Report on CAN Injection Attacks in Vehicle Theft

Jordan Theoret

Author Note

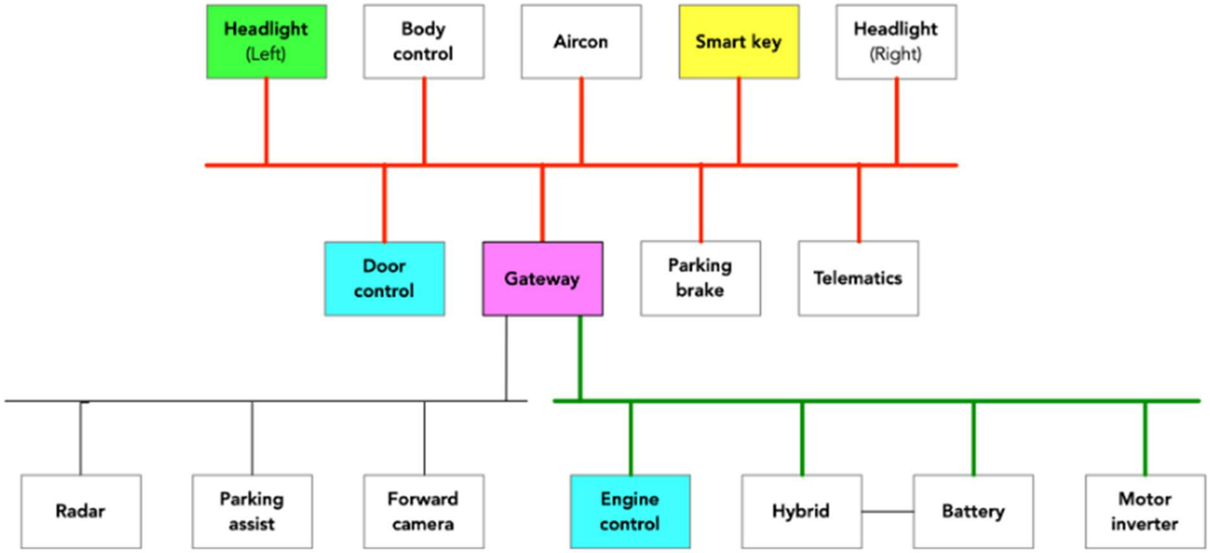
This Information is for educational Purposes only.

Abstract

This comprehensive report examines the sophisticated technique of Controller Area Network (CAN) injection attacks, a prevalent method in modern vehicle theft. It delves into the detailed tactics, techniques, and procedures (TTPs) employed in these attacks, the types of equipment used, their acquisition and disguise, and the countermeasures that vehicle owners can implement.

I. Introduction

The advent of advanced electronic systems in modern vehicles, particularly the CAN bus system, has introduced new vulnerabilities exploitable by sophisticated thieves. The CAN bus system is a network of microcontrollers and devices within a vehicle that communicate with each other to control various functions, including security and engine management. However, this system can be compromised through CAN injection attacks, where unauthorized commands are introduced to manipulate vehicle functions (The Register, 2023).



Simplified Diagram of RAV4 CAN bus. There are three CAN buses shown:

- *A control CAN bus (which has ECUs for headlights, door control, telematics, aircon, etc.)*
- *A powertrain CAN bus (which has ECUs for engine control, the hybrid battery and motor control, etc.)*
- *An autonomy CAN bus (which has ECUs for radar, forward looking camera, and self-parking)*

II. Theft TTPs

A. Target Identification

Thieves typically target high-value vehicles or those known for specific vulnerabilities in their CAN bus systems. The selection is often based on the ease of access to the CAN bus through external points and the value of the vehicle (The Register, 2023).

B. Equipment Preparation

The primary tools for a CAN injection attack include a laptop with specialized software for hacking into the CAN bus, a CAN bus interface device such as an OBD-II scanner, and in some cases, signal interception or amplification tools. These tools are usually sourced from online marketplaces, the dark web, or through criminal networks (Autoblog, 2023).

C. Physical Access

Access to the CAN bus is gained through external points like headlights or taillights. Modern vehicles have increasingly integrated these components into the CAN network, making them accessible points for initiating a CAN injection attack (The Register, 2023).

D. CAN Bus Interaction

Once connected to the CAN bus, the attacker sends specific commands to disarm the vehicle's security systems, unlock the doors, or even start the engine. This process requires an understanding of the specific CAN bus protocols and messaging formats used by the vehicle (The Register, 2023).

III. Equipment Acquisition and Disguise

While traditional tools like OBD-II scanners are common, attackers have become more ingenious in disguising their equipment. A notable instance involved a device built into a JBL Bluetooth speaker, where the play button was configured to trigger a CAN injection attack (Autoblog, 2023). Other devices can be concealed in everyday objects, such as phone chargers or electronic car accessories, to avoid detection.

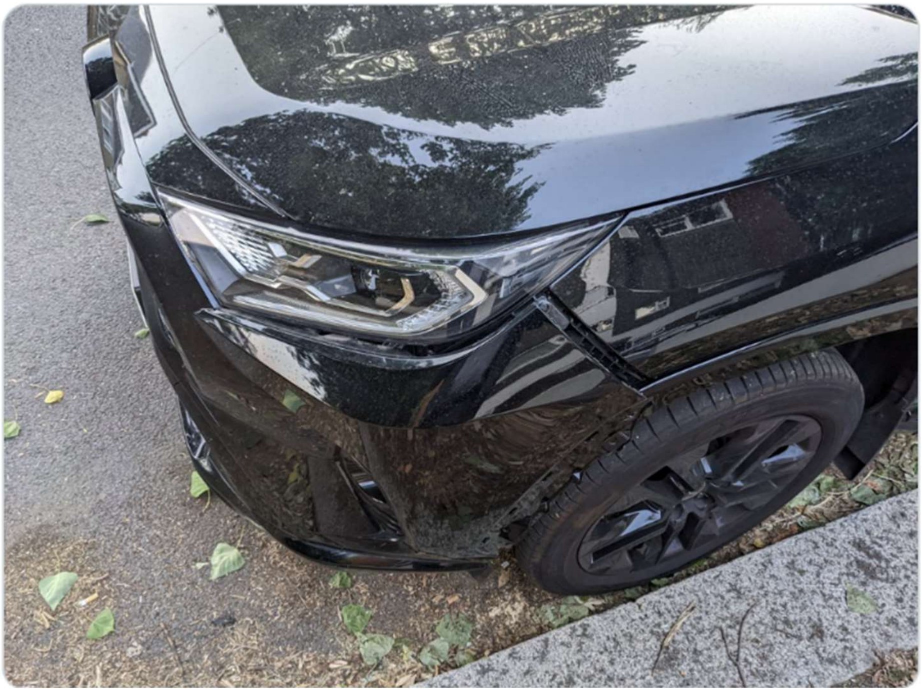
IV. Countermeasures

A. Technological and Practical Countermeasures

To combat CAN injection attacks, vehicle owners are advised to implement both technological and practical countermeasures. These include regularly updating vehicle software, installing advanced aftermarket security systems, and using physical barriers like steering wheel locks. Strategic parking in well-lit, monitored areas can also deter thieves. Additionally, VOXX Electronics recommends parking in areas that restrict easy access to a vehicle's headlights as a simple yet effective measure against these attacks (Autoblog, 2023).

B. Awareness and Vigilance

Staying informed about the latest vehicle security threats and being vigilant about unusual activities around one's vehicle are essential in preventing theft.



Example of Vehicle damaged required for CAN access.

V. Conclusion

The sophistication of CAN injection attacks necessitates a multifaceted approach to vehicle security. Manufacturers and vehicle owners must continuously adapt to the evolving landscape of automotive security to protect against these advanced theft methods.

References

- The Register. (2023). How thieves steal cars using vehicle CAN bus. Retrieved from https://www.theregister.com
- Autoblog. (2023). Thieves are now stealing cars via a headlight 'CAN injection'. Retrieved from https://www.autoblog.com
- CANIS Automotive Labs CTO Blog https://kentindell.github.io/2023/04/03/can-injection/
- A Comprehensive comments section On CAN Injection Attacks. Comments include details on CAN bus wiring harnesses and the kind of Data that is relayed on the Controller Area Network. https://www.schneier.com/blog/archives/2023/04/car-thieves-hacking-the-can-bus.html