A Brief History of Automotive Insecurities

Martin Schmiedecker

$whoami

- Bosch Engineering by day
- Online privacy by night
- Digital forensics in between
- Meme artist
- Goes by @Fr333k

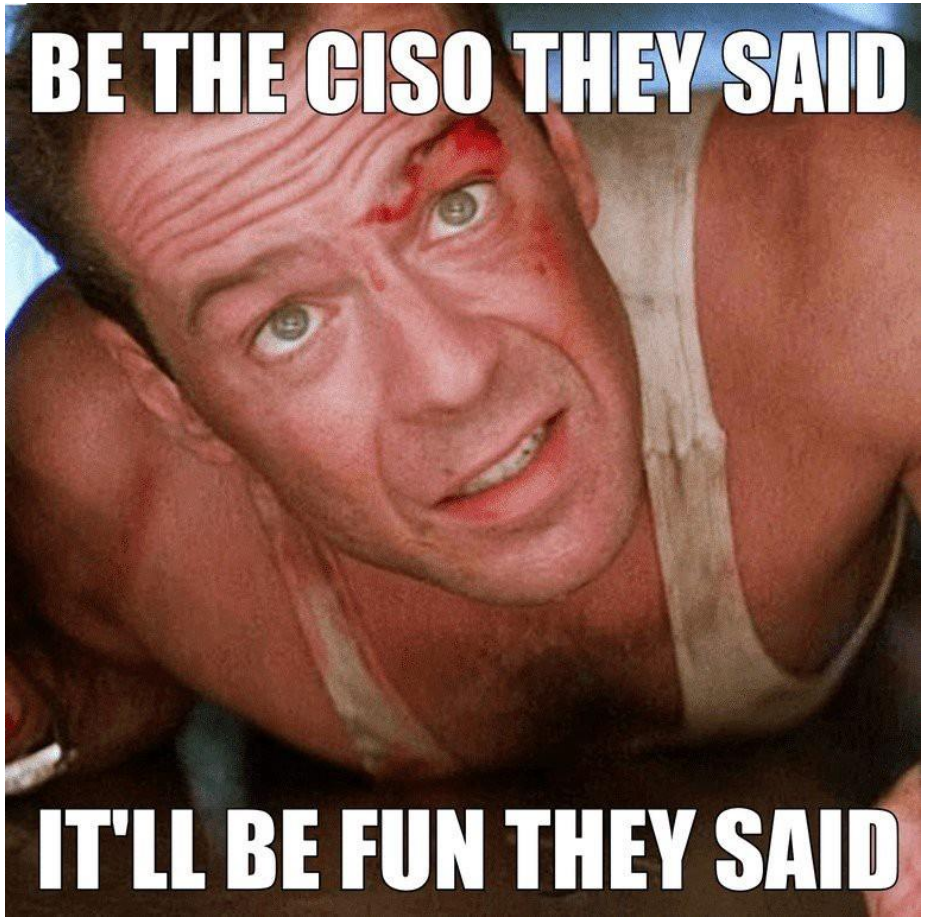
- References = klick the picture

Goal of this talk

- VERY busy area of research
- Identify the most relevant ones
- Your mileage may vary

Objectives:

- Real-world, not theoretical
- Bypassing security goal



What to expect

- Only public stuff
- Just a selection

Basically, two groups:

- Hackers, for the fame
- Companies, for the fame (& fortune)

Not included

- Automotive basics
- APIs and backend security
- Charger communication
- Tuning
- Immobilizers
- Relay attacks
- Locking i.e., Megamos, HiTag2

2010 Koscher et. al

- Paper at IEEE Security & Privacy 2010
- Replay, inject & fuzz CAN messages
- Kill engine, apply brakes, disable brakes

Experimental security analysis of a **modern automobile**

K Koscher, A Czeskis, F Roesner... - ... on **security** and ..., 2010 - ieeexplore.ieee.org

Modern automobiles are no longer mere mechanical devices; they are pervasively monitored and controlled by dozens of digital computers coordinated via internal vehicular ...

☆ Speichern 99 Zitieren Zitiert von: 2048 Ähnliche Artikel Alle 49 Versionen

2010 Koscher et. al

2011 Checkoway et. al

- Paper at USENIX Security 2011
- Command and control using IRC
- Location tracking
- In-vehicular audio exfiltration
- CD firmware update unsigned
- Buffer overflow in WMA parser
- Remote exploit in calling telematics unit

2013 Houtenbos/Kloosterman

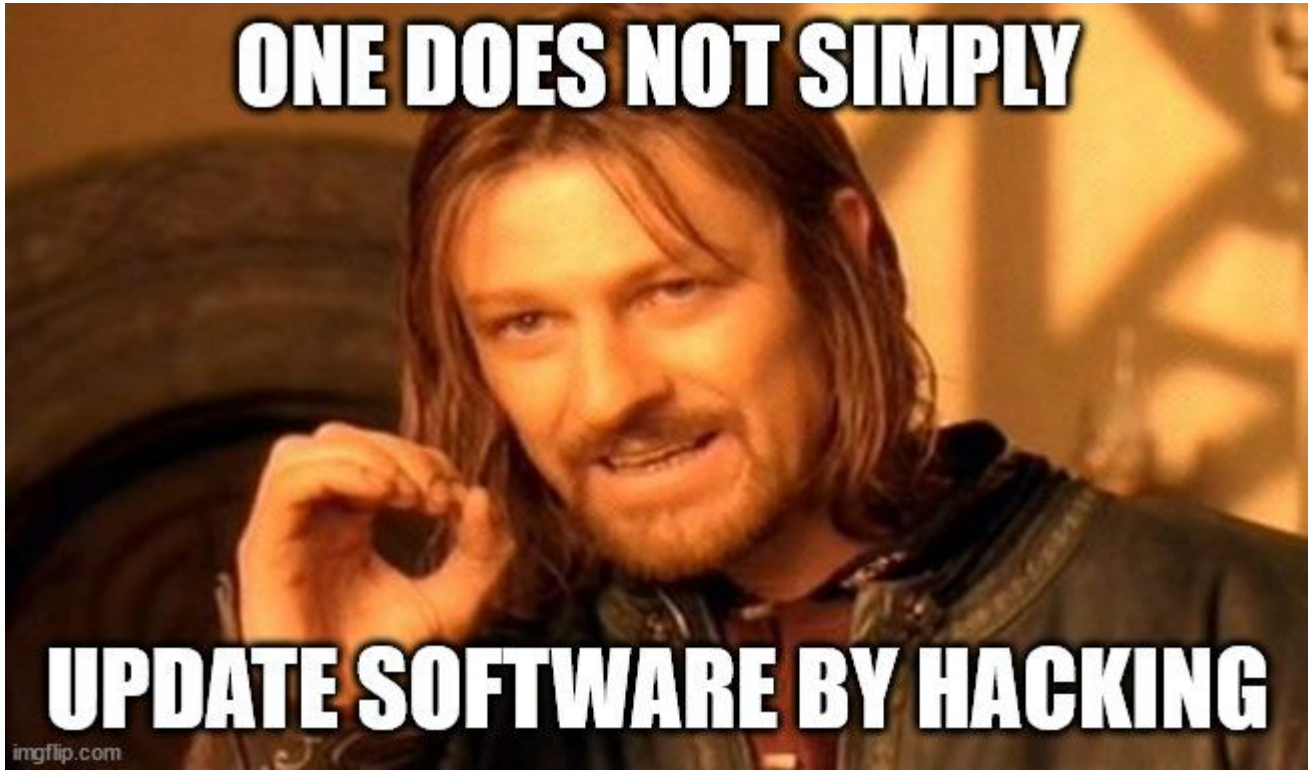
- *Tinfoil Attack* against BMW ConnectedDrive
- Students from University of Amsterdam
- HTTP proxy with plain (base64) authentication
- Dedicated APN with 160.50.0.0/16
- UserAgent: Firefox 3.5 on Win7?

2015 ADAC/Spaar

- Cinterion GPRS/Edge modem in *Combobox*
- Fake base station as IMSI catcher
- Fleet keys for SMS encryption
- HTTP GET for unlocking
- Unauthenticated XML for config updates
- 2.2 million vehicles affected (BMW, Mini, Rolls Royce)

2015 GM OnStar

- GM hacked itself, kind-a
- Remote software update
- With no previous capability
- About 2 million OnStar 8



2015 Miller/Valasek

2015 Miller/Valasek

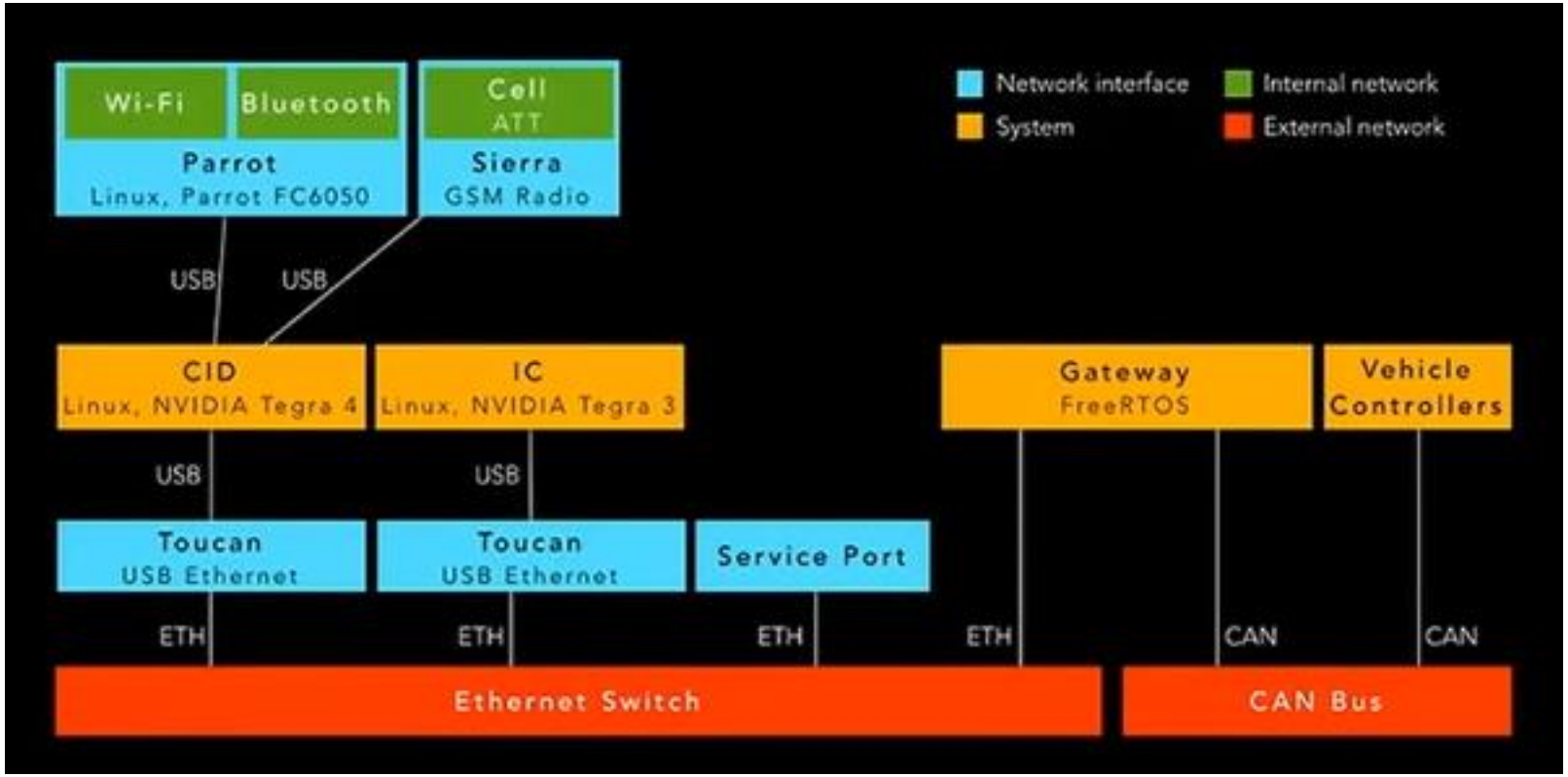
2015 Miller/Valasek

- Uconnect unit, running QNX
- Sprint 3G connection
- Open ports over wifi (D-BUS)
- Software updates over USB for jailbreak

- Two IPs per car, one for 3G services
- Scanning 21.0.0.0/8 and 25.0.0.0/8
- Connect, done

2015 Rogers/Mahaffey

- DEF CON 23
- Pentest with local focus
- VPN to Mothership
- Backdoored with SSH
- Turn car off, open doors



2015 Foster et. al

- Aftermarket OBD-II dongle
- 2G (3G for later models) and USB
- Same SSH keypair on all
- SSH, telnet and SSH on WAN interface
- 2k+ devices on Shodan

2016 Miller/Valasek

- Blackhat 2016
- Get ECU into bootrom mode
- Send conflicting messages
- Pre-date counters
- Engage brakes
- Steering
- Acceleration

2016 Keen Labs

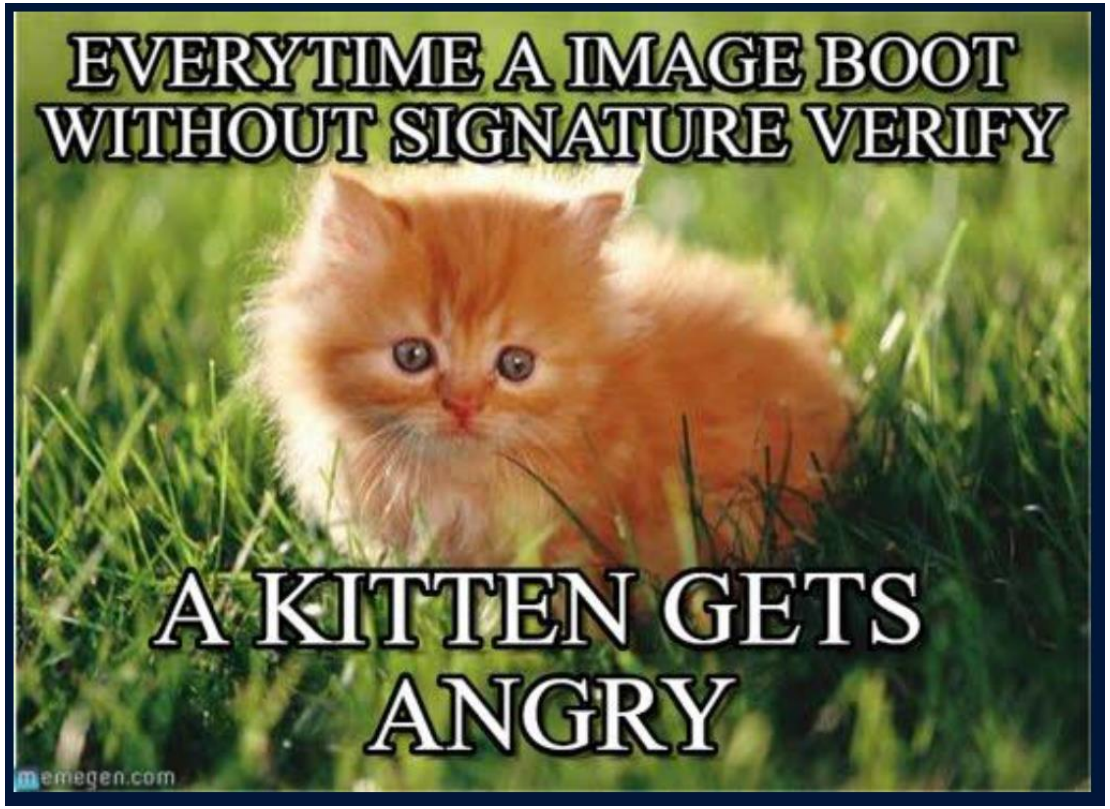
- Achieved CAN sending over wifi on Tesla S
- Wifi auto connect
- Trigger webkit exploit
- Elevate privileges with known kernel vulnerability

2017 Keen Labs

- Presented at Blackhat 2017
- Malicious update for gateway
- Not signed – afterwards everything signed
- Pushing kernel from 2.6.36 to 4.4.35
- Xmas show

2018 Keen Labs

- Blackhat 2018, Tesla X
- Targeting gateway & body controller
- Kernel module for Tegra for elevating privileges
- Bypass signature verification with leading spaces
- Details on the Tesla X Xmas show



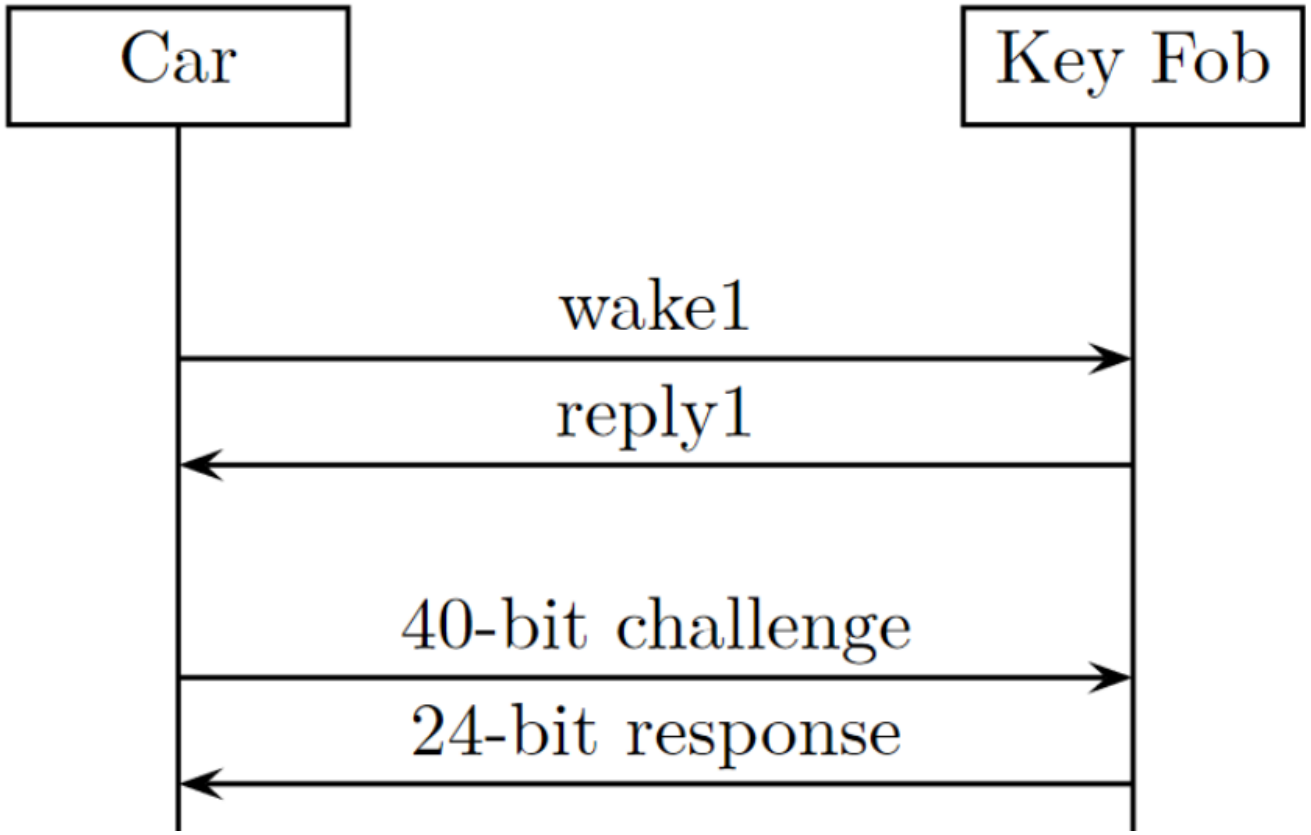
2018 Wouters

Required:

- Two challenges (from car)
- One response (form keyfob)

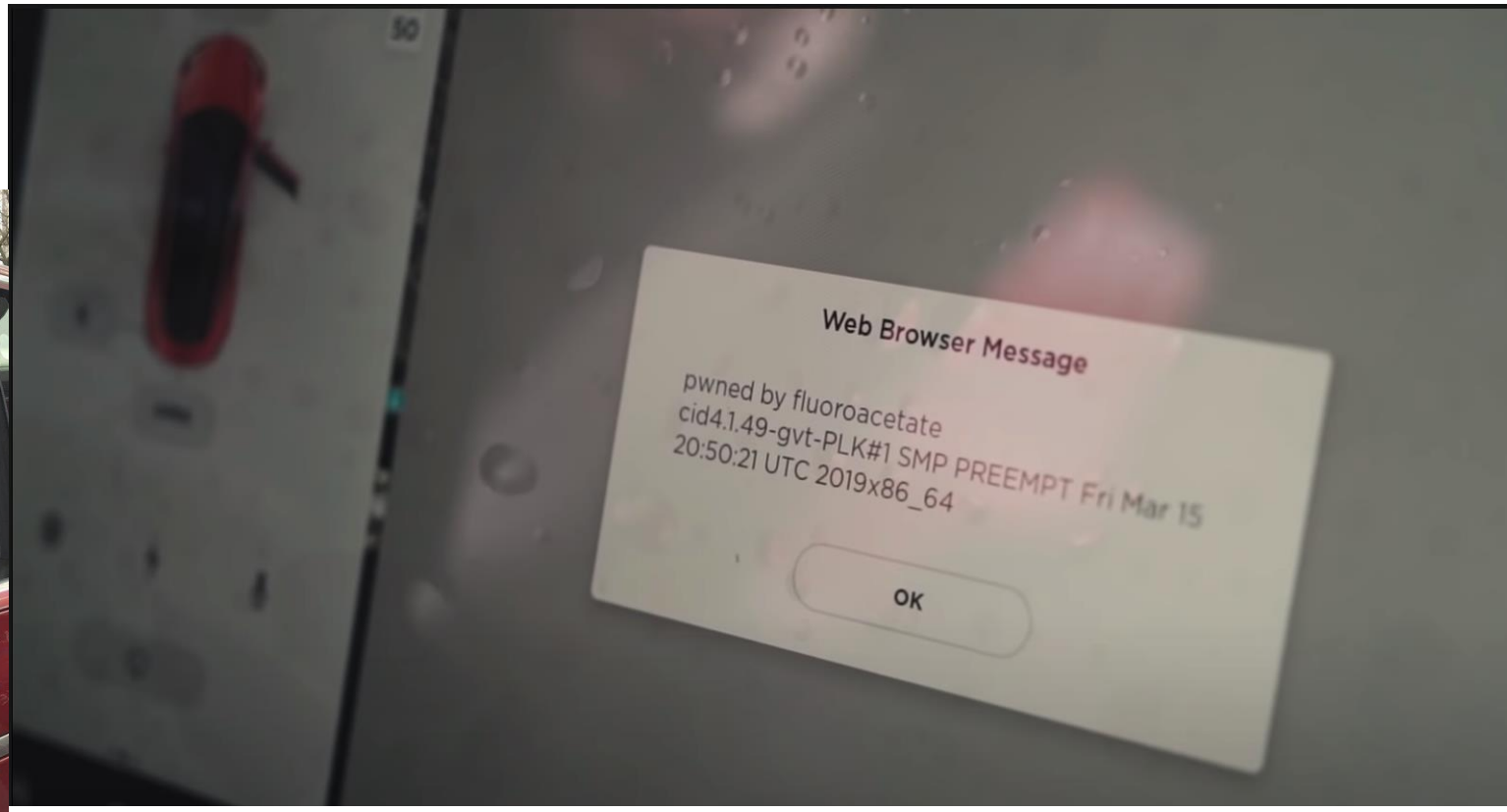
2018 Wouters

- External supplier
- Proprietary crypto (DST40)
- Built a rainbow table with 5.6 TB



2019 pwn2own

- Tesla 3 infotainment running 4.14 kernel
- JIT bug in Browser
- 35,000$

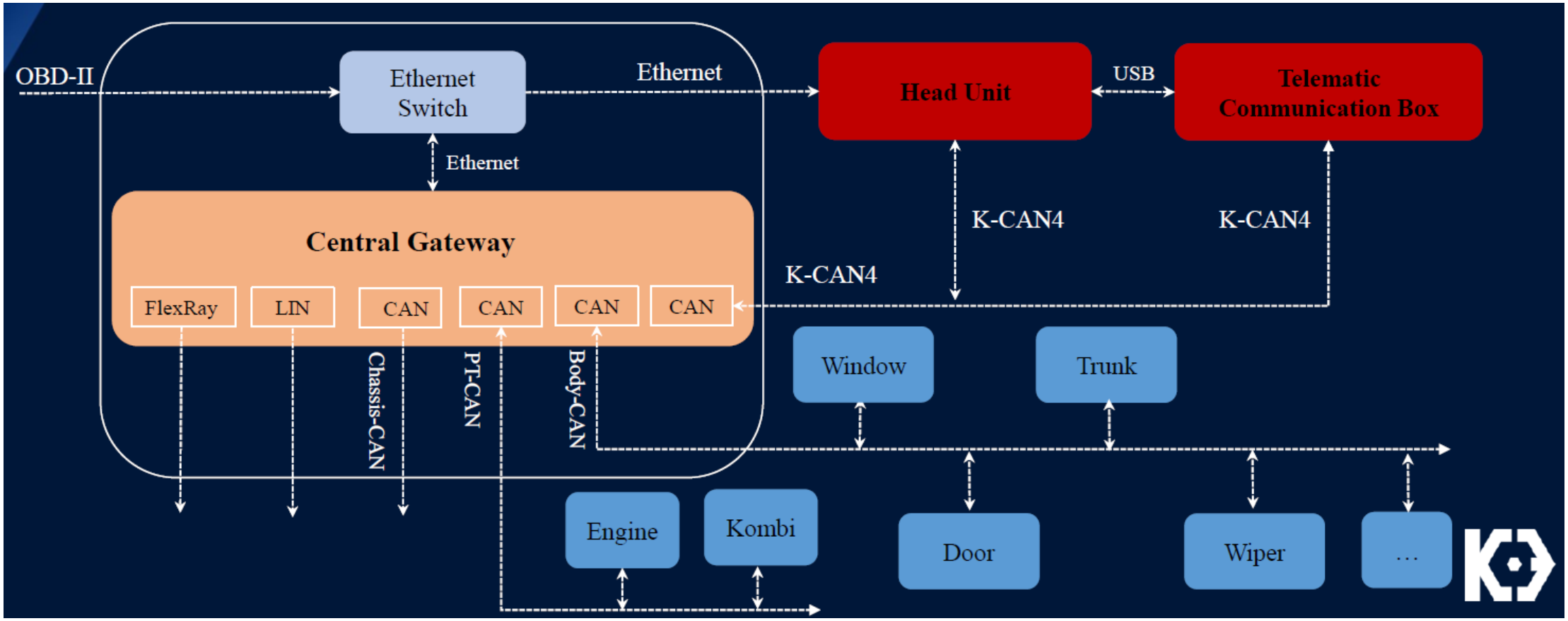


2019 Keenlabs

- Blackhat 2019
- 14 CVEs, some remote
- BMW head unit, gateway and telematics

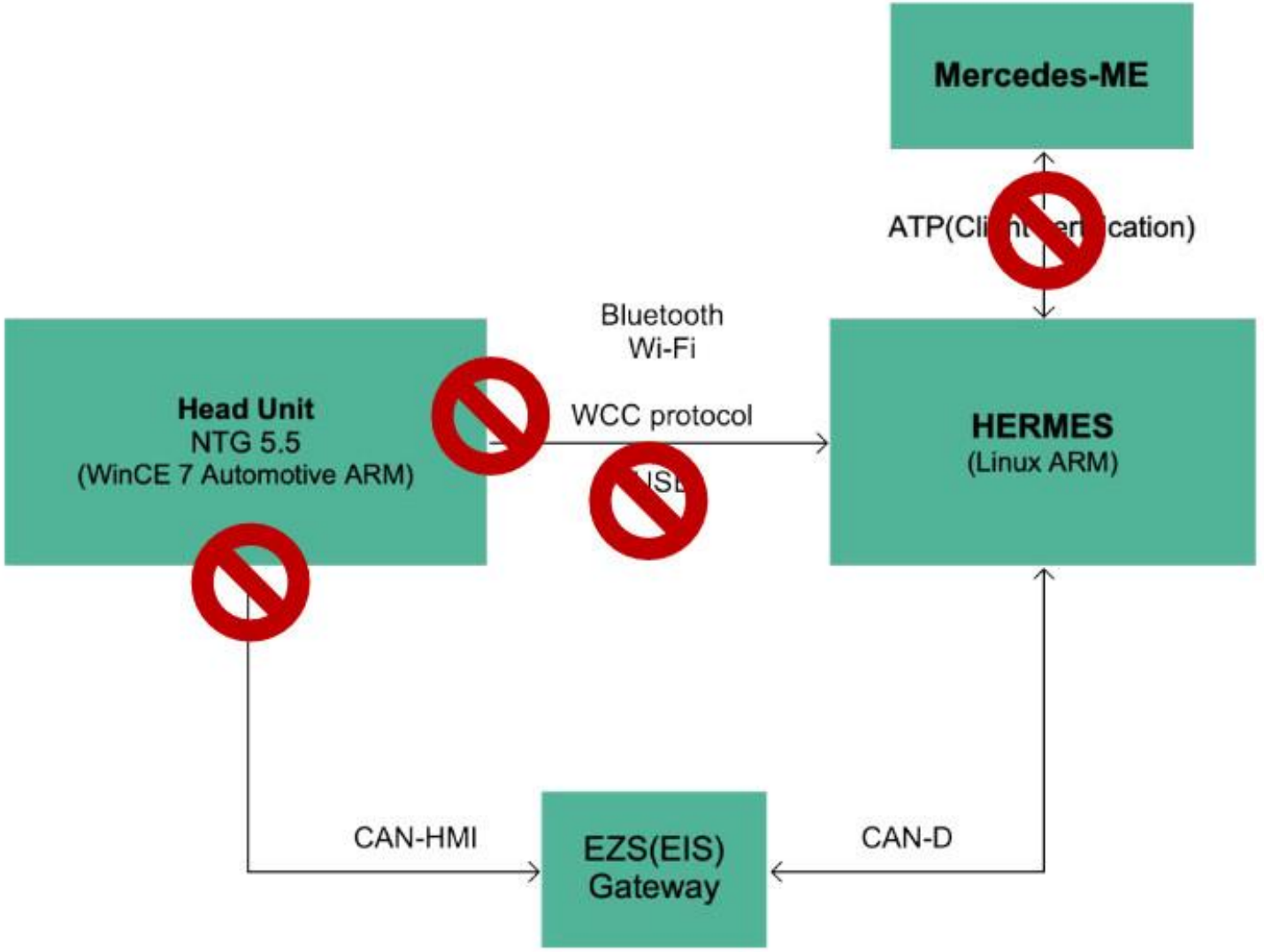
No.	Vulnerability Description	Access	Affected Components	Reference
1	All the detail information has been reserved due to security concerns.	Local (USB)	HU_NBT	CVE-2018-9322
2		Local (USB/OBD)	HU_NBT	
3		Remote	HU_NBT	Logic Issue
4		Remote	HU_NBT	Reserved
5		Local (USB)	HU_NBT	CVE-2018-9320
6		Local (USB)	HU_NBT	CVE-2018-9312
7		Remote (Bluetooth)	HU_NBT	CVE-2018-9313
8		Physical	HU_NBT	CVE-2018-9314
9		Physical	TCB	Reserved
10		Remote	TCB	Logic Issue
11		Remote	TCB	CVE-2018-9311
12		Remote	TCB	CVE-2018-9318
13		Indirect Physical	BDC/ZGW	Logic Issue
14		Indirect Physical	BDC/ZGW	Logic Issue

2019 Keenlabs



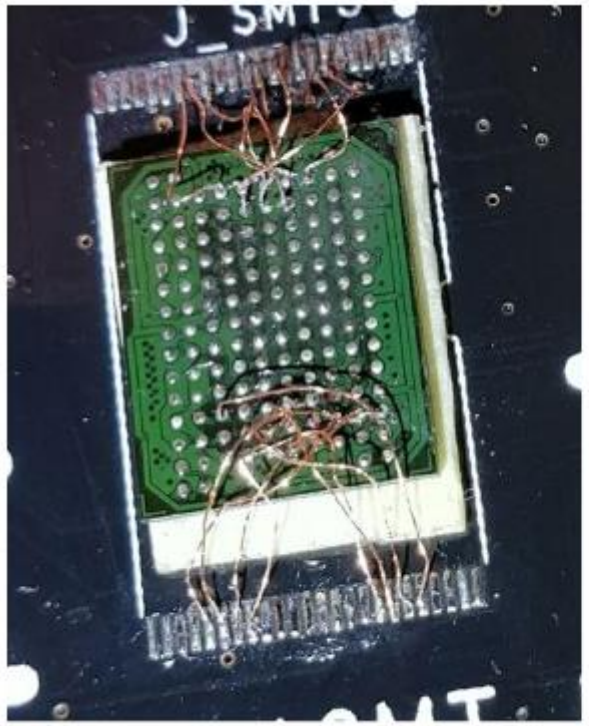
2020 Sky-Go 360 Group

- Blackhat 2020
- Connected Daimler cars
- 2 million cars (in China)
- Didn’t succeed at WinCE 7
- But: jailbreak telematics!
- And connect to backend



2020 Sky-Go 360 Group

- Used all the big tools!
- NAND reading with BGA rework station
- Theft protection reversing
- X-ray for finding JTAG
- Reballing for implanting a backdoor



2021 ea_foundation

2021 ea_foundation

- Rather old Bosch infotainment, 2.6-ish kernel
- Serial ports, u-boot console, read-write access
- Command injection using USB file system name

```
# Determine the name for the mount point.  First check for the
# uuid, then for the label and then for a unique name.
if [ -n "${ID_FS_UUID}" ]; then
    mountdir=${ID_FS_UUID}
elif [ -n "${ID_FS_LABEL}" ]; then
    mountdir=${ID_FS_LABEL}
```

2021 Wouters

ANDY GREENBERG SECURITY 11.23.2020 07:00 AM

This Bluetooth Attack Can Steal a Tesla Model X in Minutes

The company is rolling out a patch today for the vulnerabilities, which allowed one researcher to break into one in 90 seconds and drive away.

The technique takes advantage of a collection of security issues—both major and minor—in the Model X's keyless entry system. PHOTOGRAPH: CHRISTIAN CHARISI IMAGES

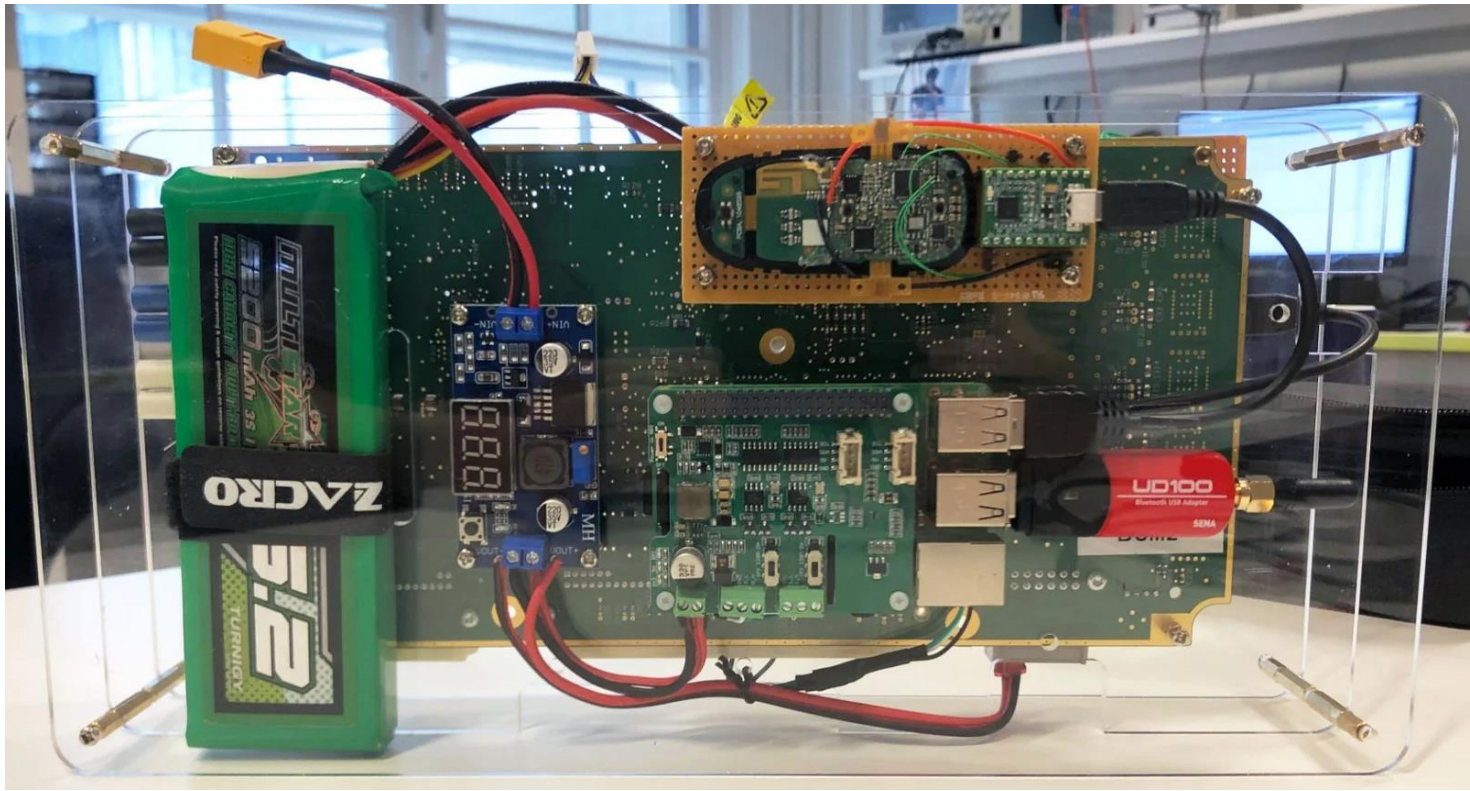
My other car is your car: compromising the Tesla Model X keyless entry system - Lennert Wouters

477 Aufrufe • Premiere am 07.08.2021 17 0 TEILEN SPEICHERN ...

2021 Wouters

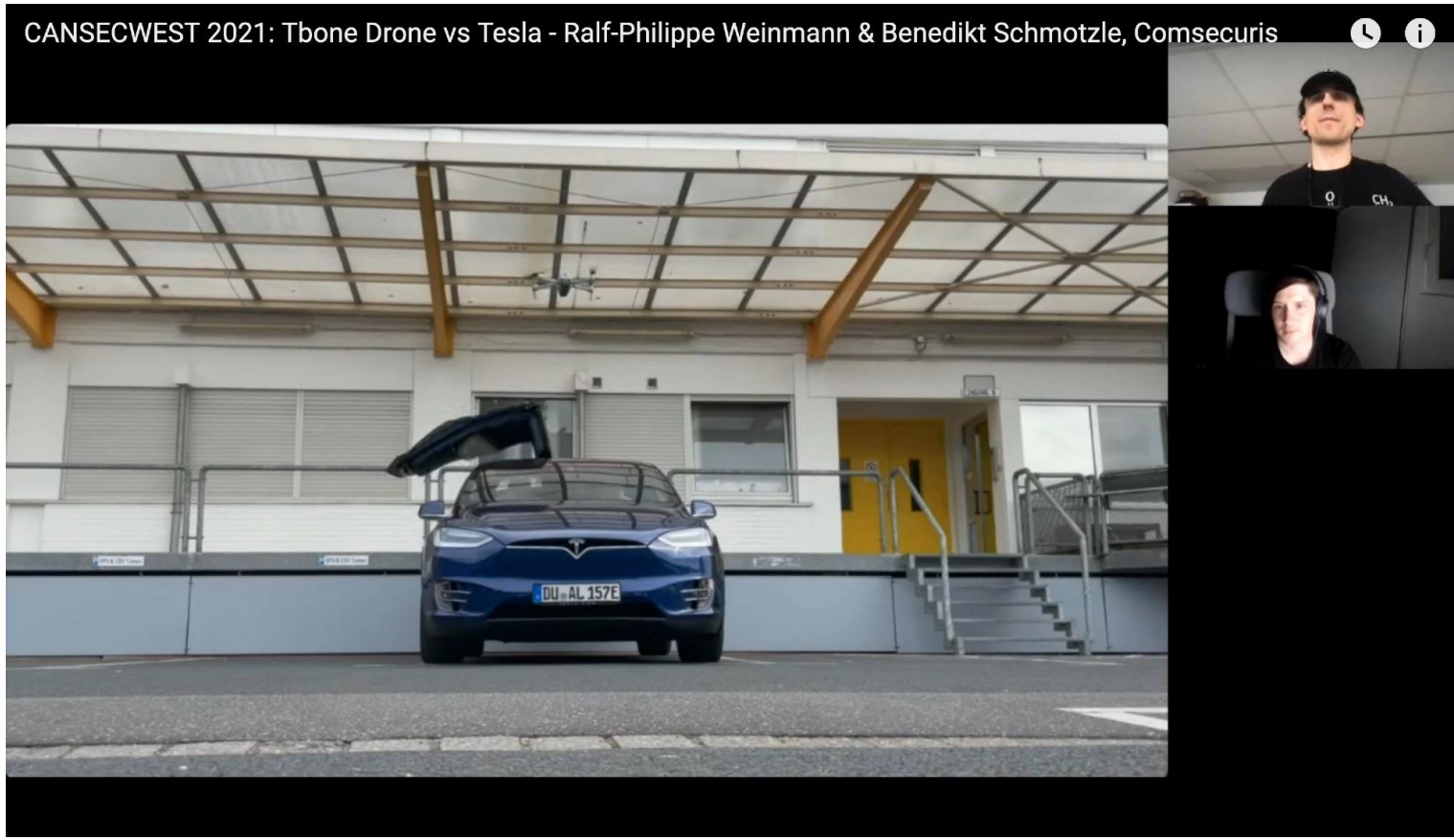
How the attack works:

- Wake up BLE interface of keyfob using VIN
- Flash software update to extract unlock token(s)
- Updated signed, but response ignored
- Attach to body computer
- Train new keyfob



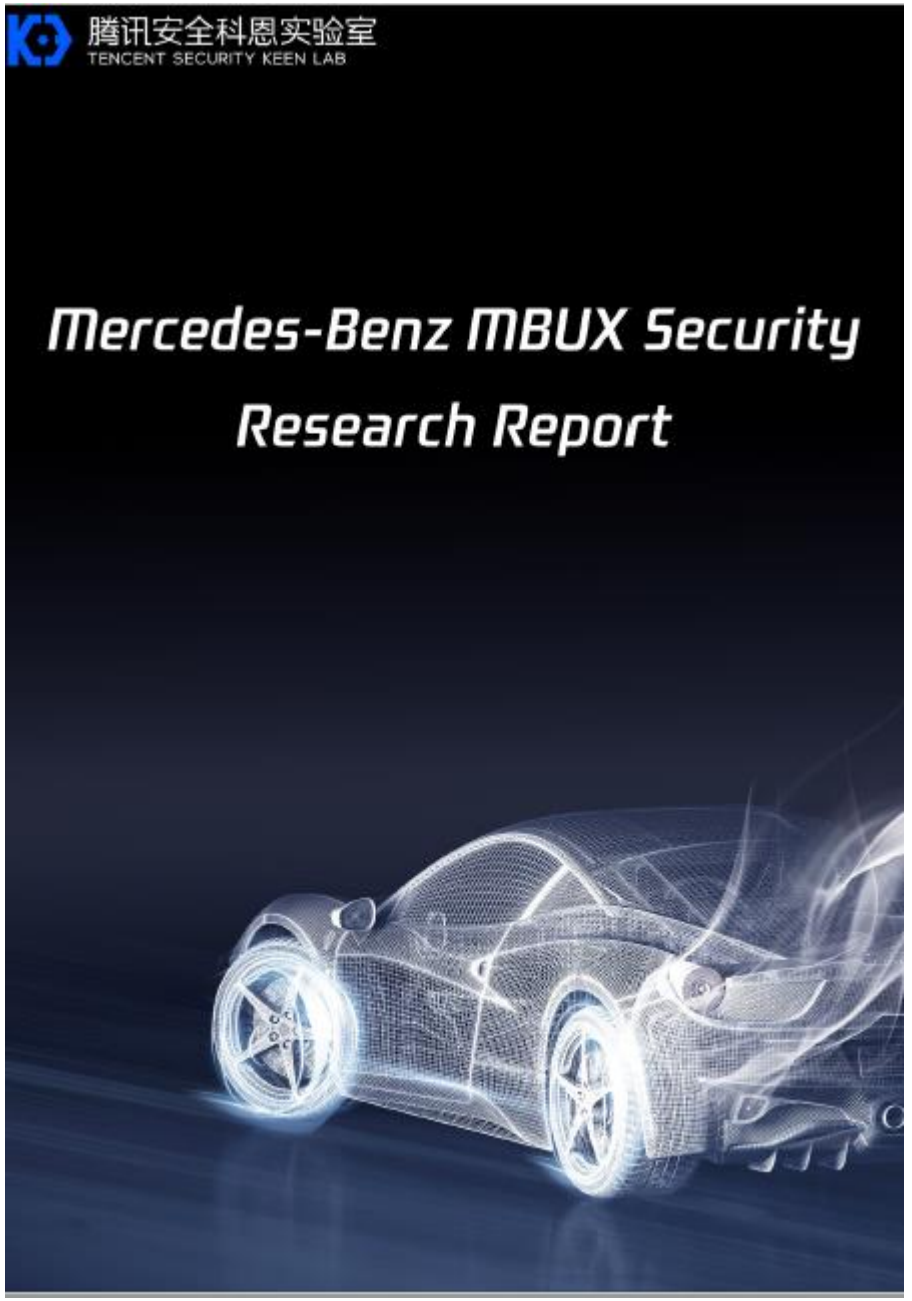
2021 Weinmann/Schmotzle

- Talk at CanSecWest 2021
- *TBONE*, with a drone
- memcpy() stack overflow in ConnMan
- Exploitable over wifi
- Privilege escalation using kernel module?



2021 Keen Labs

- Daimler MBUX headunit
- Headunit and T-box connected
- Private WPA2-encrypted wifi
- Proprietary HiQnet protocol with buffer overflow(s)
- 3.18-ish kernel



2021 Keen Labs

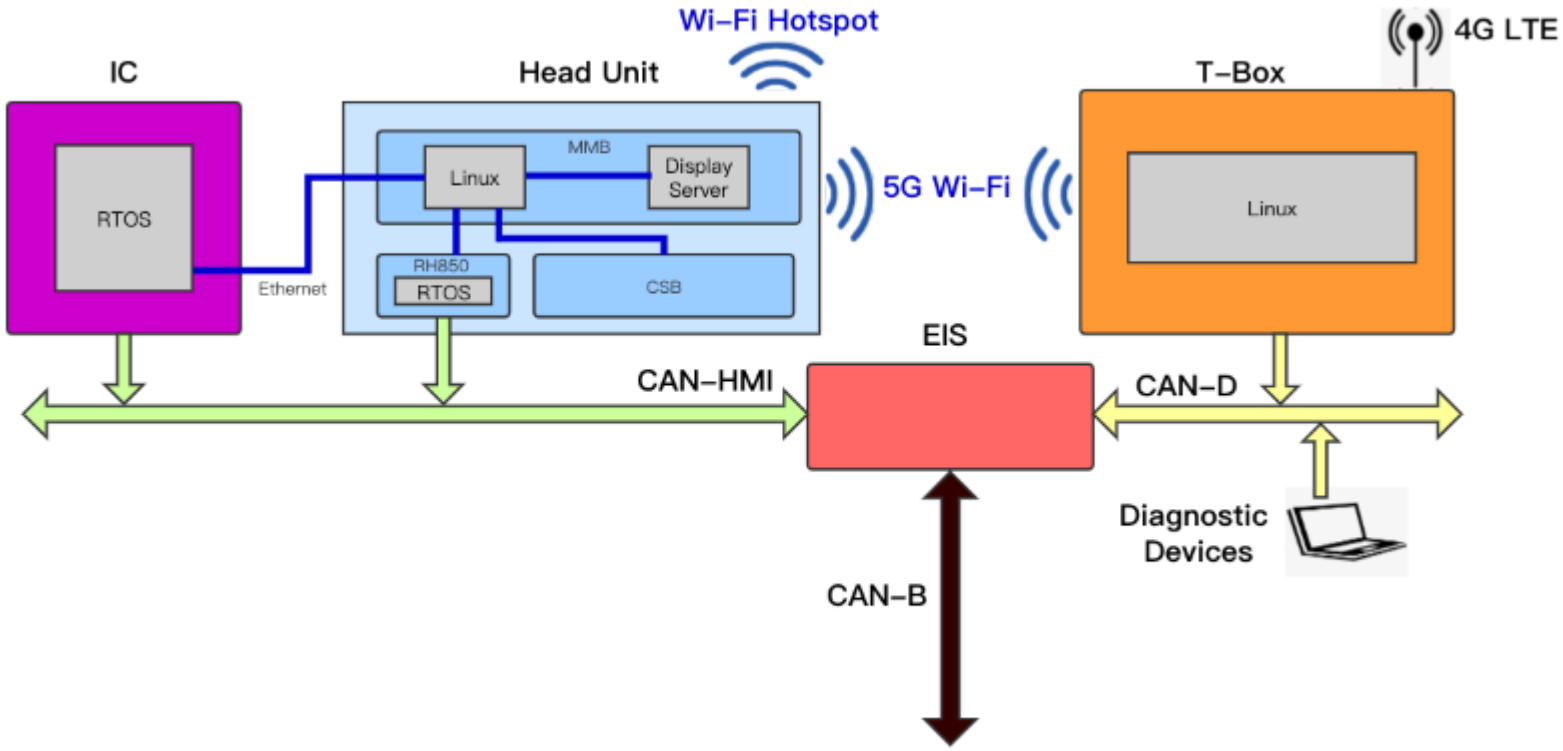
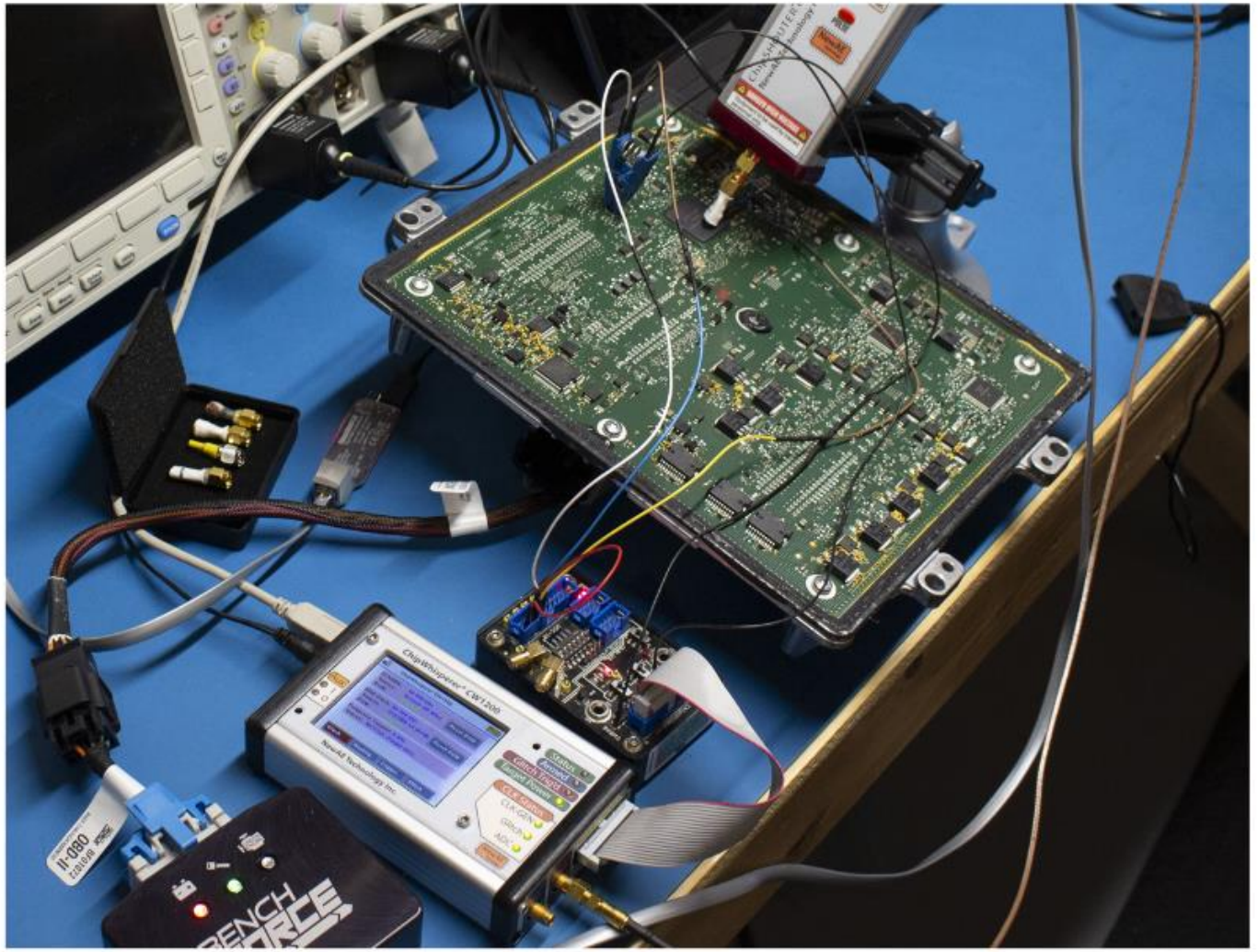


Figure 2.1: Architecture overview

2021 O'Flynn

- Blackhat 2021
- Glitching ECUs to bypass UART password
- Corvette E41 engine controller
- µC was NXP MPC55x



(c) E41 ECU "In-Situ" Target

2022 Melching

- Steering ECU from 2008
- ReadMemoryByAddress
- Update files
- Pipe into Ghidra
- Identify bootloader & flash your customizations

2022 Synactiv

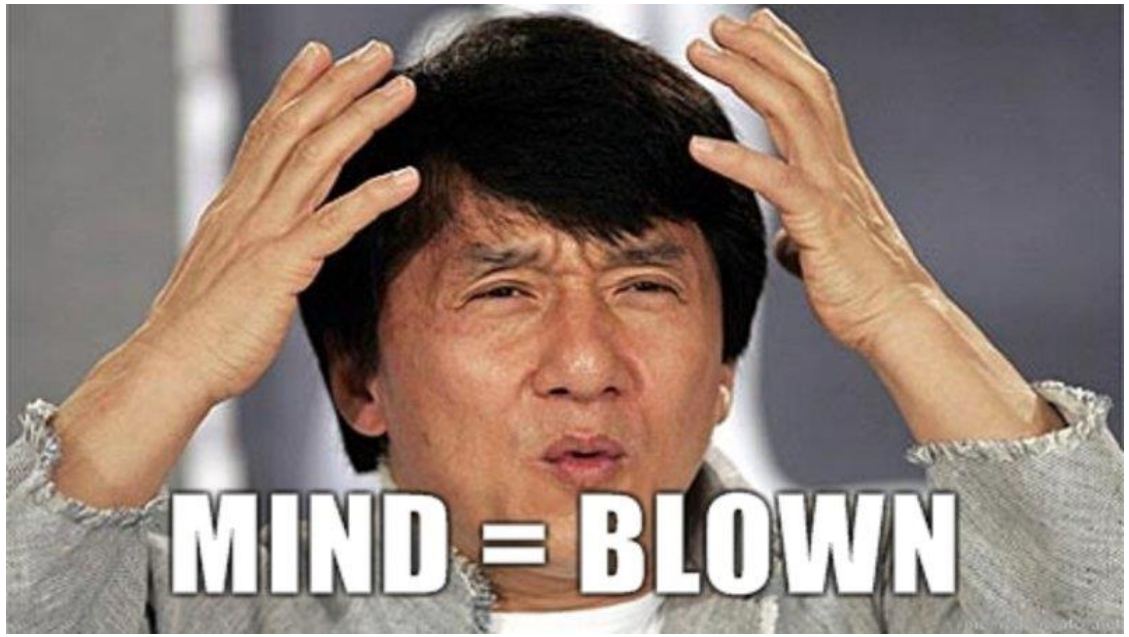
- Pwn2own in May
- 3 vulns, 1 known
- But no writeup yet
- Talk in October at Hexacon 2022

2022 Argus


black hat
ASIA 2022
ARGUS
CYBER SECURITY
AUTONOMOUS
Backdooring of Real Time
Automotive OS Devices

2022 Argus

- Talk at Blackhat Asia 2022
- Instrument cluster with some Renesas RH850
- Buffer overflow over CAN-FD
- Leak keys, execute shell code
- Make them lights blink



- Hat tip to @we155_n

2022 Herfurt #1

- CanSecWest 2022 BLE relay against Tesla 3
- Wirelessly, over Internet
- Two other groups, about the same time

2022 Herfurt #2

2022 Herfurt #2

- NFC unlock allows phone pairing
- No user notification
- Limited to 130 seconds
- Close proximity required
- Better use pin2drive

FIN

!!! DO NOT HACK CARS, YOU MIGHT HURT YOURSELF, OR OTHERS !!!

How to keep informed?

- Twitter, obviously
- Car Hacking Village
- Automotive security research group (ASRG.io)