PhDIIn Day 2018

New Insights on Automotive Cybersecurity: Vulnerabilities, Solutions and Challenges

PhD Student: Francesco Pascale (XXXII Ciclo)
DIIn, University of Salerno

Introduzione

Grazie alle moderne tecnologie, sempre più autoveicoli sono connessi alla rete Internet (Fig. 1). In generale, i moderni veicoli possono essere considerati come degli oggetti dell'Internet of Things (IoT) [1]. Esistono molti sistemi che permettono l'interconnessione in ambito automotive, come ad esempio gli On Board Units (OBU), le Road Side Unit (RSU), i Vehicular Ad Hoc Networks (VANET), i sistemi di infotainment, etc.. [2]. In questo scenario, il rapido incremento di autoveicoli connessi ha ampliato le possibilità d'attacco. L'obiettivo di questo lavoro di ricerca è quello di identificare i principali rischi connessi alla sicurezza informatica degli autoveicoli e fornire alcune possibili soluzioni [3].

Figura 1. Esempio di veicolo connesso

Modello di minaccia e Analisi dei rischi

Prima di tutto, dobbiamo capire quali sono le vulnerabilità connesse alla sicurezza informatica nel settore automobilistico. Un modo per procedere con questa analisi è attraverso l'uso del Threat Modeling [4]: questo modello analizza l'architettura del bersaglio attaccato, identifica quali componenti sono coinvolte e come queste comunicano tra loro e con il mondo esterno. Applicando questo approccio al settore automobilistico, è possibile dividere il modello di minaccia in 3 livelli (Fig. 2).

Esistono diverse possibilità di attacco, che differiscono in base al punto di ingresso utilizzato:

- Esterno a lungo raggio (ad es., Accesso senza chiave fisica o tramite telecomandi wireless)
- Esterno a corto raggio (ad es. Bluetooth, RFID, ecc.)
- Interno fisico (ad es., ODBII)
- Connessione interna (ad es., Unità di controllo elettronico (ECU))

Le possibili contromisure a tali attacchi posso essere le seguenti:

- Protocolli di autenticazione
- Uso dell'architettura TrustZone
- Tecniche di crittografia
- Tecniche di rilevamento delle intrusioni (IDS)

In generale, tutti i possibili attacchi, sia quelli originati dall'esterno del veicolo che quelli provenienti dall'interno, sono pensati per controllare il CANBus, attraverso il quale possono essere inviati messaggi potenzialmente pericolosi [5] [6]. Obiettivo della ricerca è quello di introdurre un livello di protezione che agisca direttamente sul CANBus.

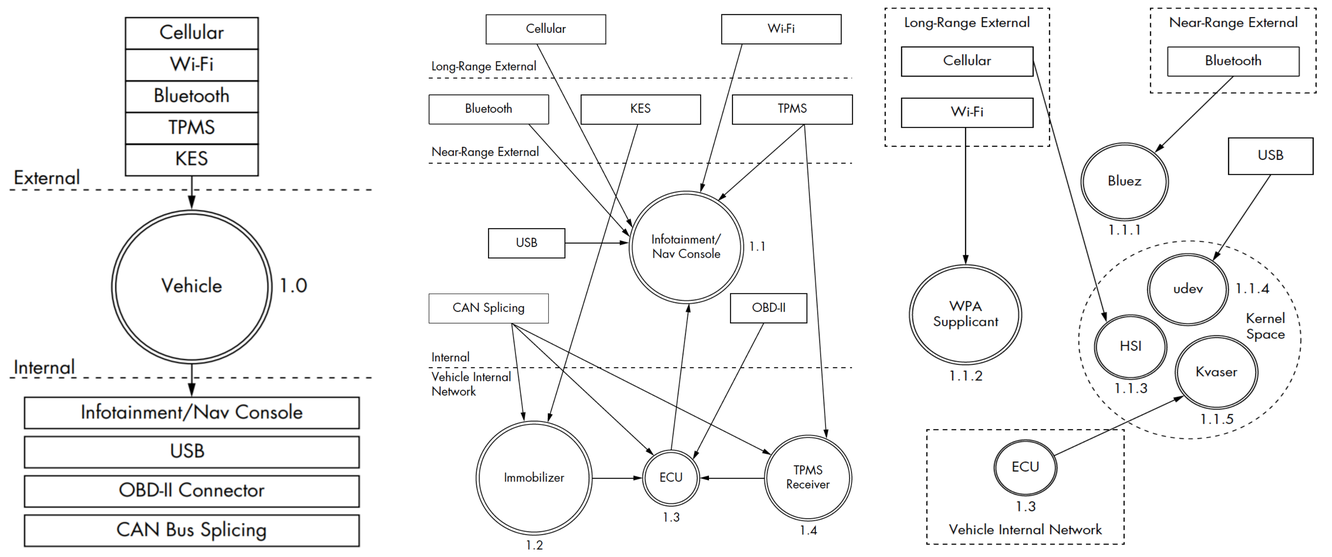

Figura 2. Input, Mappa degli input e dei collegamenti del veicolo, Infotainment Console [4]

Soluzione proposta

Si vuole realizzare un approccio di difesa che passi dalla criptazione dei messaggi presenti all'interno del CANBus. Obiettivo è quello di utilizzare un approcci che non degradino le prestazioni del protocollo. La soluzione proposta è basata sulla tecnica ISR (Instruction Set Randomization): una tecnica che consente di codificare un messaggio in modo sicuro. Attraverso una chiave di codifica, generata per ogni messaggio da inviare su CANBus, viene creato un set unico di istruzioni randomizzate (Fig. 3):

- Queste nuove istruzioni sostituiranno i messaggi originali. Parallelamente, verrà creato un ambiente di esecuzione unico, ignoto all'utente malintenzionato che non potrà intervenire a livello macchina senza conoscere la chiave.

Per la codifica e la decodifica dei messaggi, verranno utilizzati due approcci alternativi:

- XOR bit a bit tra messaggio e chiave.
- Trasposizione casuale di bit (basata su chiavi).

Caso di studio preliminare

Per testare la metodologia proposta, si è costruito un prototipo software attraverso Automotive Grade Linux [7]: un ambiente software basato su Linux che consente di simulare tutte le caratteristiche e le azioni di un veicolo connesso. Il prototipo ottenuto è in grado di simulare i diversi sottosistemi che scambiano messaggi sul CANBus. L'obiettivo della fase sperimentale è valutare la metodologia proposta rispetto a possibili manomissioni o attacchi in termini di efficacia e di efficienza (Fig. 4).

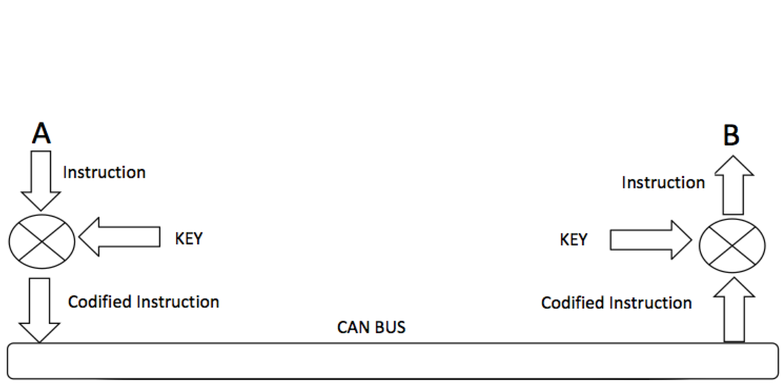

Figura 3. Istruction Set Randomization

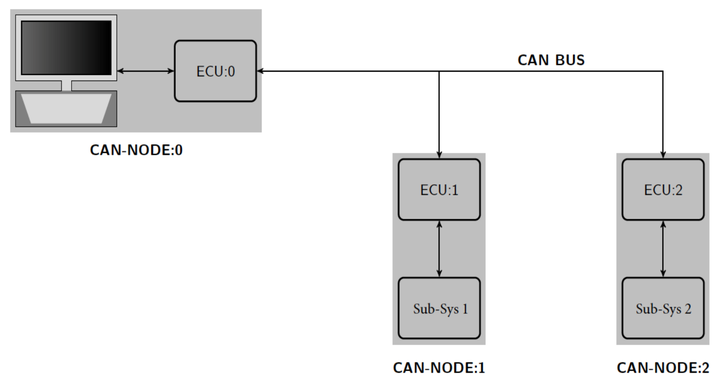

Figura 4. Lo Scenario Proposto

Sviluppi futuri

A valle della sperimentazione del prototipo si intende introdurre l'approccio sviluppato in contesti reali al fine di verificarne l'efficacia. Ulteriore obiettivo sarà quello di introdurre algoritmi di cifratura più complessi in grado di rendere ancora più robusto l'approccio proposto

Contatti

<Francesco Pascale>
<University of Salerno, DIIn>
Email: fpascale@unisa.it
Website: www.knoman.unisa.it
Telefono: +39089964031

Riferimenti

[1] Ben Mccluskey, "Connected cars – the security challenge [Connected Cars Cyber Security]", Engineering & Technology, Volume: 12, Issue: 2, March 2017;
[2] Dietmar P. F. Möller, E. Haas, K. B. Akhilesh "Automotive electronics, IT, and cybersecurity", IEEE International Conference on Electro Information Technology (EIT), 2017;
[3] Zachary A. Collier, Daniel DiMase, Steve Walters, Mark Mohammad Tehranipoor, James H. Lambert, Igor Linkov, "Cybersecurity Standards: Managing Risk and Creating Resilience", Computer, Volume: 47, Issue: 9, Sept. 2014;
[4] Craig Smith, "The car hacker's handbook. A Guide for the Penetration", ISBN-13: 978-1593277031;
[5] Sam Abbott-McCune and Lisa A. Shay, "Intrusion Prevention System of Automotive network CAN bus", IEEE International Carnahan Conference on Security Technology (ICCST), 2016;
[6] Yong Xie, Member, IEEE, Liangjiao Liu, Renfa Li, Senior Member, IEEE, Jianqiang Hu, Yong Han, and Xin Peng, Security-aware Signal Packing Algorithm for CAN-based Automotive Cyber-physical Systems, IEEE/CAA JOURNAL OF AUTOMATICA SINICA, VOL. 2, NO. 4, OCTOBER 2015.
[7] Automotive Grade Linux. url: www.automotivelinux.org.