Lessons learned from “Car Hacking” for fun and science

Sasan Jafarnejad

Sasan.jafarnejad@uni.lu
vehicularlab.uni.lu

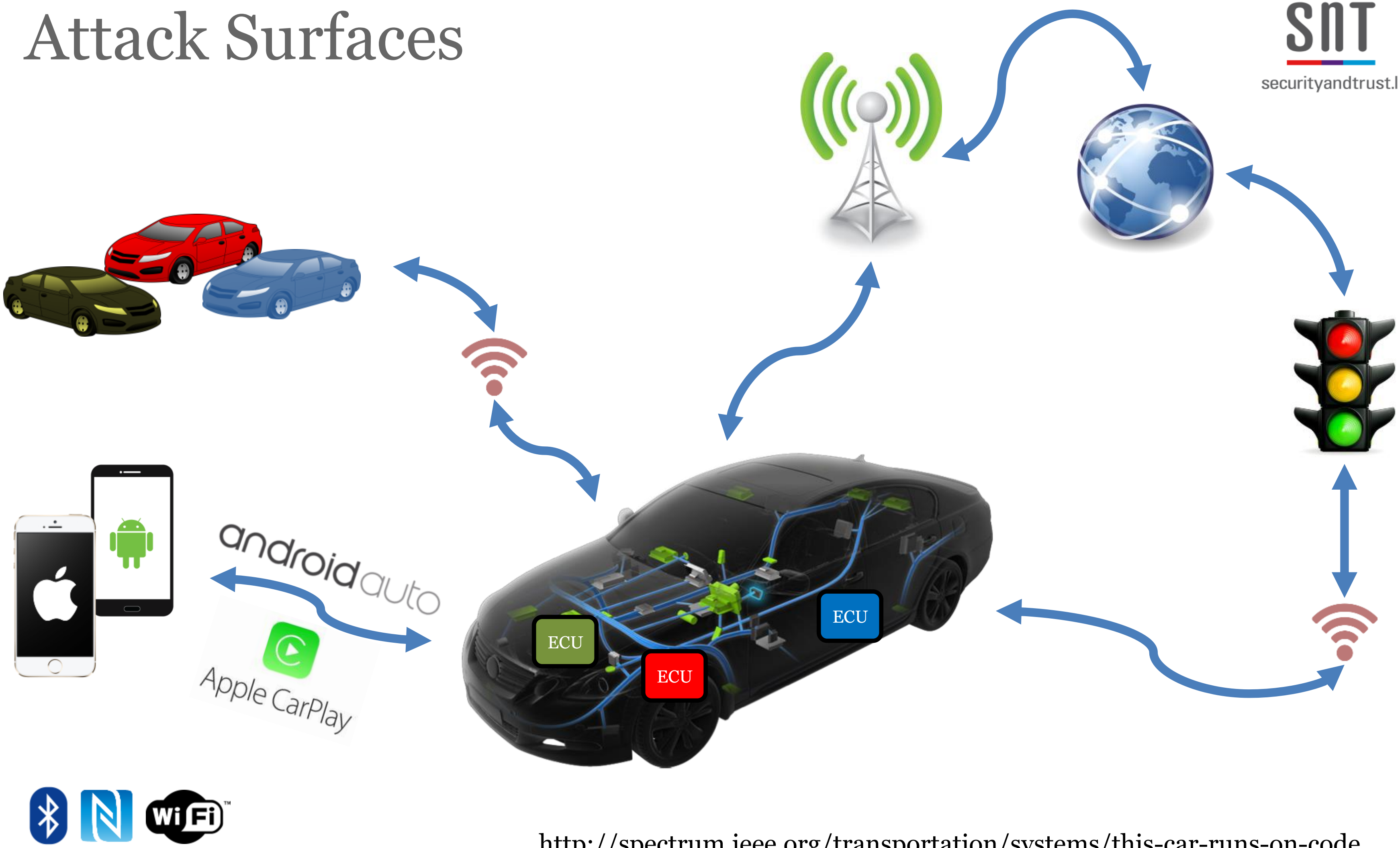
What? Car Hacking?

Jeep

http://goo.gl/5vlMjA

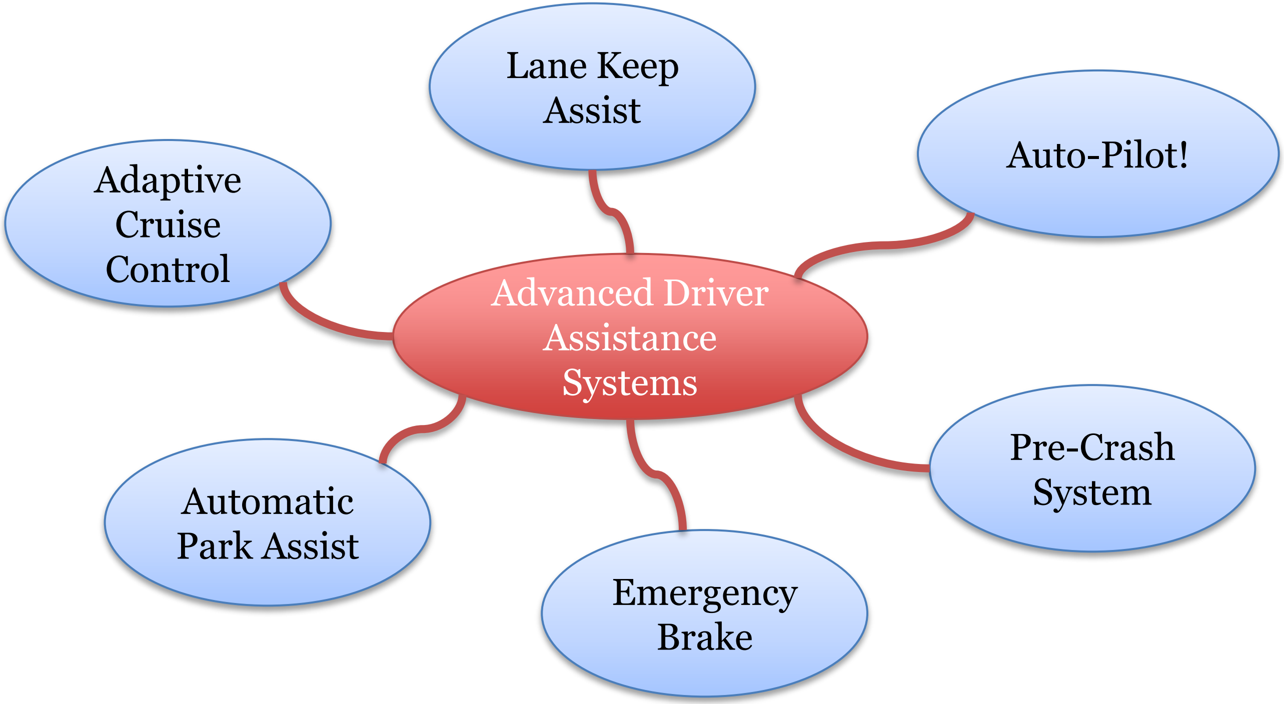
http://goo.gl/ZVyKw2

Attack Surfaces



http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

Potential Target Systems

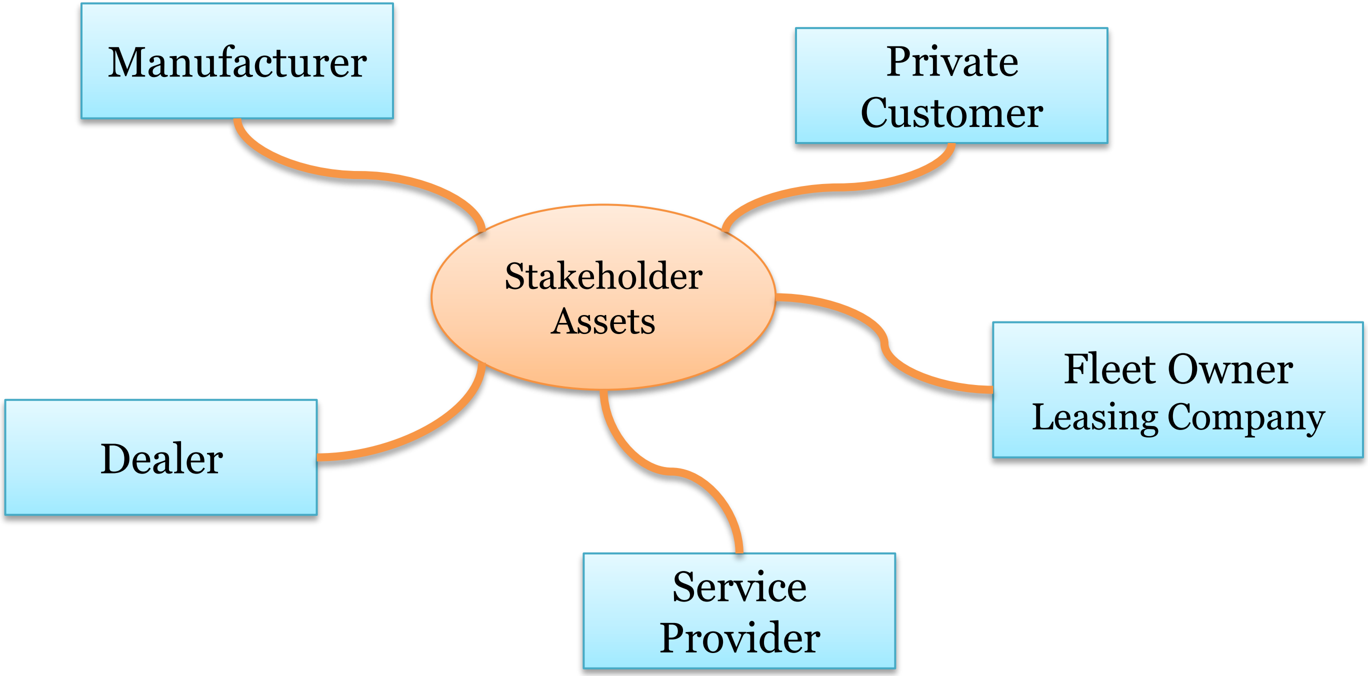


Motivation

- Car theft [1]
- Electronic Tuning
- Sabotage
- Privacy breach [2]
- Fun!!!
- Research

[1] http://goo.gl/9ibxq7
[2] Stephen Checkoway et al. “Comprehensive experimental analyses of automotive attack surfaces.” In USENIX Security Symposium, 2011.

Stakeholders



R. R. Brooks, S. Sander, J. Deng, and J. Taiber, “Automobile security concerns,” *IEEE Vehicular Technology Magazine*, vol. 4, no. 2, pp. 52–64, Jun. 2009.

Goal

1. Evaluate and discover security vulnerabilities

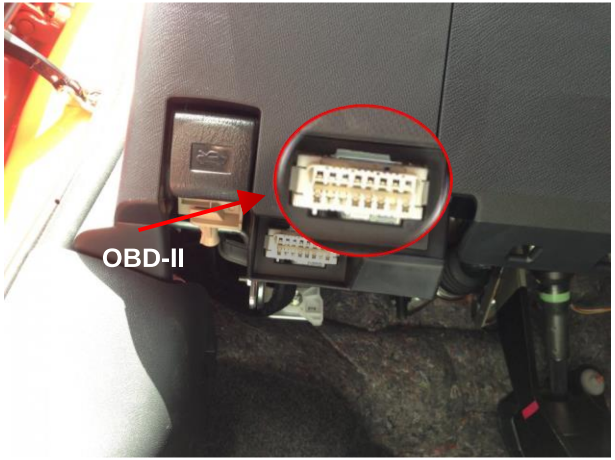
2. Demonstrate the vulnerabilities

Renault Twizy

Toyota Prius

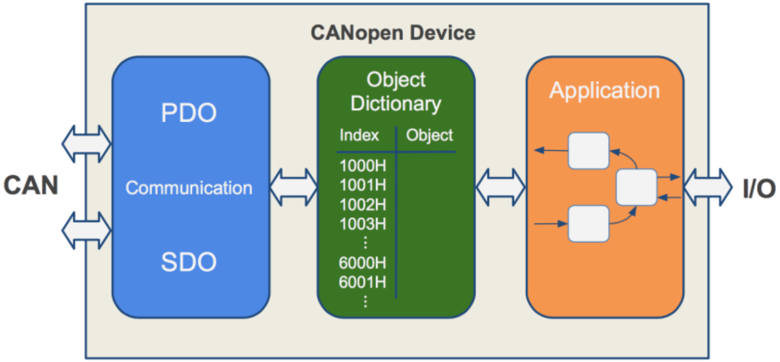
Approach

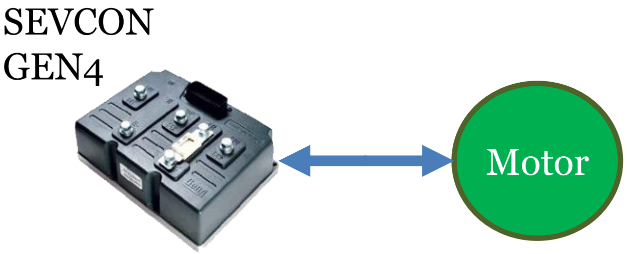
- Attacks on CAN bus
- Through OBD-II port



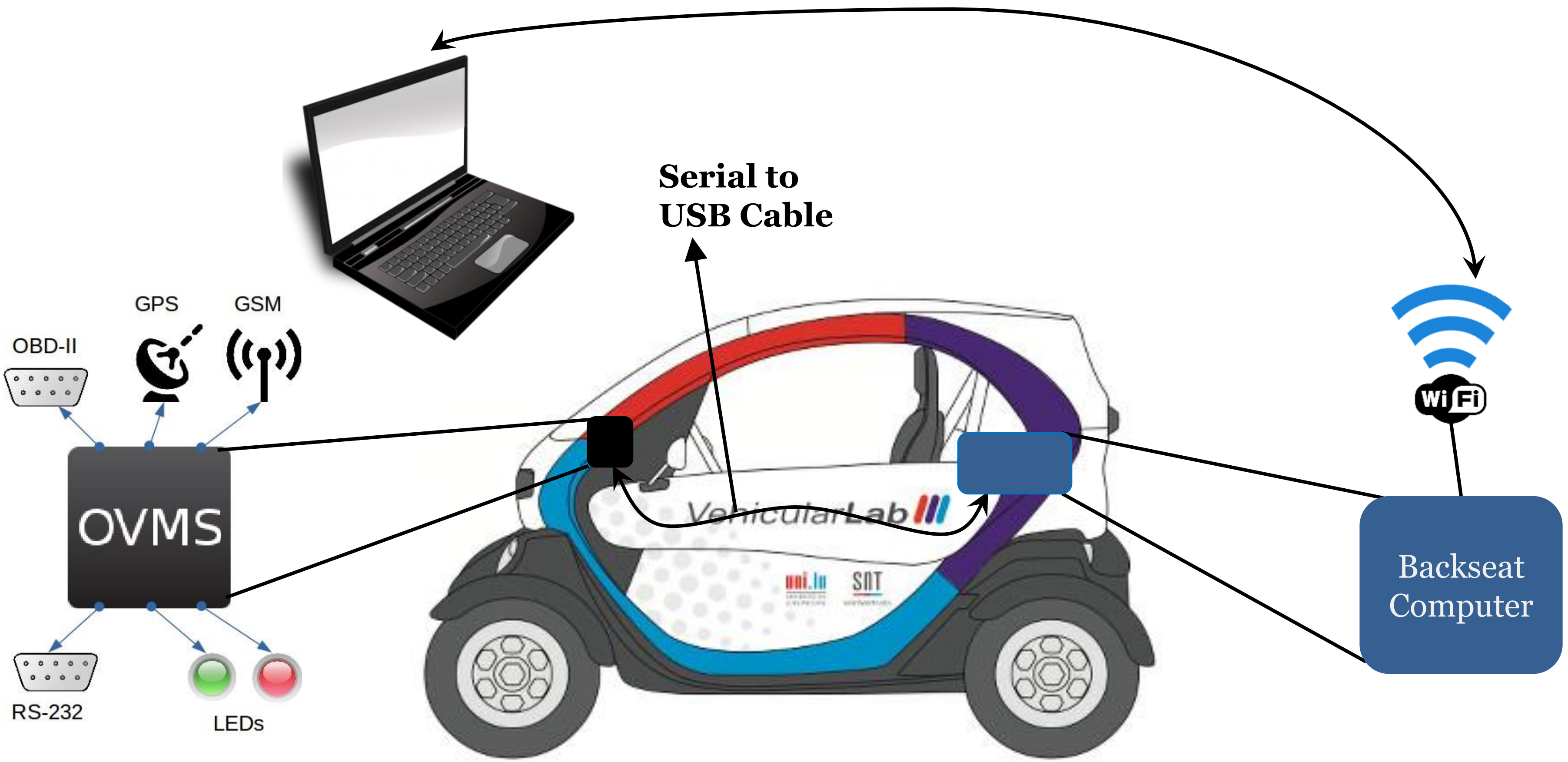
Renault Twizy

- All electric car
- No door locks or windows
- Employs SEVCON GEN4 as motor controller
- Uses CANopen as higher layer protocol



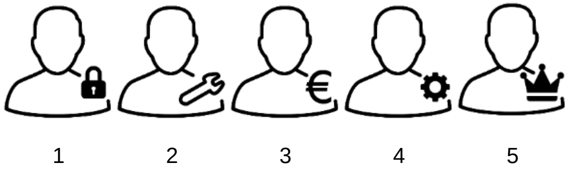


Experimental Setup

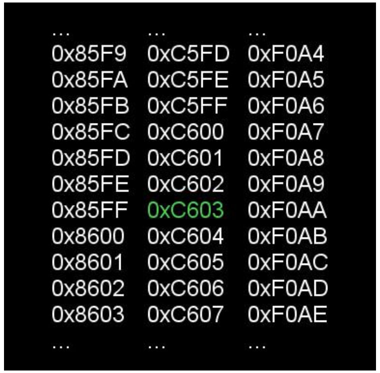


Reconfiguration

In SEVCON Gen4 some entries require authentication



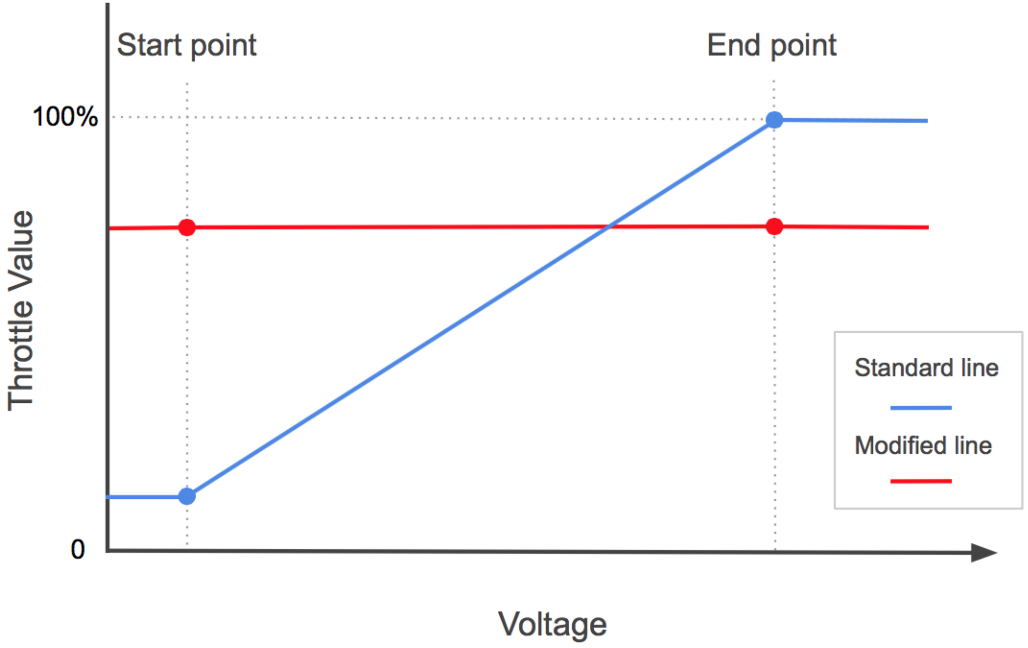
Authentication needs a 2-bytes long passcode



```
…        …        …
0x85F9   0xC5FD   0xF0A4
0x85FA   0xC5FE   0xF0A5
0x85FB   0xC5FF   0xF0A6
0x85FC   0xC600   0xF0A7
0x85FD   0xC601   0xF0A8
0x85FE   0xC602   0xF0A9
0x85FF   0xC603   0xF0AA
0x8600   0xC604   0xF0AB
0x8601   0xC605   0xF0AC
0x8602   0xC606   0xF0AD
0x8603   0xC607   0xF0AE
…        …        …
```

Findings

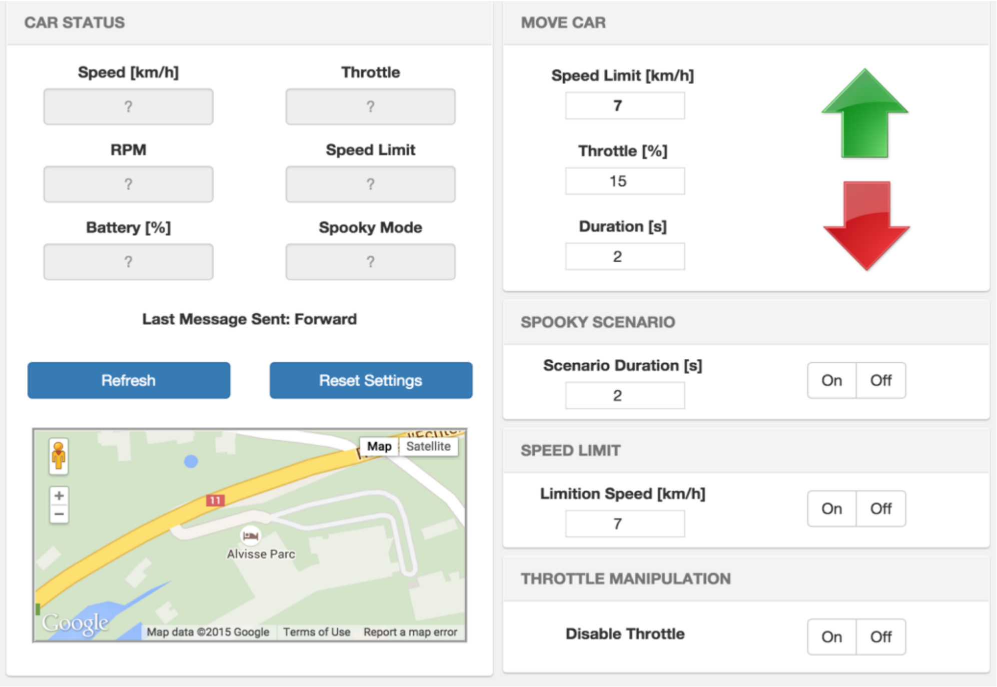
- Control throttle [1]
- Motor direction
- Limit the speed
- Disable throttle and etc.



[1] S. Jafarnejad, L. Codeca, W. Bronzi, R. Frank, T. Engel, ”A Car Hacking Experiment: When Connectivity meets Vulnerability” IEEE GLOBECOM’15 - Wi-UAV Workshop

Remote Control

Web Interface



CAR STATUS

Speed [km/h]: ?

Throttle: ?

RPM: ?

Speed Limit: ?

Battery [%]: ?

Spooky Mode: ?

Last Message Sent: Forward

MOVE CAR

Speed Limit [km/h]: 7

Throttle [%]: 15

Duration [s]: 2

SPOOKY SCENARIO

Scenario Duration [s]: 2

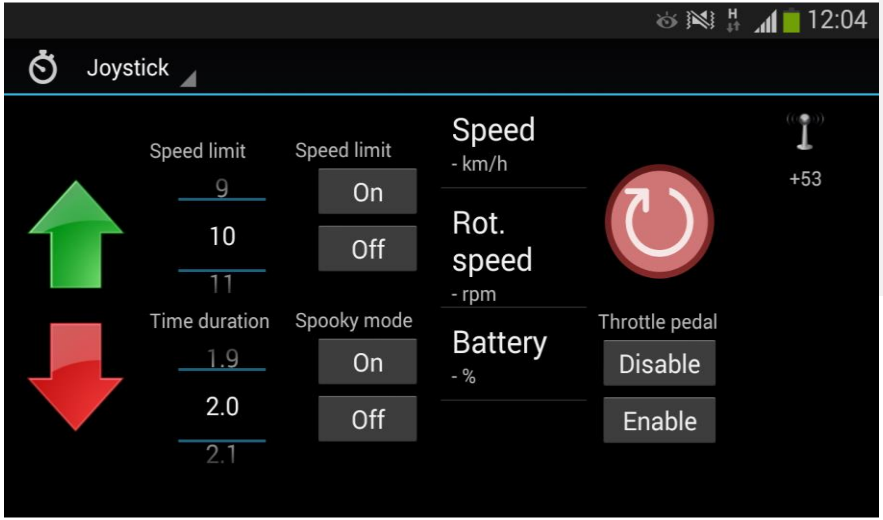
SPEED LIMIT

Limition Speed [km/h]: 7

THROTTLE MANIPULATION

Disable Throttle

Android Application

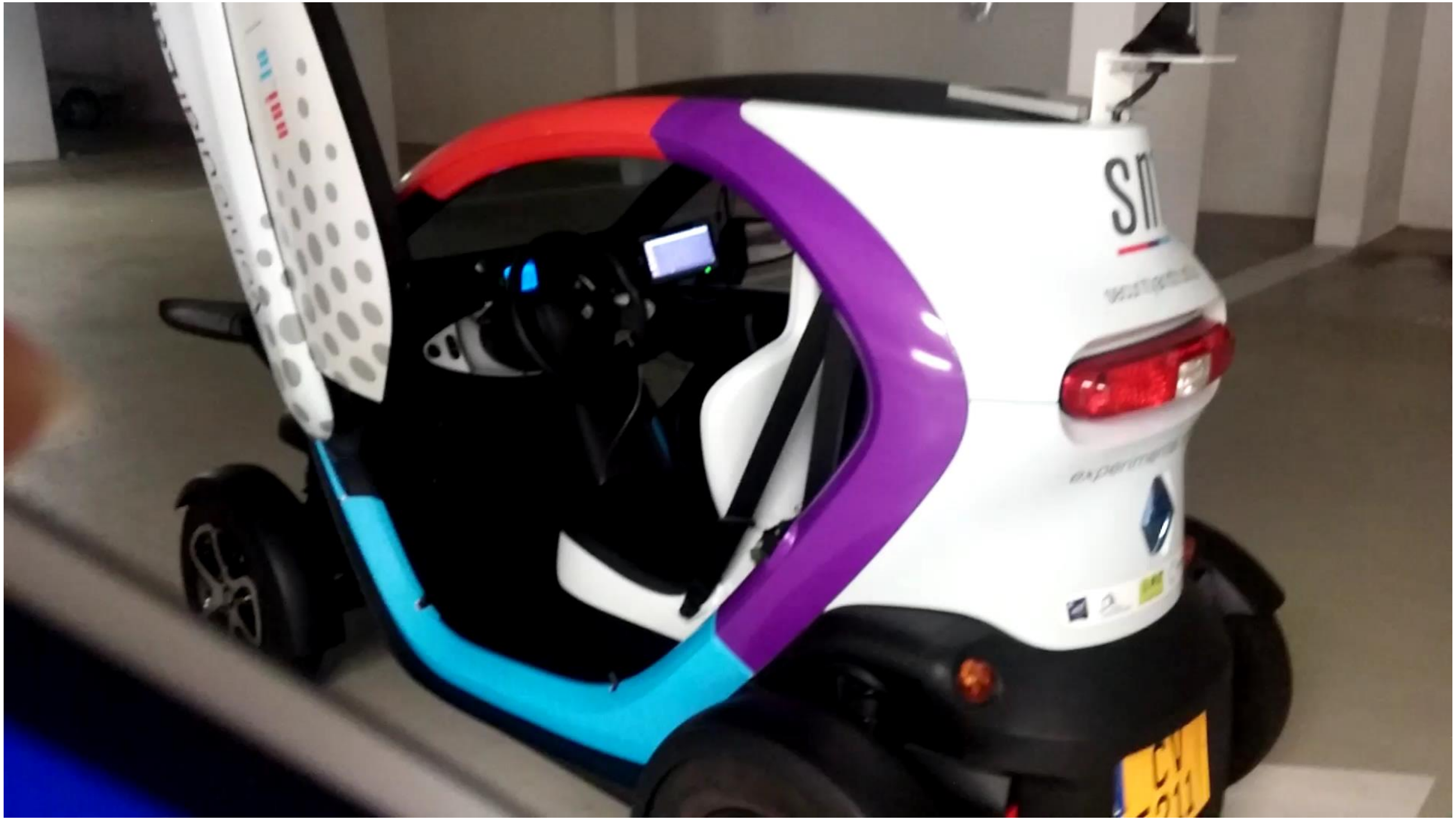


Attack Scenarios for Twizy

- Forcing the car to go forward or backward.
- Limiting the speed.
- Setting unsafe motor and voltage parameters.
- Randomly changing motor direction.
- Randomly change the conversion map.

Attacks can be triggered by:

Demo Video



Toyota Prius

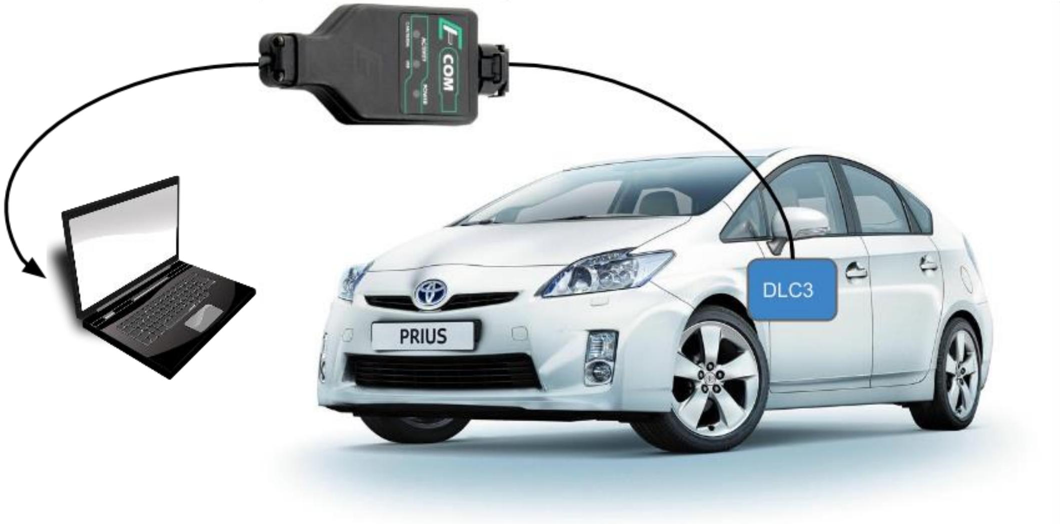
Based on a work by Miller and Valasek [1]

- Full hybrid electric
- Electronic controls
- Cyber-Physical Systems:
  - Lane Keep Assist, Intelligent Park Assist
  - Pre Collision System, Adaptive Cruise Control

[1] Charlie Miller and Chris Valasek. Adventures in automotive networks and control units. In DEF CON 21 Hacking Conference. Las Vegas, NV: DEF CON, 2013.

Experimental Setup

ECOM Cable



Normal CAN Packets

- Are periodically sent over network

ID_{High} ID_{Low} Length Data

- Mostly have checksum in Data[Length-1]

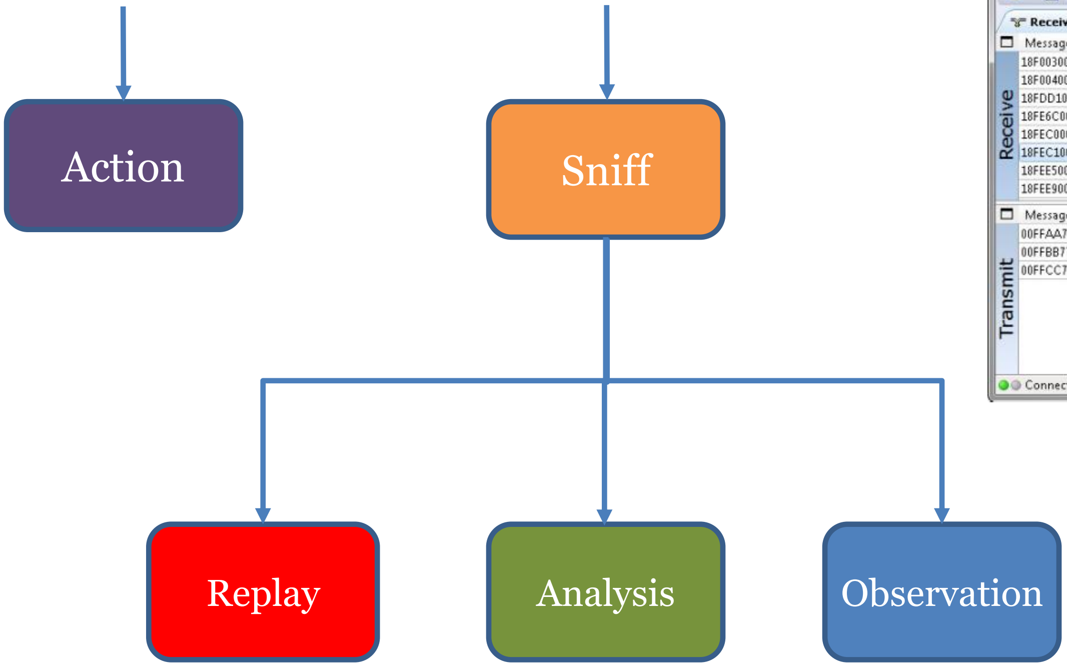
$$\text{Checksum} = (\text{ID}_{\text{High}} + \text{ID}_{\text{Low}} + \text{Length} + \sum_{i=0}^{Length-2} Data[i]) \bmod 256$$

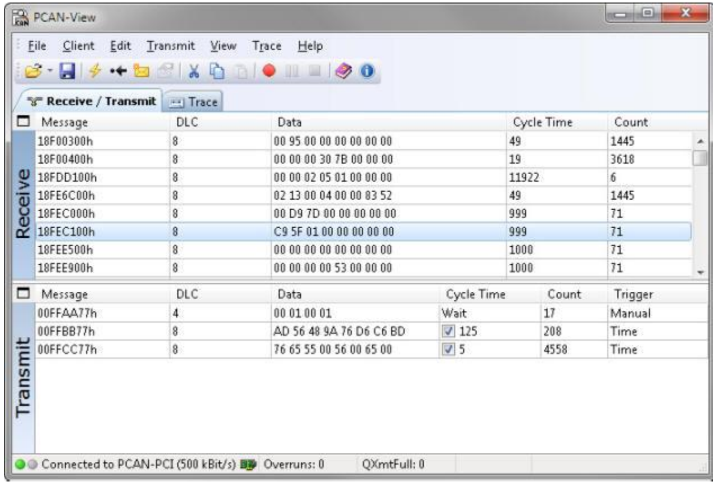
- Example Packet: Speed

ID: 00B4, Length: 8, Data: 00 00 00 00 91 07 94 E8

  - 0x91 is sequence number 00-FF
  - 0x0794 is the speed times 100 in kph
  - 0xE8 is the checksum

Replay Basics





Message	DLC	Data	Cycle Time	Count
18F00300h	8	00 95 00 00 00 00 00 00	49	1445
18F00400h	8	00 00 00 30 7B 00 00 00	19	3618
18FDD100h	8	00 00 02 05 01 00 00 00	11922	6
18FE6C00h	8	02 13 00 04 00 00 83 52	49	1445
18FEC000h	8	00 D9 7D 00 00 00 00 00	999	71
18FEC100h	8	C9 5F 01 00 00 00 00 00	999	71
18FEE500h	8	00 00 00 00 00 00 00 00	1000	71
18FEE900h	8	00 00 00 00 53 00 00 00	1000	71

Message	DLC	Data	Cycle Time	Count	Trigger
00FFAA77h	4	00 01 00 01	Wait	17	Manual
00FFBB77h	8	AD 56 48 9A 76 D6 C6 BD	☑ 125	208	Time
00FFCC77h	8	76 65 55 00 56 00 65 00	☑ 5	4558	Time

Connected to PCAN-PCI (500 kBit/s) Overruns: 0 QXmtFull: 0

Diagnostics CAN Packets

securityandtrust.lu

- Typically sent only by diagnostic tools
- Needs Toyota TechStream and Pass-Through cable
  - Sniff and Analyze the communications
- Instead we used information from Miller and Valasek [1]

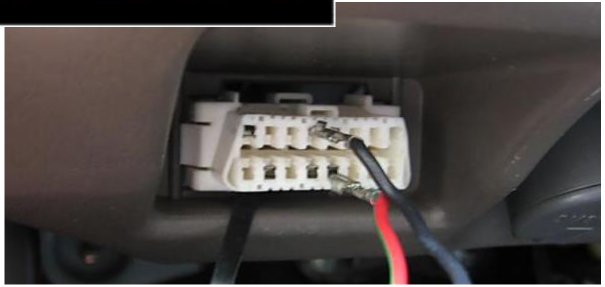
[1] Charlie Miller and Chris Valasek. Adventures in automotive networks and control units. In DEF CON 21 Hacking Conference. Las Vegas, NV: DEF CON, 2013.

Findings

Normal Packets	Diagnostics Packets
• Braking –By forging ACC packets • Steering – Using IPAS – Using LKA but very limited • False speed indicator • False gear indicator	• Doors and Trunk –Lock/Unlock • Fuel Gauge • A/C Fan • Seat belt Tightening

Challenges

- No safe way for testing
- No access to internal wiring
- Serious error messages
- Frames have **checksum**
- Frames have **pre-conditions**:
  - Steering requires false speed and gear state
  - Although **brake** using ACC worked, **acceleration** did not



Attack Scenarios

Assuming attaching a device such as OVMS

- Manipulating the instrument panel
- Producing errors on CAN bus disables Hybrid Synergy Drive
- Brake abruptly on high speeds
- Steering at high speeds
- Continuously braking does not let the car move

Attacks can be triggered by:

Demo Video

Suggestions

Renault Twizy	Toyota Prius
• Anti brute-force mechanism	• Respect sequence numbers better
• Distinct passcode for each device	• Detect added packets
• Prevent unsafe reconfiguration	
• Provide door locks and windows!	

Discussion

Problems	Solutions
• Glue codes [1] • Deviations from standards [1] • Lack of security standards • Cost limitations • Vehicle lifetime	• Respect current standards and guidelines • Integrating security considerations into standards such as ISO-26262 • Legislations • IDS for cars

[1] Stephen Checkoway et al. “Comprehensive experimental analyses of automotive attack surfaces.” In USENIX Security Symposium, 2011.

Takeaway message

If your car has any
Cyber-Physical Systems
you may need to be worried!

Current Research

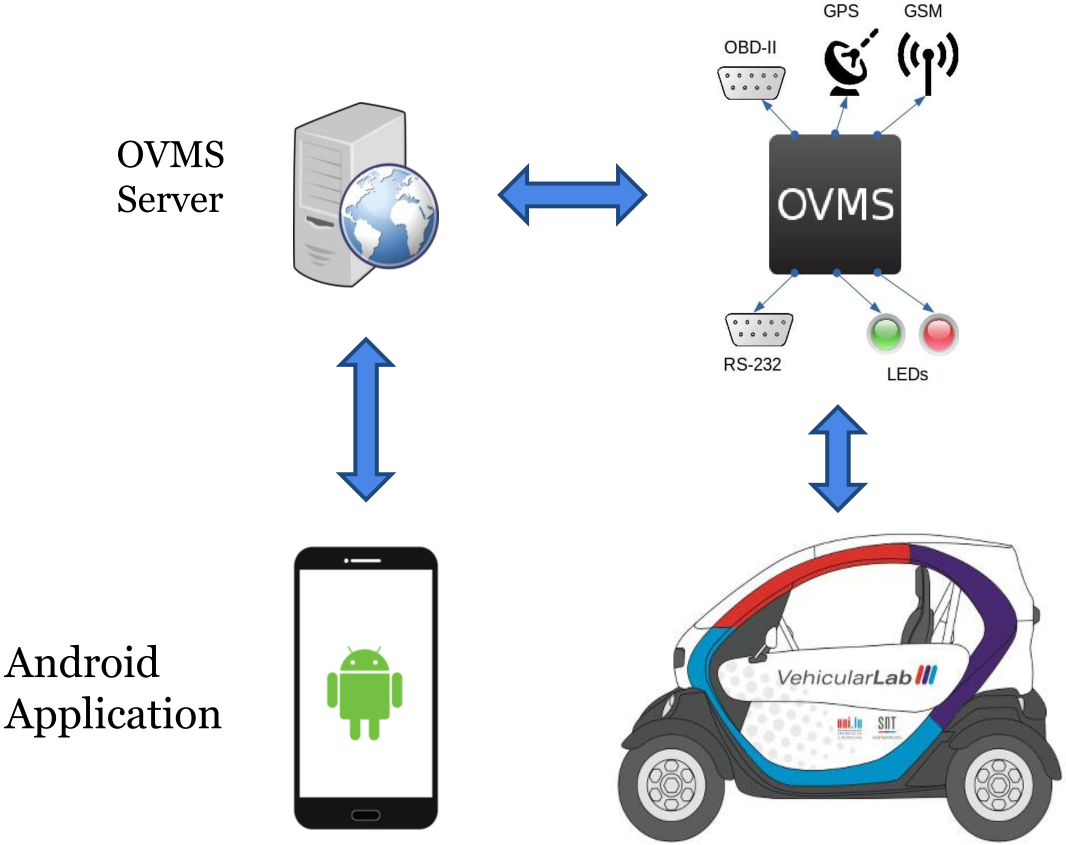
Privacy aware driver profiling

- Efficient detect of risky maneuvers based on vehicle data and contextual information.
- Prevent information leakage while preserving data utility.

Questions?

sasan.jafarnejad@uni.lu
vehicularlab.uni.lu

Experimental Setup

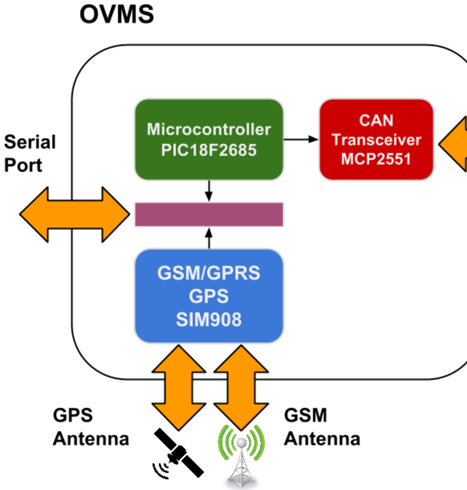


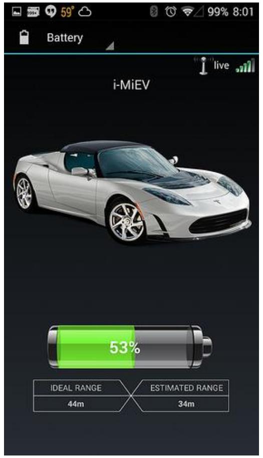
OVMS Server

Android Application

OVMS

- Open Vehicles Monitoring System


OVMS
Serial Port
Microcontroller PIC18F2685
CAN Transceiver MCP2551
CAN OBD-2
GSM/GPRS GPS SIM908
GPS Antenna
GSM Antenna


99% 8:01
Battery
live
i-MiEV
53%
IDEAL RANGE
44m
ESTIMATED RANGE
34m