teoresi group Engineering for human life

Automotive Spin Italia:2025

A Modular Fuzzer for CAN Network Security

Cybersecurity is a top priority in the modern era

- Modern cars are vulnerable to cyberattacks (easily found via a quick Google search)
- **ISO 21434** sets the standard for managing automotive cyber threats.
- There's a growing need for automated tools to detect these vulnerabilities

Tesla car hacked using drone

13 May 2021

Hackers Remotely Kill a Jeep on the Highway—With Me in It

21 July 2015

CAN do attitude: How thieves steal cars using network bus

6 April 2023

Challenges in Developing Tools

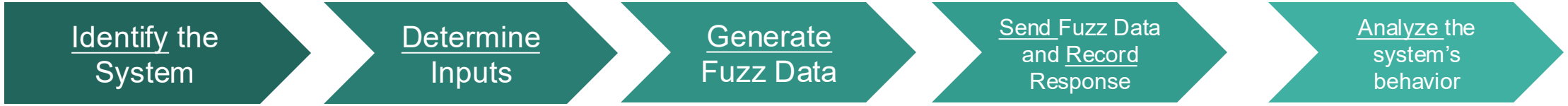
- **Variety in vehicle types**: each manufacturer uses different components and coding systems
- **Variety in attack types**: vehicle theft, remote control while driving, data theft
- **Variety in attack vectors**: Wi-Fi, Bluetooth, smart devices, Vehicle-to-Vehicle, Vehicle-to-Everything.

Fuzzy Testing

Objectives and Methodology

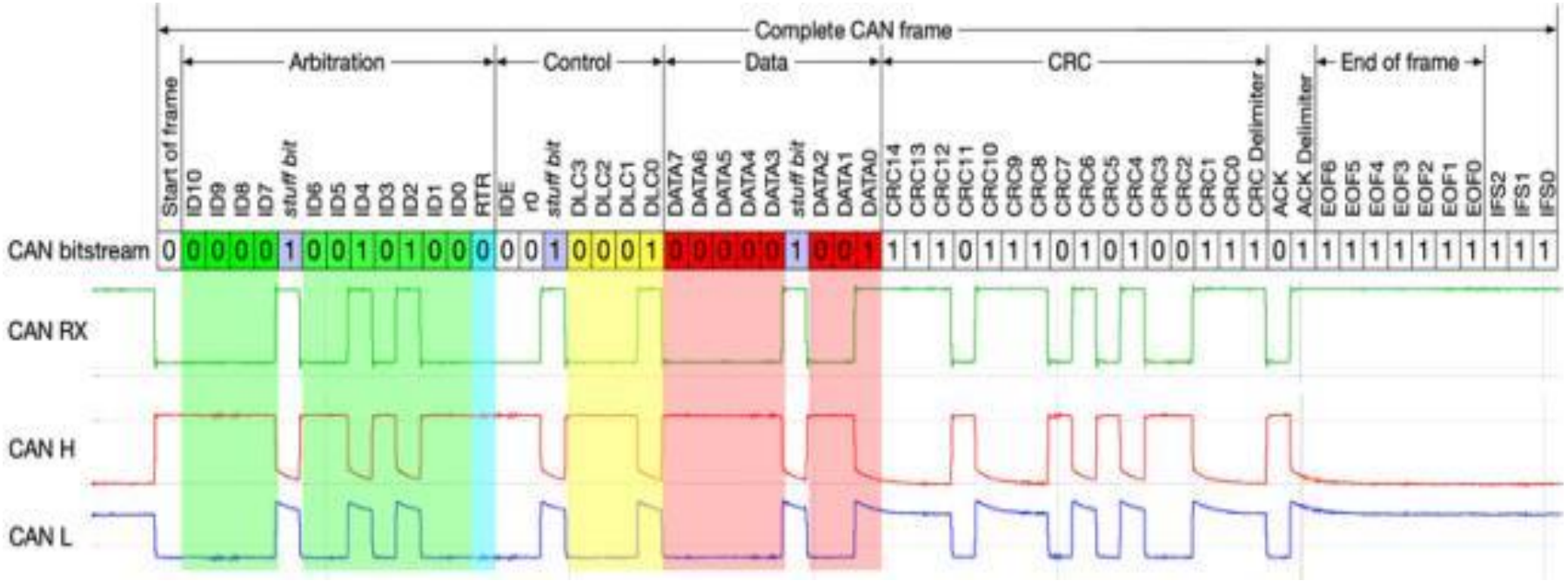
Fuzzing Testing

- Automated testing using random or crafted inputs to find crashes, errors and unexpected behaviour
- Supports black-box and white-box approaches
- Covers diverse input scenarios with effective test cases
- Enables early detection of software flaws



The CAN Protocol

- Central Nervous System of a car, connecting all ECUs
- Serial, message-based, asynchronous and broadcast Nature



CAN Bus Vulnerabilities

- CAN bus lacks encryption, allowing attackers to easily eavesdrop on vehicle data.
- Spoofing messages to control car functions may compromise vehicle safety.
- CAN protocol violates core **CIA** security principles

C I A

Confidentiality

Achieved through Encryption

Integrity

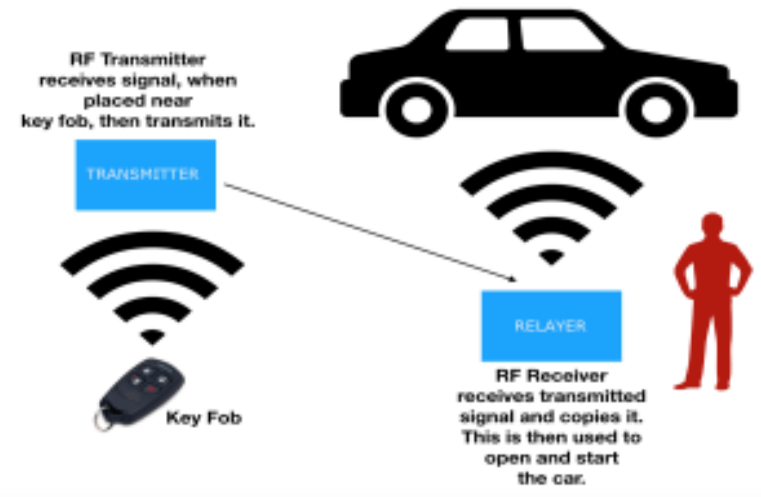
Achieved using a Digest

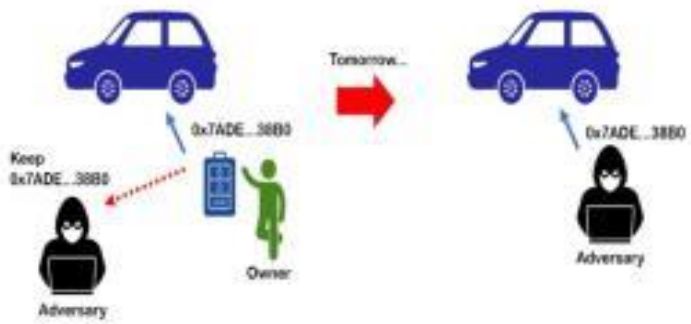
Authentication

Achieved using MAC or Digital Signature

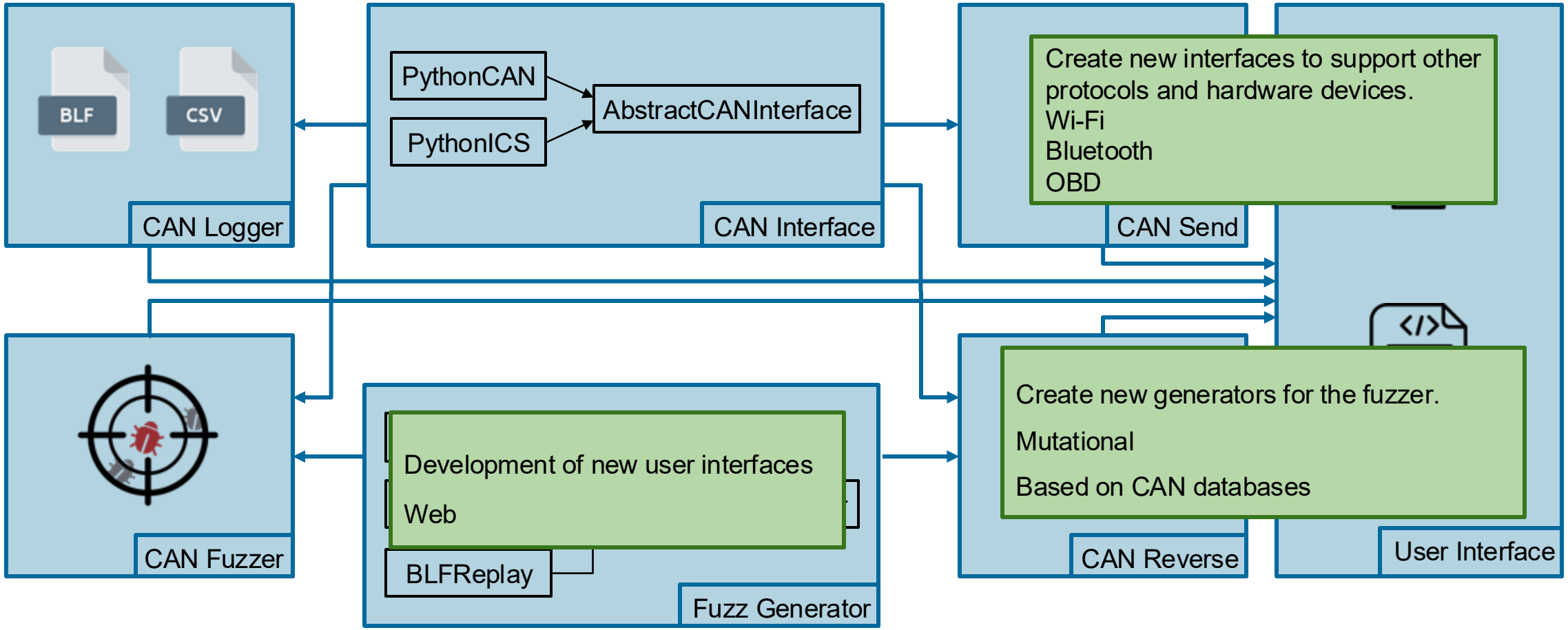
Real World example: Keyless Car Theft

- CAN frames can be injected to unlock the doors and start the engine
- Bypass security features of Smart Key due to the CAN network structure **(Key fob/RF/NFC)**
- BMW X6 M





Working Flow of Software Modules

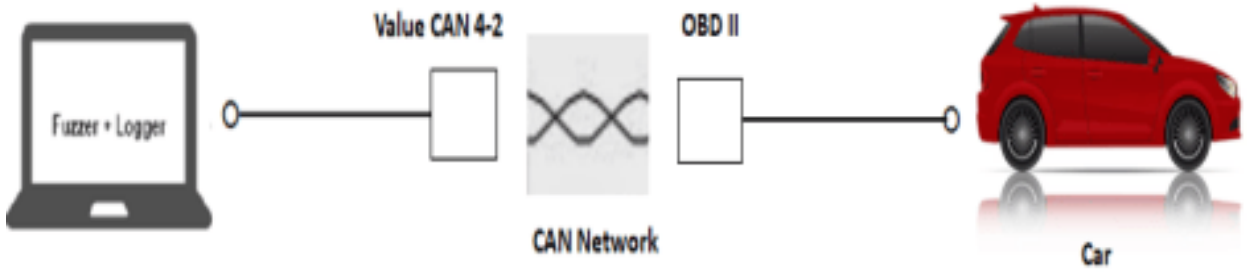


Virtual CAN BUS Attack

- **Safe Simulation**: Software-based CAN bus for testing without hardware
- **Real-World Use**: Supports fuzzing and ECU vulnerability testing
- **Python-Based**: Uses python-can for custom message injection
- **Cost-Effective**: Flexible, risk-free testing across scenarios

	timestamp	arbitrationId	isExtendedId	isCanFD	DLC	data	isErrorFrame	direction
1	1719743131.8148532	0x68	False	False	8	a95c7b41a7690fda	False	SENT
2	1719743131.82507	0x79	False	False	5	708cbf024a	False	SENT
3	1719743131.8352501	0x68	False	False	4	e9a299a5	False	SENT
4	1719743131.8454497	0x75	False	False	4	261aaab5	False	SENT
5	1719743131.8556368	0x75	False	False	0	<null>	False	SENT
6	1719743131.8657823	0x75	False	False	8	b58a8f7da8067f18	False	SENT
7	1719743131.875964	0x68	False	False	6	844976c20915	False	SENT

Real Environment



- Implementing a fuzzer attack on a generic city car
- Targeting vulnerabilities in the car's systems
- Goal to disrupt the car's ECU system

Scenario of a Generic City Car

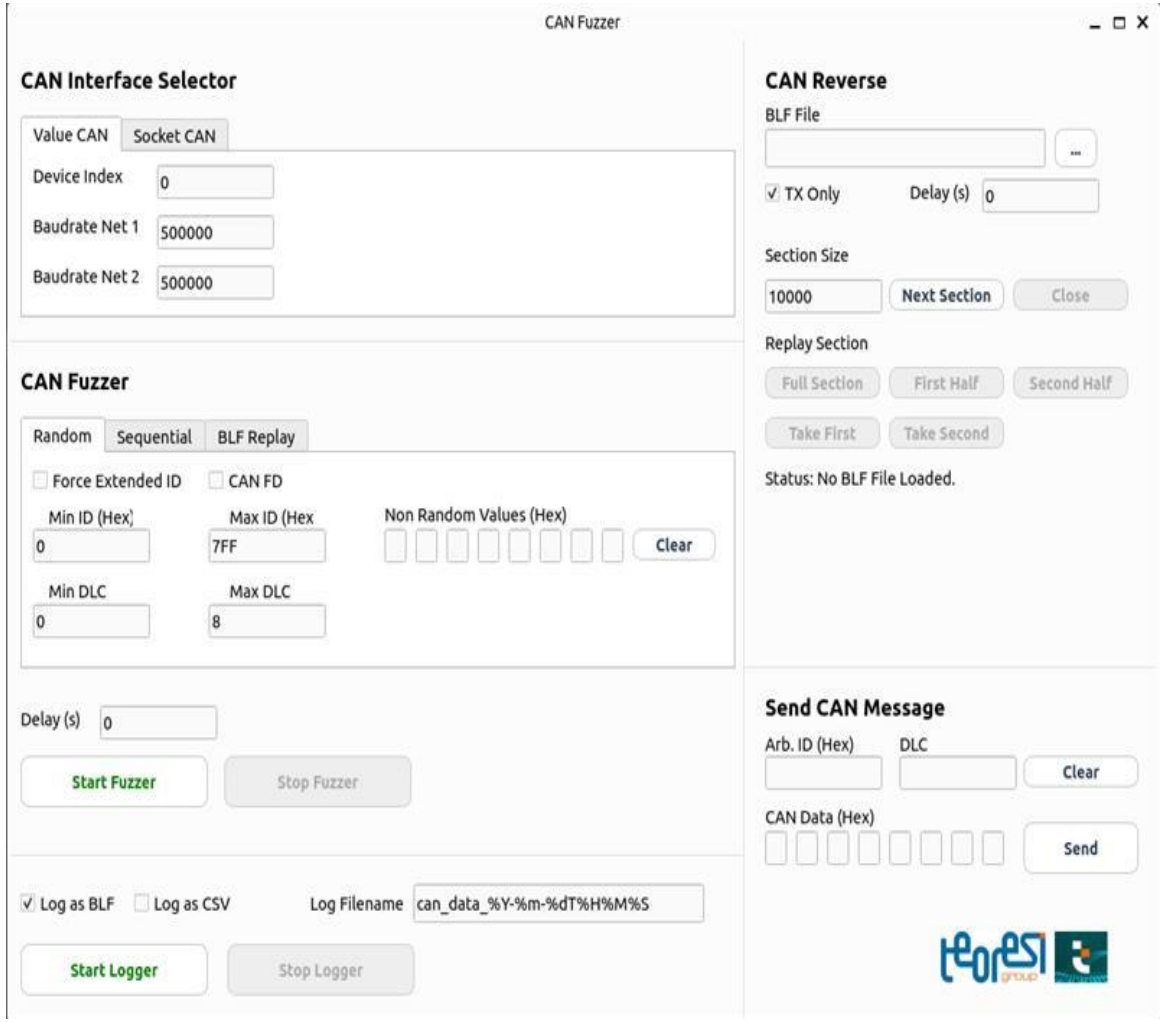
Reaction of Infotainment System

- During the attack, all display icons blinked, with a prominent red "Motor Failure" message showing error code 0184.

VCU(motor Failure)

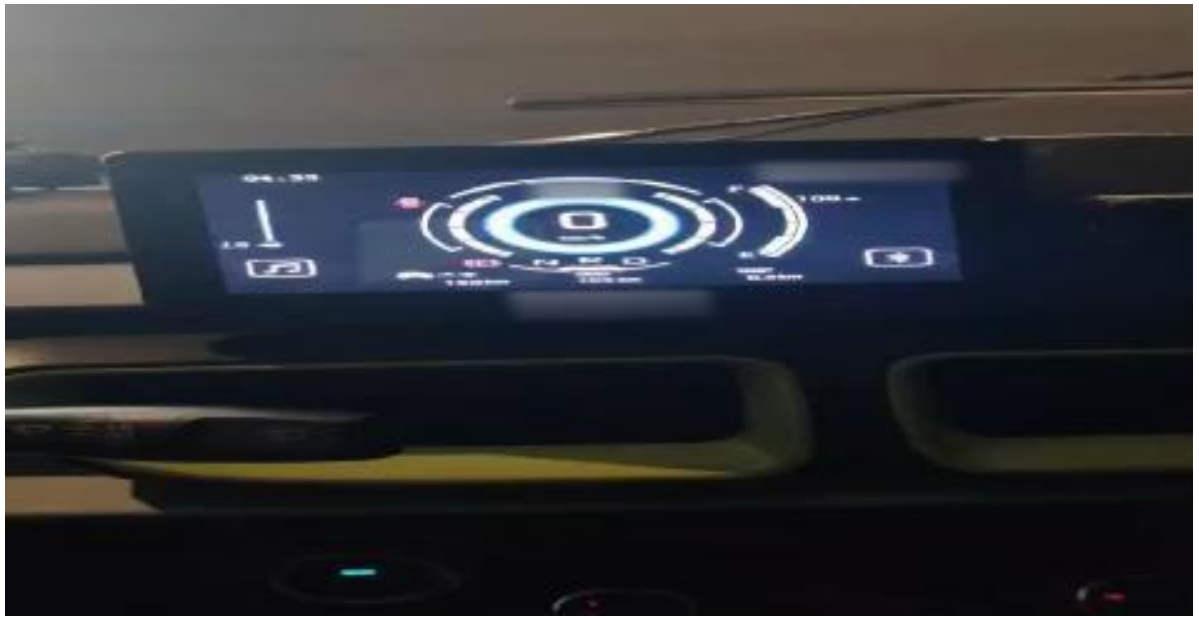
- Reverse engineering revealed the CAN ID causing the motor failure warning.
- It can trigger power steering lock and loss of other functions.

	timestamp	arbitrationId	isExtendedId	isCanFD	DLC	data	isErrorFrame	direction
1	16058395759	0x411	False	False	8	c40fde04e60a9700	False	RECV
2	16058405367	0x415	False	False	8	1027ee0db47f0790	False	RECV
3	16058498657	0x605	False	False	8	0000010000000000	False	RECV
4	16058508440	0x151	False	False	8	c401000000000000	False	RECV
5	16058518046	0x152	False	False	8	410000000f5451f	False	RECV
6	16058562619	0x150	False	False	8	4000000000000000	False	RECV



Vulnerability in Vehicle Instrument Cluster

- The initial attack disrupted the CAN bus, causing false data on the cluster.
- It also identified a message ID linked to the digital speedometer

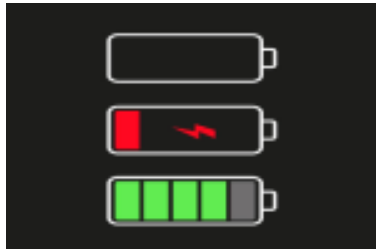


Security Risks on the Road

- Identified vulnerability in the Anti-lock Braking System (ABS)
- Leads to wheel lock-up during braking
- May cause loss of vehicle control (In emergency situation)

Random Attack on a vehicle

- Electronic systems were disrupted due to the attack, which occurred without prior knowledge of IDs.
- Caused blinking infotainment icons and **flickering** headlights
- Triggered autonomous **window** movements and **audible** alerts
- Led to sudden **battery** drain
- Displayed **error** notifications on the instrument cluster



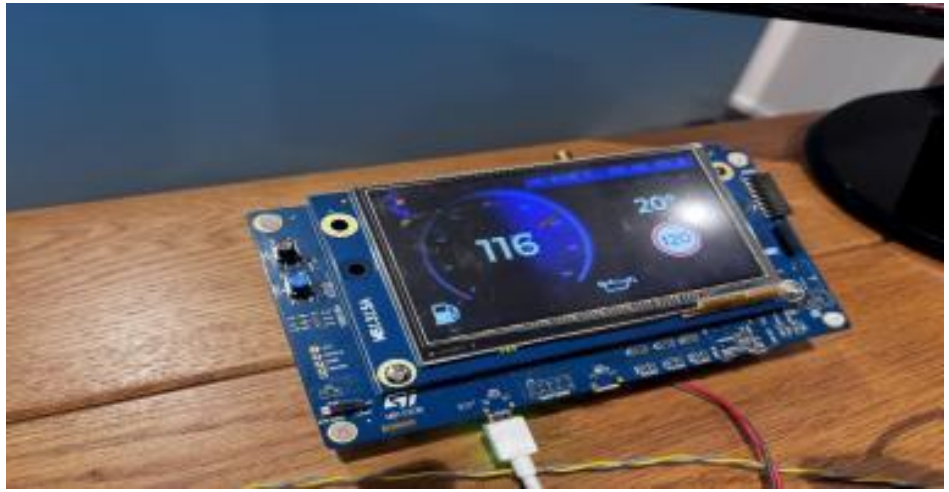
Teoresi Lab Expo

CAN Fuzzer Tool: Injects and tests CAN messages in real-time.

Setup: Uses NeoVI Pi interface and STM32 dashboard display.

Functions: Supports fuzzing, manual message sending, logging, and replay.

Purpose: Facilitates automotive cybersecurity testing, reverse engineering, and vulnerability identification in vehicle communication systems.



Thank You For Your Attention