power in vehicles, early methods that required large message datasets for analysis may have resulted in delayed detection times.

A lightweight intrusion detection method has been proposed to address this problem by streamlining detection algorithms for faster responses and lower computing power consumption in vehicles.

**Light Weight IDS:**

1. **Threat model**
2. To identify known attack signatures and unusual events in vehicle networks, a hybrid intrusion detection system has been suggested. Its main objective is to detect message injection attacks by examining anomalies in traffic that are related to the frequency of messages. Attackers can still manipulate electronic devices like ECUs by injecting messages into CAN even though it does not contain source or target information in its messages.
3. In Normal status, ECU-generated messages have consistent frequencies or intervals. Nevertheless, these frequencies or intervals unexpectedly alter during an injection attack. The message rate on the network significantly rises because of ECUs sending messages cyclically while attackers injects messages.
4. The detection method depends on message rate monitoring, but attacks take time to manifest before they are discovered. In order to address this, a more rapid response time while retaining high accuracy is achieved by streamlining the detection process.
5. There are two types of CAN injection attacks: standard message injections that mimic ECU messages and CAN diagnostic message injections. For experimental purposes, these attacks are divided into three categories: Type 1 involves the injection of a single CAN ID message, Type 2 includes the injection of random or pre-ordered messages of multiple CAN IDs, and Type 3 involves massive message injection, like a Denial of Service (DoS) attack. While each type has a distinct function, they are all executed similarly.

Three types of attacks utilizing message injection are analyzed:

**Type 1:** Constantly injecting a particular message to interfere with how the vehicle operates. The process of detection includes finding messages with shorter time intervals.

**Type 2:** Using pre-ordered or random messages containing multiple CAN IDs to cause system malfunction. Finding clusters of messages with shorter time intervals is one aspect of detection.

**Type 3:** Overwhelming communication through a massive message injection. Monitoring the message transmission rate and flagging anomalies, like messages with intervals shorter than 0.2 milliseconds, are key components of detection.

1. **Intrusion Detection**

To identify message injection attacks, the IDS system focuses on examining the time intervals of messages sent over the CAN bus.

This is a summary of the detection process:

1. Whenever a new message shows up on the CAN bus by first verifying the CAN ID, the IDS calculates the time interval from the arrival time of the latest message.
2. The IDS recognizes a new message as injected if its time interval is less than half of the average, which is shorter than usual.
3. If consecutive messages have a time interval of less than 0.2 milliseconds, raises the DoS attack score by 1 per message
4. If the score exceeds a predetermined threshold, the event is classified by IDS as a denial-of-service attack.
5. On normal status, messages are sent every 0.5 milliseconds on average, and they are sent every 0.14 milliseconds on average. In order to lower the false positive ratio in DoS attack detection, a threshold is used because some normal messages have time intervals shorter than 0.2 milliseconds.

A diagram of a computer program

Description automatically generated

Fig.1 Diagram of proposed IDS. After analysis of time interval of each detection module. The one is detecting or malfunction. Another one is detecting DoS attack to disturb CAN communication.

Reference

1. Song, H. M., Kim, H. R., & Kim, H. K. (2016, January). Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In *2016 international conference on information networking (ICOIN)* (pp. 63-68). IEEE.
2. Liu, J., Zhang, S., Sun, W., & Shi, Y. (2017). In-vehicle network attacks and countermeasures: Challenges and future directions. *IEEE Network*, *31*(5), 50-58.
3. Dupont, G., Den Hartog, J., Etalle, S., & Lekidis, A. (2019, November). Evaluation framework for network intrusion detection systems for in-vehicle can. In *2019 IEEE International Conference on Connected Vehicles and Expo (ICCVE)* (pp. 1-6). IEEE.