Impersonation attack with Controller Area Network (CAN)

Impersonation attacks are a significant security thread in automotive systems caused by lack of message authentication in CAN protocol. These masquerading attacks as legitimate nodes in Electronic Control Units (ECU) risking safety, privacy and functions of automobile by vehicle operation manipulation.

Understanding Impersonation Attacks

The CAN protocol in-vehicle communication systems, enabling ECUs to exchange messages for various vehicle functions, including safety-critical systems like braking and steering. Its design, prioritizing efficiency and simplicity, omits message authentication, encryption, and integrity verification, allowing attackers to inject, modify, or replay messages without detection.

Mechanism of Impersonation Attacks

Physical access through ports like OBD-II or remotely exploiting vulnerabilities in connected services like infotainment systems is gained. The attacker can monitor and analyze CAN traffic to identify message patterns and functionalities controlled by ECU. And then crafting and sending forged messages, exploiting the lack of authentication to command unauthorized actions or overtake legitimate communication.

Implication

Operational Interference: Unauthorized commands can disrupt vehicle functionality, like altering dashboard displays to grave dangers like disabling brakes.

Safety Risks: Direct control over critical functions could result in catastrophic scenarios, endangering lives.

Privacy Breaches: Accessing telematics data could compromise user privacy, revealing location history and personal data.

Countermeasures: Secure CAN protocols

Secure CAN standard

1.CAN with Flexible Data-Rate (CAN-FD): CAN-FD extends the payload size and increases the possibility for more sophisticated security, including encryption and authentication and more in extended space in payload.

2. Controller Area Network Security (CANsec): The concept of CANsec introduces security layers on top of CAN, proposing message authentication and encryption using Hash-based Messages Authentication (HMAC) or symmetric key cryptography to validate the integrity and origin of messages.

3. Local Interconnect Network (LIN) and FlexRay : While not direct evolutions of CAN, these networks offer alternative communication protocols with potential for enhanced security features. They support more complex communication patterns and, in the case of FlexRay, provide built-in support for encryption and error detection, which could mitigate some impersonation threats when used for critical communications.

Implementation Considerations

Adding security layers to CAN network affect real-time performance, a critical consideration in automotive environments. Ensuring that security enhancements are compatible with existing infrastructure is crucial. This could mean incremental updates to ECUs or employing gateways that provide security functions without altering the entire network architecture. Widespread adoption of secure protocols requires industry-wide standardization. Efforts by consortia like AUTOSAR, which defines standardized software architecture for automotive systems, are vital in promoting and implementing secure communication protocols.

Conclusion

Impersonation attacks exploit fundamental weaknesses in the CAN protocol, posing significant risks to automotive safety and privacy. Countermeasures, specifically the evolution towards Secure CAN protocols, mitigate these risks. Implementing such measures requires careful consideration of performance impacts, compatibility, and standardization. As vehicles become increasingly connected and autonomous, the urgency for robust in-vehicle network security only escalates. Embracing Secure CAN protocols is a step towards safeguarding the future of automotive transport against the evolving landscape of cybersecurity threats.