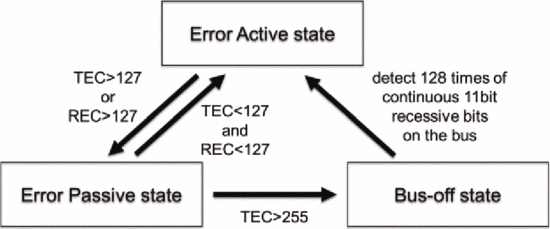
**ECU Impersonation attacks**

Before we delve into the topic of impersonation/spoofing attacks on an ECU, we need first to understand the significance of an ECU in a CAN bus. As described by M. J and K. C(2021), an Electronic Control Unit or ECU is a component in every single vehicle[1]. Every vehicle comes with ECU nodes and each of them is designed to task one specific task, for example, to monitor the seat-belt status, or to check the temperature, humidity, or altitude of the vehicle. A single higher-powered controller computer then takes the data from the ECU nodes and runs an algorithm to verify the messages. On the other hand, in a CAN bus, in case of an error, an ECU sends an error frame to inform other ECUs in the network. Once the error is detected by the controller, it increases the bits of TEC and REC.



In the paper “Spoofing attack using bus-off attacks against a specific ECU of the CAN bus” by K. Iehira, H. Inoue, and K. Ishida(2018), they have described a spoofing attack method that cannot be detected by the controller[3]. The proposed attack forces a legitimate ECU into a bus-off state, where it is unable to transmit or receive any messages, thus preventing the controller from detecting spoofed messages injected by the attacker. This happens due to the attacker causing errors in the messages from the authorized ECU, thus transitioning it into an off-state, and injecting the spoofed messages onto the CAN bus.

Mimicking the cycle and the IDs of legitimate messages, the attacker’s spoofed messages go unnoticed, which in turn compromises the integrity and safety of the vehicle’s network. This can result in false readings from the ECU nodes and result in fatal errors in extreme cases. The impersonation attack in this case is successful as there’s no authentication process and doesn’t have any way to identify the source of the message.

To mitigate these types of attacks, a study by Yang Y et. al.(2020) proposes a deep learning model for detecting spoofing attacks in-vehicle CAN networks, thus utilizing a theoretical framework of the CAN physical layer to authenticate data frame IDs[2]. By using extensive simulated CAN signal data, they apply a recurrent neural network (RNN) with long short-term memory (LSTM) to identify deep features of CAN signals and pinpoint malicious ECU nodes. However, they also note that their work still has a long way to go to be implemented in a real-life scenario, as they would need the model to work in a real-time setting and need data from a diverse dataset of real CAN bus signals.

**The Jeep Cherokee Attack**

The Jeep Cherokee cyberattack by Charlie Miller and Chris Valasek truly bridged the gap between modern automotive technology and cybersecurity. This eye-opening event has revealed that the connectivity we enjoy in vehicles also opens doors to potential cyber intrusions[7].

Following this revelation, there's been a concerted effort within the automotive industry to fortify the digital defenses of vehicles[8]. As for safeguarding tactics, there's a growing focus on implementing multi-layered defense mechanisms. This includes segregating critical vehicle networks, ensuring the integrity and confidentiality of firmware updates, and adopting the principle of least privilege to minimize potential attack surfaces. These measures are non-trivial, given the complex and proprietary nature of automotive systems, which vary significantly across different manufacturers and models[9].

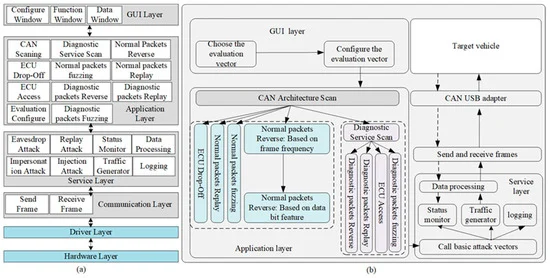
The computational prowess needed to mount such an attack is considerable but within reach for skilled hackers, given the advancements in technology[9]. More challenging, however, is the intricate knowledge required to navigate the proprietary systems of various vehicles, which adds a layer of complexity to the execution of widespread attacks.

This attack has started a broader awareness and action within the automotive sector, driving home the point that vehicle safety now transcends the physical into the digital realm. The combined efforts towards establishing industry-wide cybersecurity standards exemplify the proactive steps being taken to safeguard modern vehicles against cyber threats[8].

**Replay Attacks**

Replay attacks represent a significant security threat to the CAN in vehicles. In such attacks, attackers capture valid network communication and replay it to induce unauthorized actions or responses from the network. This type of attack exploits the CAN's lack of built-in security features like authentication and encryption, which were originally omitted to keep the network lightweight and efficient[6]. The CAN was designed in a time when in-vehicle networks were not exposed to external connections, making security less of a concern. However, with the increasing connectivity of vehicles, including the Internet of Things (IoT), vehicle-to-x communication, and over-the-air updates, the potential for cybersecurity threats, including replay attacks, has significantly increased​​.

One practical approach to evaluating and mitigating the risk of replay attacks on CAN is the use of a security evaluation tool like CANsec. This tool can monitor changes in vehicular status, log evaluation activities, and replay captured CAN frames to test the vulnerability of the network to replay attacks. Experiments conducted using CANsec on a vehicle revealed that the replay attack was indeed effective against the vehicle's instrument panel, demonstrating the capability

Figure 2: CANsec Architecture[6]

of such attacks to manipulate vehicle functionalities like engine speed, turn signals, door status, and wipers. The success of these attacks highlights the inherent security vulnerabilities of the CAN bus broadcasting mechanism.

To mitigate the vulnerabilities exposed by replay attacks, a secure boot scheme has been proposed as a mitigation strategy. This scheme utilizes cryptographic data integrity algorithms to ensure that only authentic and untampered software can run on the vehicle's ECUs. The presence of malicious code in one or more ECUs is a common root cause of CAN bus attacks, and secure boot schemes can effectively prevent the execution of such codes. Testing and comparison of different data security algorithms implemented on a hardware security module (HSM) demonstrated that certain schemes, such as the secure boot with the cipher-based message authentication code (CMAC) and the secure boot with the elliptic curve digital signature algorithm (ECDSA), offer a favorable balance between security level and performance. A novel variation of the ECDSA algorithm based on the CMAC algorithm also showed a 19% performance improvement over the standard ECDSA-based secure boot scheme[6].

**Malicious Diagnostic Applications**

Another prominent way of attacks these days is gaining control of the vehicle by attacking the CAN bus through malicious apps. The apps are specifically designed for infiltrating the vehicle’s network, exploiting the vulnerabilities, and allow the hackers to gain control of the CAN bus to send unauthorized signals. Recently one of the most infamous examples was the Jeep Cherokee attack where the researchers took control of the vehicle via cellular network[7]. Another notable mention involves Tesla, where the security experts identified and exploited vulnerabilities to remotely execute unauthorized malicious attacks, showcasing the critical need for security measures in modern-day vehicles[10].

Simple tasks like sending false signals can be done pretty easily and need minimal resources like a smartphone or a laptop with an internet connection. Incidents like these remind vehicle owners to be more vigilant about the apps they install on their devices and ensure they come from reputable sources and are kept up-to-date with the latest security practices.

References:

1. M. J and K. C, "Smart vehicle monitoring for detecting anomalies on CAN bus," 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 2021, pp. 1-6, doi: 10.1109/CONECCT52877.2021.9622628
2. Yang Y, Duan Z, Tehranipoor M. Identify a Spoofing Attack on an In-Vehicle CAN Bus Based on the Deep Features of an ECU Fingerprint Signal. Smart Cities. 2020; 3(1):17-30. <https://doi.org/10.3390/smartcities3010002>
3. K. Iehira, H. Inoue and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2018, pp. 1-4, doi: 10.1109/CCNC.2018.8319180.
4. Adly, S., Moro, A., Hammad, S., & Maged, S. A. (2023). Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles. Applied Sciences, 13(16), 9374. https://doi.org/10.3390/app13169374
5. Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 7, 82721–82743. https://doi.org/10.1109/ACCESS.2019.2924045
6. Zhang H, Meng X, Zhang X, Liu Z. CANsec: A Practical in-Vehicle Controller Area Network Security Evaluation Tool. Sensors. 2020; 20(17):4900. <https://doi.org/10.3390/s20174900>
7. Brookings. (2015, August 5). Jeep Cherokee hack offers important lessons on the “Security of Things”. Retrieved from https://www.brookings.edu
8. Autoblog. (2019, September 21). How a hacked Jeep Cherokee led to increased security from cyber carjackers. Retrieved from https://www.autoblog.com
9. Carnegie Mellon University - Software Engineering Institute. (n.d.). Vehicle Cybersecurity: The Jeep Hack and Beyond. Retrieved from https://insights.sei.cmu.edu
10. Zhou, K., & Staggs, J. (2018). "A Survey of Remote Automotive Attack Surfaces." IEEE Security & Privacy, 16(3), 16-28. While not focused solely on Tesla, this paper reviews various remote automotive attack surfaces, including those relevant to the Tesla incidents discussed by Keen Security Lab.