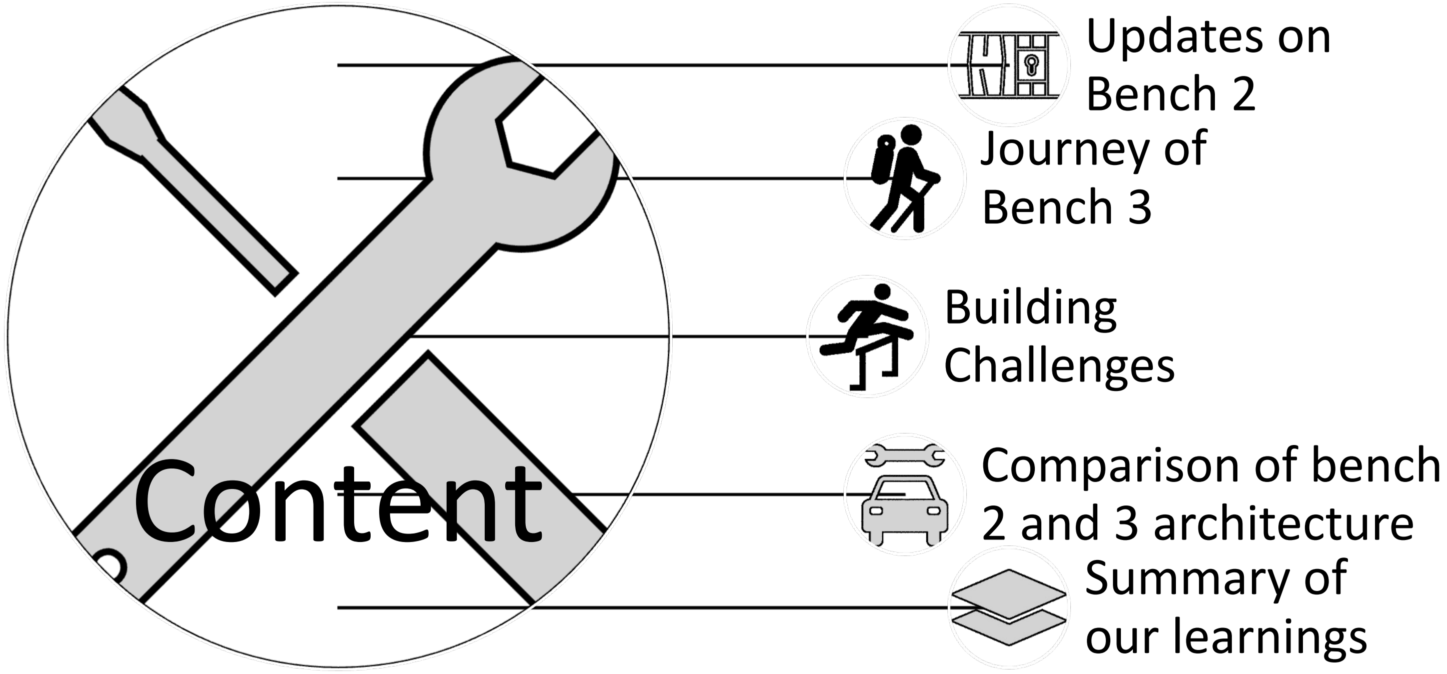
Analysis of an In-vehicular network: CAN bus to infotainment

ROOTCON 17 2023

Content



- Updates on Bench 2
- Journey of Bench 3
- Building Challenges
- Comparison of bench 2 and 3 architecture
- Summary of our learnings

$whoami

- **Alina (@0x410x54)**

Founder – CSQ

Interest – Car racing, Pen testing OT and Automotive Systems

- **Pei Si (@kaskrex)**

Pioneer Member – CSQ

Interest – DFIR, Hardware Hacking, DevSecOps

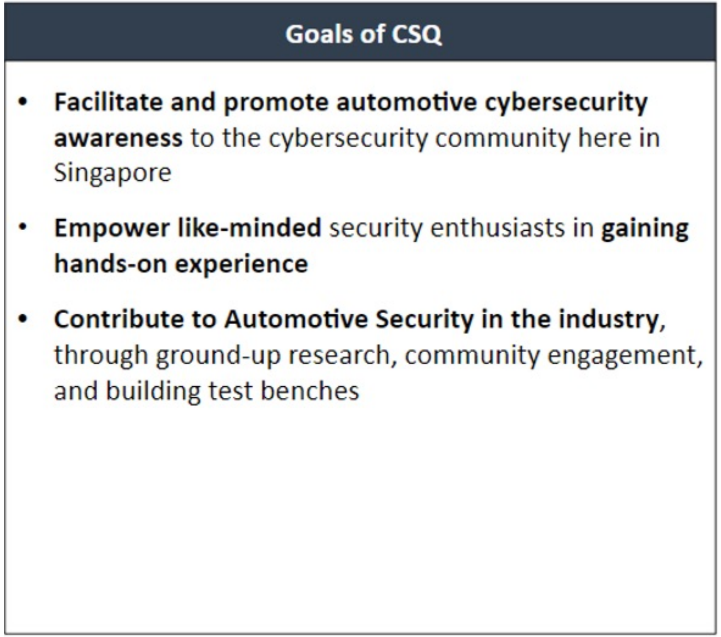
CAR SECURITY QUARTER

01011001 01100101 01110011 00100000 01010111 01100101 00100000 01000011 01000001 01001110 00100001

@CSQDiv0

- Total Members: 20+
- Part of a wider cybersecurity community – Division Zero (Div0)
- Powers Automotive Security Research Group, Singapore (ASRG-SIN)

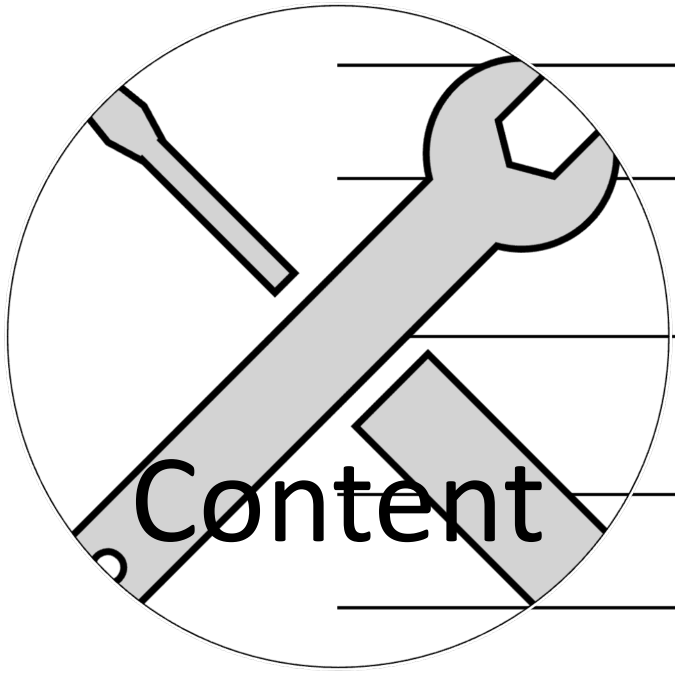
Goals of the Car Security Quarter (CSQ)



Goals of CSQ

- **Facilitate and promote automotive cybersecurity awareness** to the cybersecurity community here in Singapore
- **Empower like-minded** security enthusiasts in **gaining hands-on experience**
- **Contribute to Automotive Security in the industry**, through ground-up research, community engagement, and building test benches

Content



Updates on Bench 2

Journey of Bench 3

Building Challenges

Comparison of bench 2 and 3 architecture

Summary of our learnings

A quick recap on Bench 2

- We chose to build test bench 2 with the following critical components to build upon: Central Gateway module, Infotainment Unit, and Telematics
- We improvised and added a few more items – Cluster Meter and DDE
- The bench contains 3 different layers to simulate the vehicle's architecture

1

Layer 1

2

Layer 2

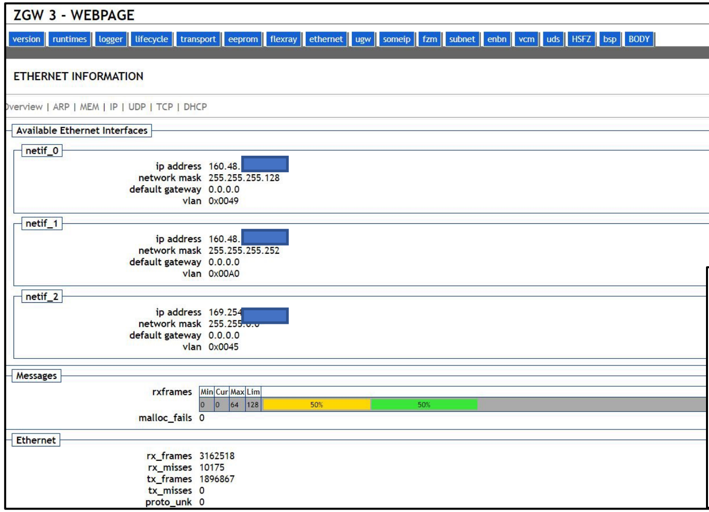
3

Layer 3

Updates on Bench 2

- We were able to connect to the central gateway module (ZGW) and **identified that it uses a combination of Ethernet and CAN bus**. We were also able to locate the **internal IP addresses** (160.48.XX.XX and 160.48.XX.XX) **through the webpage of the gateway (port 80)** and **validated that the ZGW communicates with the internal server periodically**.

- Through our testing observations, the **vehicle will log our IP address once we are connected to it**. The web page has quite **a few interesting tabs such as testing of Diagnostics functionality**.



ZGW 3 - WEBPAGE

[redacted]

ETHERNET INFORMATION

Available Ethernet Interfaces

netif_0

```
     ip address  160.48.[redacted]
   network mask  255.255.255.128
default gateway  0.0.0.0
           vlan  0x0049
```

netif_1

```
     ip address  160.48.[redacted]
   network mask  255.255.255.252
default gateway  0.0.0.0
           vlan  0x00A0
```

netif_2

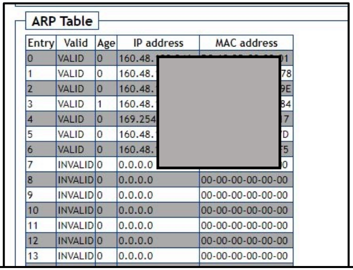
```
     ip address  169.254[redacted]
   network mask  255.255[redacted]
default gateway  0.0.0.0
           vlan  0x0045
```

Messages

```
   rxframes  Min Cur Max Lim
             0   0   64  128   50%   50%
malloc_fails 0
```

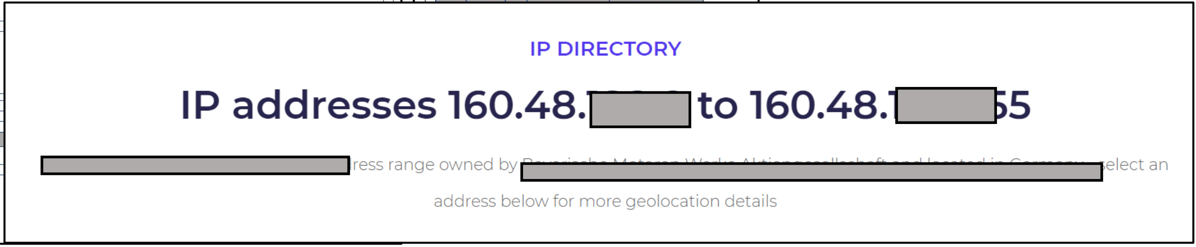
Ethernet

```
 rx_frames  3162518
 rx_misses  10175
 tx_frames  1896867
 tx_misses  0
 proto_unk  0
```



ARP Table

Entry	Valid	Age	IP address	MAC address
0	VALID	0	160.48.[redacted]	[redacted]
1	VALID	0	160.48.[redacted]	[redacted]
2	VALID	0	160.48.[redacted]	[redacted]
3	VALID	1	160.48.[redacted]	[redacted]
4	VALID	0	169.254[redacted]	[redacted]
5	VALID	0	160.48.[redacted]	[redacted]
6	VALID	0	160.48.[redacted]	[redacted]
7	INVALID	0	0.0.0.0	[redacted]
8	INVALID	0	0.0.0.0	00-00-00-00-00-00
9	INVALID	0	0.0.0.0	00-00-00-00-00-00
10	INVALID	0	0.0.0.0	00-00-00-00-00-00
11	INVALID	0	0.0.0.0	00-00-00-00-00-00
12	INVALID	0	0.0.0.0	00-00-00-00-00-00
13	INVALID	0	0.0.0.0	00-00-00-00-00-00

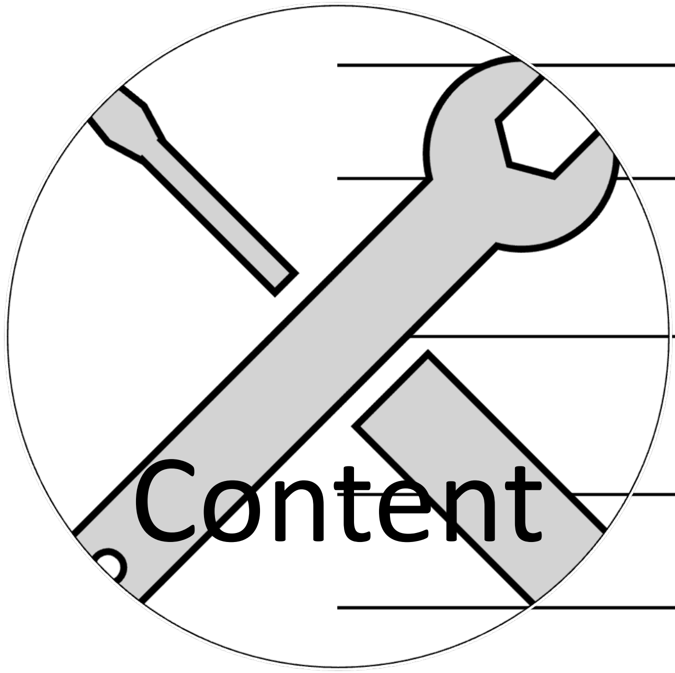


IP DIRECTORY

IP addresses 160.48.[redacted] to 160.48.[redacted]55

[redacted]ress range owned by [redacted]elect an address below for more geolocation details

Content



Updates on Bench 2

Journey of Bench 3

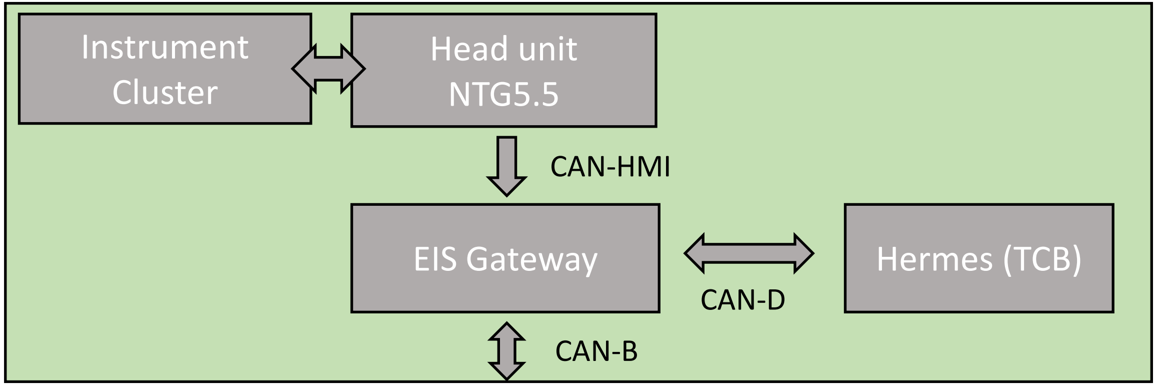
Building Challenges

Comparison of bench 2 and 3 architecture

Summary of our learnings

Journey of Bench 3 – Inspirations

- Test bench 3 was inspired by 360 Group findings announced in RSA/Black Hat U.S.A 2020.
- As we do not have the budget and it is dangerous to perform security testing on actual vehicles, we chose to build a test bench to simulate the attacks
- Bench 3 was completed in Nov 2020
- Since there were already known findings, we wanted to utilize the existing research to enhance our learnings
- Similar to test bench 2, the central gateway (EIS Gateway) contains most of the CAN protocols: CAN-HMI (infotainment CAN bus), CAN-D (Diagnostics CAN bus), CAN B (Body CAN Bus)



Source: https://skygo.360.cn/archive/Security-Research-Report-on-Mercedes-Benz-Cars-en.pdf

Component introductions (1)

Instrument Cluster

The instrument cluster displays the speedometer and infotainment screen together. It also allows wifi connectivity and is connected to the infotainment system.

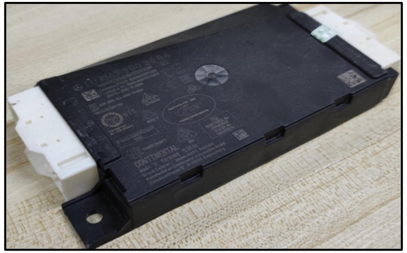
Infotainment System

The infotainment system (NTG5.5) contains the RTOS ECU to power up the infotainment in the vehicle. It is running on WinCE 7 Automotive ARM OS.

Component introductions (2)

Telematics (TCU)

The telematics module (HERMES) provides LTE network connectivity to your cell phone and provides the infotainment with internet connectivity



EIS (Electronic Ignition Switch) Gateway

Acts as the firewall to filter CAN messages and supports keyless functions

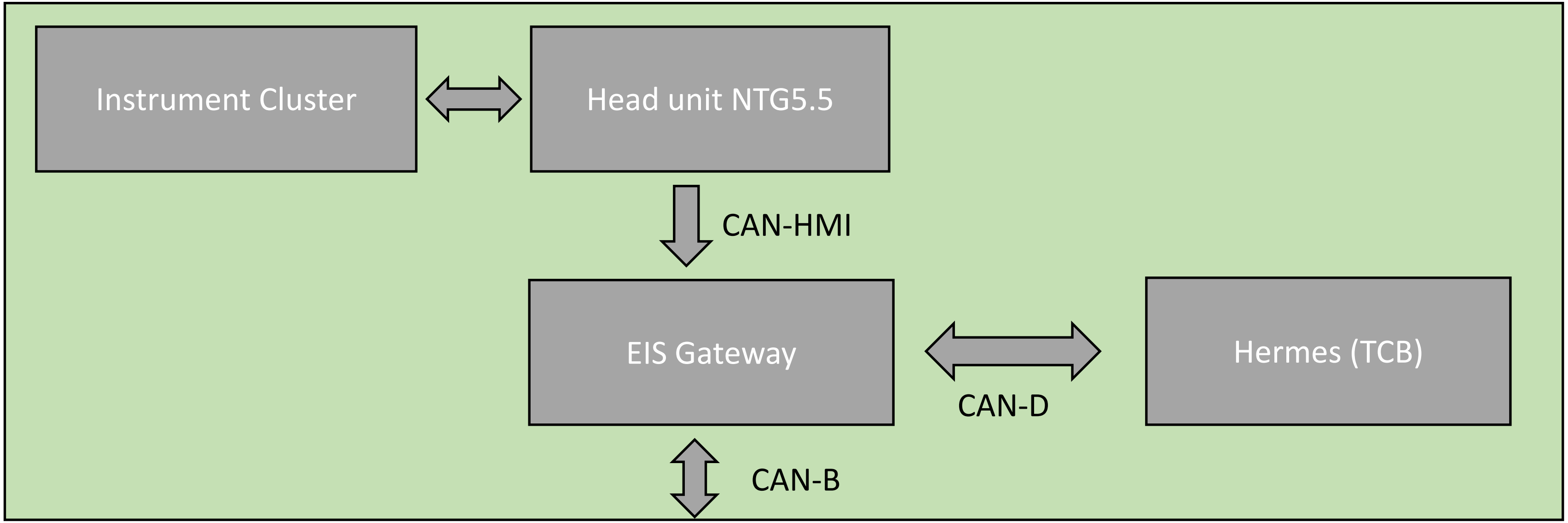
USB hub

Provides connectivity for external USB devices and also installation of GPS Maps

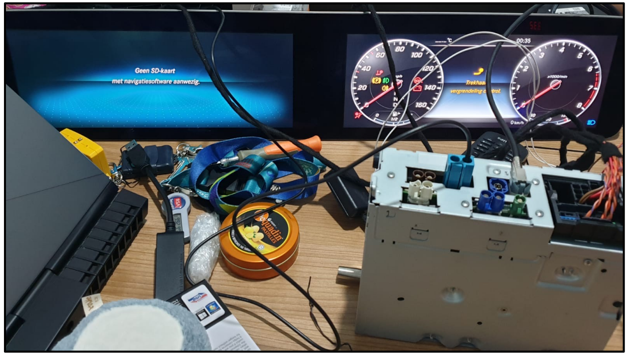
Source: https://keenlab.tencent.com/en/whitepapers/Mercedes_Benz_Security_Research_Report_Final.pdf

Bench 3 vehicular protocol introductions

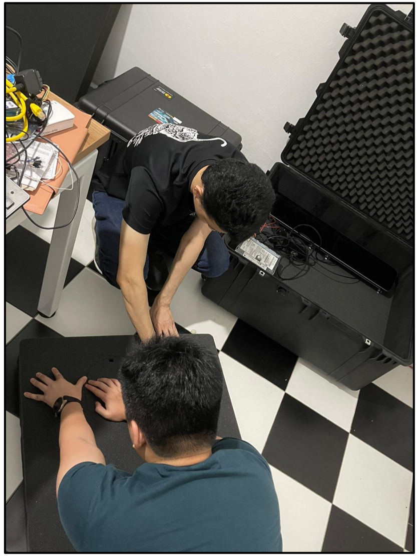
- There are different protocols within the vehicle's central gateway (EIS)
- There are also different variations of CAN bus that controls different functions within the vehicle:
- **CAN-B:** interior can bus that connects to climate control etc.
- **CAN-D**: diagnostics CAN bus that has connectivity to OBD-II etc.
- **CAN-HMI**: Infotainment CAN bus that displays information to the cluster meter etc.



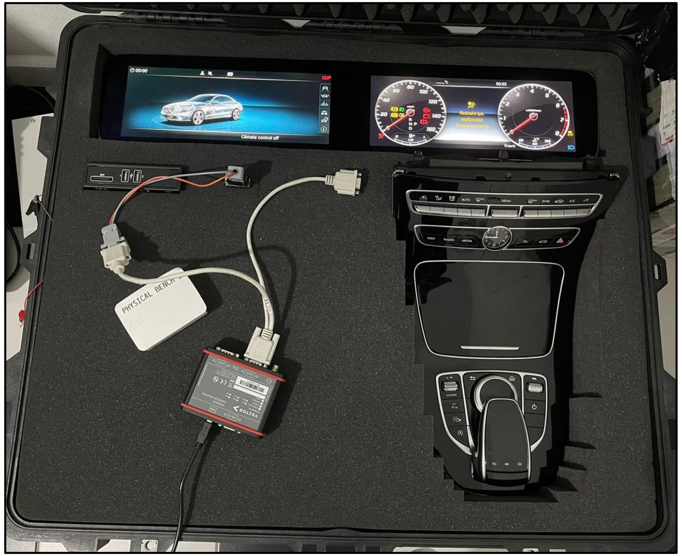
Process of assembling Bench 3



Bench 3 Raw

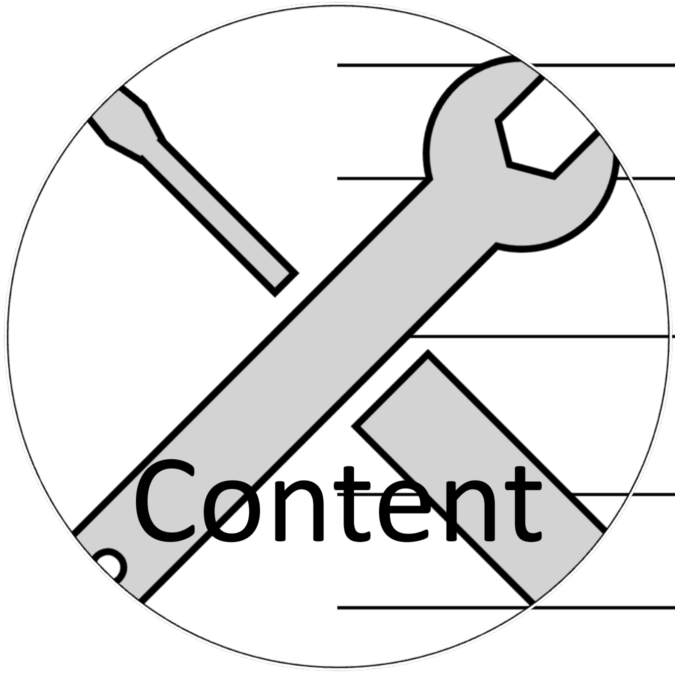


Assembly process



Bench 3

Content



Updates on Bench 2

Journey of Bench 3

Building Challenges

Comparison of bench 2 and 3 architecture

Summary of our learnings

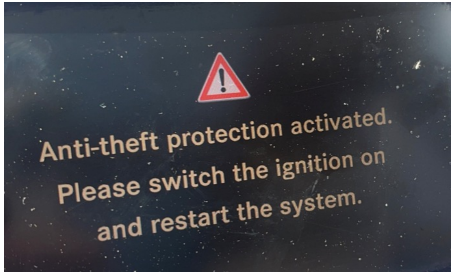
CAN Bus wake up signal

- Similar to bench 2, we had to simulate the CAN bus wake up signals in order to power on the test bench
- The following was retrieved from the vehicle to simulate the CAN bus wake up signal:

CAN Messages	CAN Wake up signals
0x25E	64 64 64 00 03 00 00 00
0x2F7	C2 50 10 57 12 5D 5F 53
0x020	39 C9 41 1C C0 00 00 C0

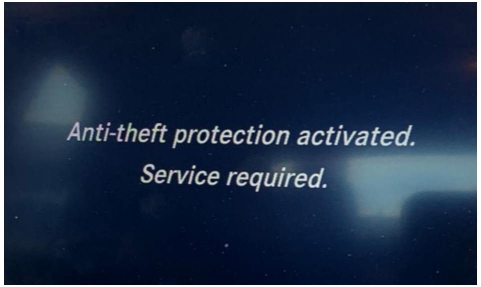
Anti-theft challenges

- Apart from can bus wake up signals, we also had anti-theft challenges
- There are three levels of anti-theft in the head unit: Level A, Level B, Level C
- However, we were lucky that the anti theft messages that we got were level A, so it was easy to fix
- Level A involves turning on and off the ignition to remove the anti-theft messages
- Level B requires developer’s assistance to remove it due to a VIN mismatch
- Level C requires developer’s assistance to remove it (this can be activated if we replayed CAN messages)



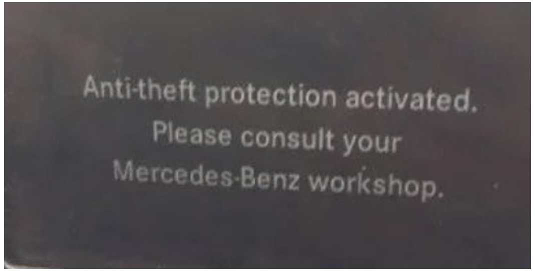
Anti-theft protection activated.
Please switch the ignition on
and restart the system.

Level A



Anti-theft protection activated.
Service required.

Level B



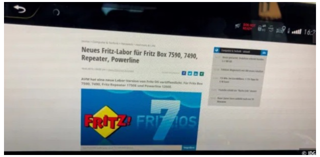
Anti-theft protection activated.
Please consult your
Mercedes-Benz workshop.

Level C

Identify the attack chain through the test bench

Activities

1 Infotainment Browser



Neues Fritz-Labor für Fritz Box 7590, 7490, Repeater, Powerline

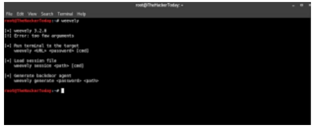
AVM hat eine neue Labor-Version von Fritz OS veröffentlicht. Für Fritz Box 7590, 7490, Fritz Repeater 1750E und Powerline 1260E.

- Attack vector through infotainment browser

2 Infotainment

- Achieve RCE through browser vulnerability to compromise the infotainment system

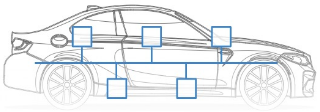
3 Planting backdoor in infotainment system



```
root@TheHackerToday:~# weevely

[+] weevely 3.2.0
[!] Error: too few arguments

[+] Run terminal to the target
    weevely <URL> <password> [cmd]

[+] Load session file
    weevely session <path> [cmd]

[+] Generate backdoor agent
    weevely generate <password> <path>

root@TheHackerToday:~# 
```

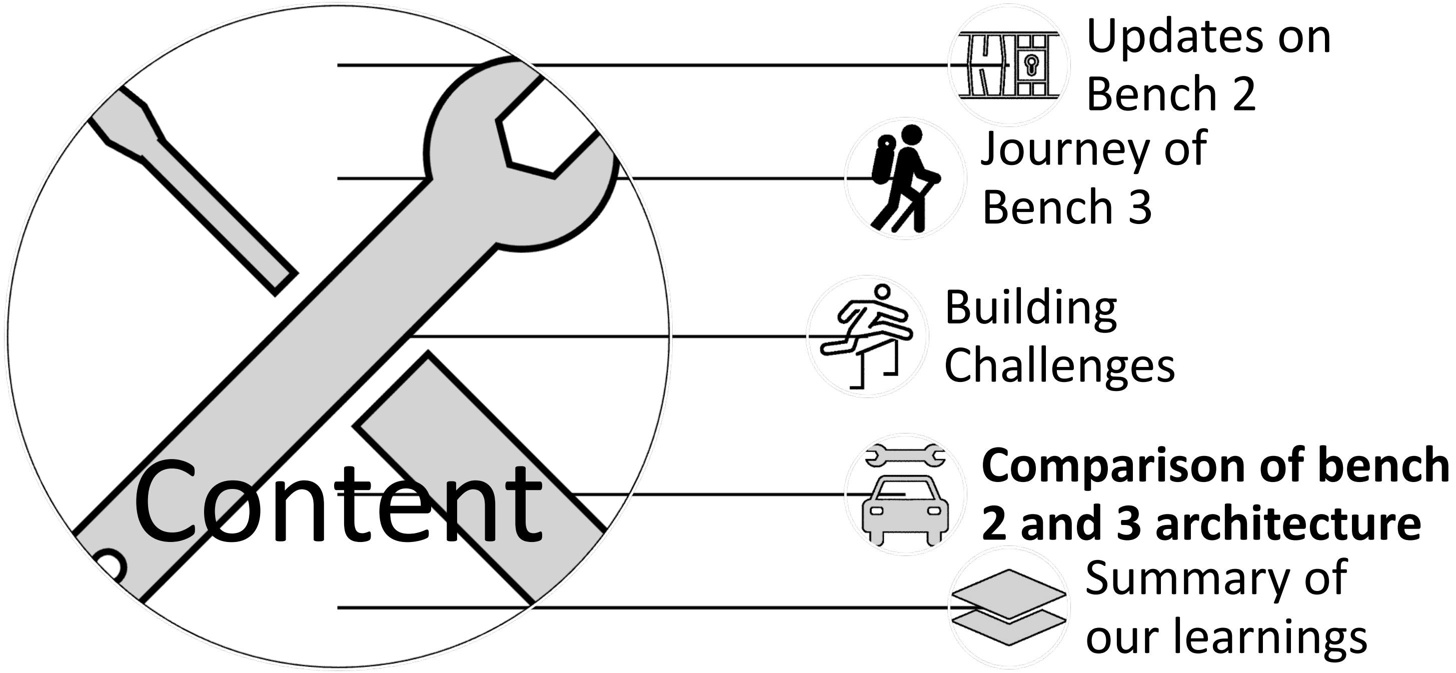
- Plant backdoor in infotainment system for future testing

4 CAN Bus Network



- Perform lateral movement towards controlling vehicular components

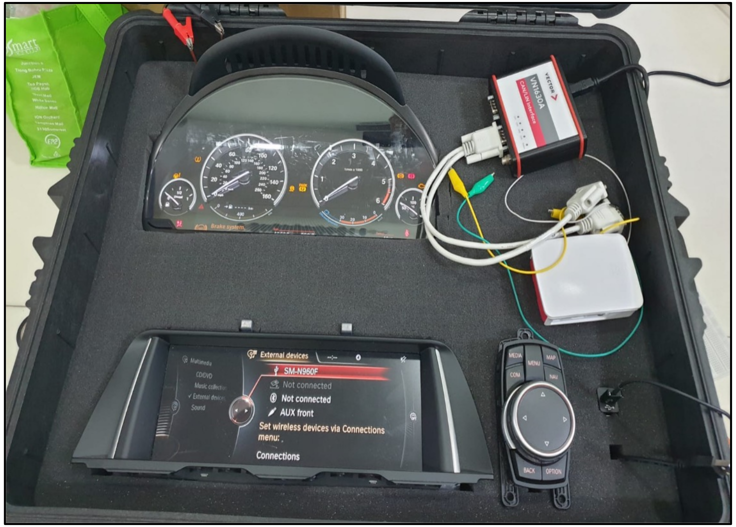
Content



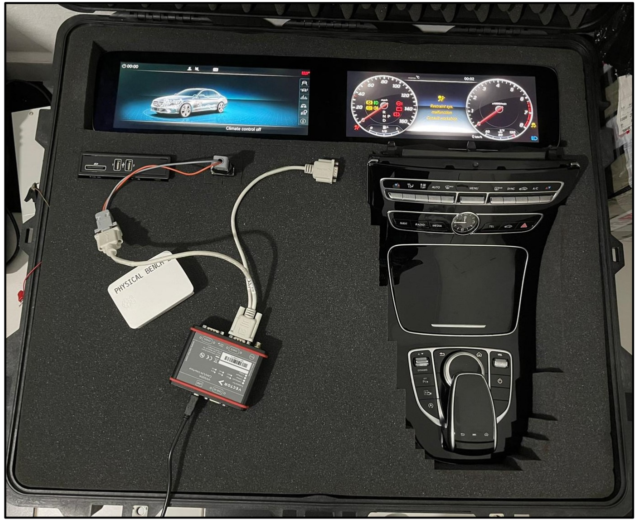
Content

- Updates on Bench 2
- Journey of Bench 3
- Building Challenges
- **Comparison of bench 2 and 3 architecture**
- Summary of our learnings

Physical Comparison of Bench 2 and 3



CSQ Bench 2



CSQ Bench 3

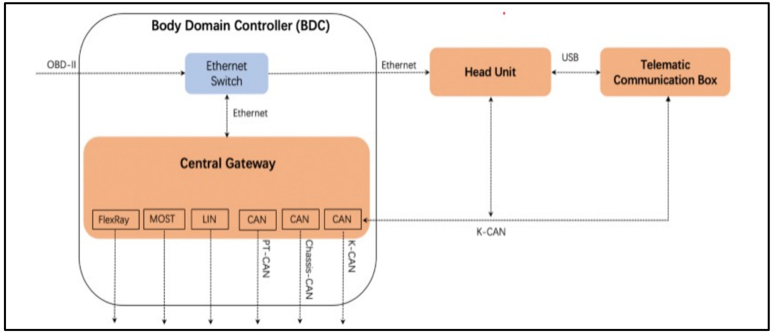
Baseline on Bench 2 and 3 vehicle architectures (1)

Observations

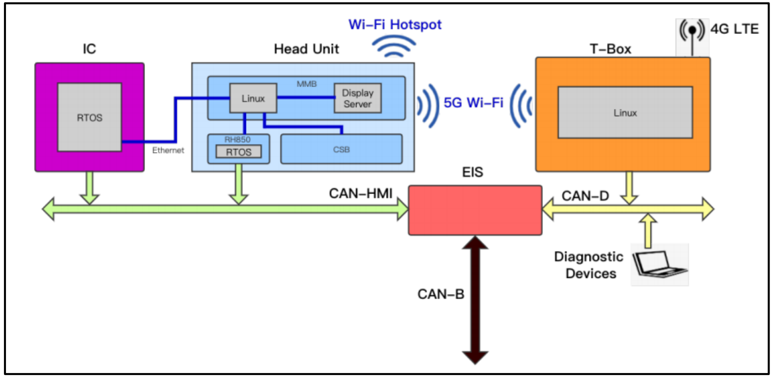
1) Through hands-on research on these two test benches, it is evident that both vehicles have the following components:

a) **Central Gateway (ZGW) Bench 2 / EIS Gateway Bench 3** (**connects various CAN bus connections** to the vehicle (i.e. Diagnostics, Powertrain, Head Unit CAN bus etc.)

b) **Head Unit** running on both WiFi and **have the capability to perform OTA** (Bench 2/Bench 3)



There are no stark architectural differences in these vehicles, except for the naming conventions, and technology used



Source: https://keenlab.tencent.com/en/whitepapers/Mercedes_Benz_Security_Research_Report_Final.pdf

Baseline on Bench 2 and 3 vehicle architectures (2)

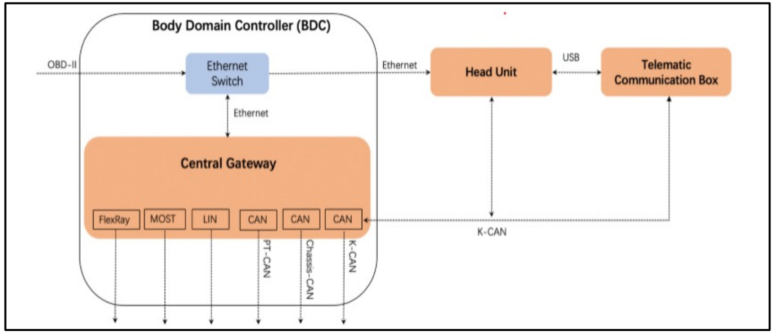
Observations

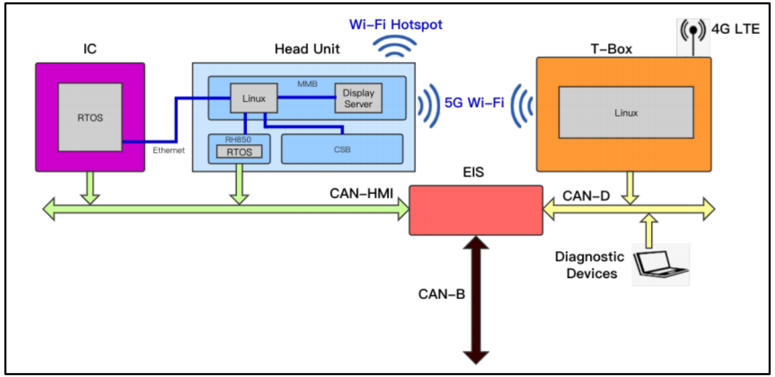
c) **Telematics Communication Box (Bench 2**)/T-Box (Hermes) [Bench 3] that **connects to the head unit which enables 4G LTE connection**

d) **d. Ethernet Switch** (Bench 2)/ **Ethernet** (Bench 3) that **connects the head unit to the instrument cluster**

e) **e. CAN-bus messages filtration** is done at **the central/EIS gateway**

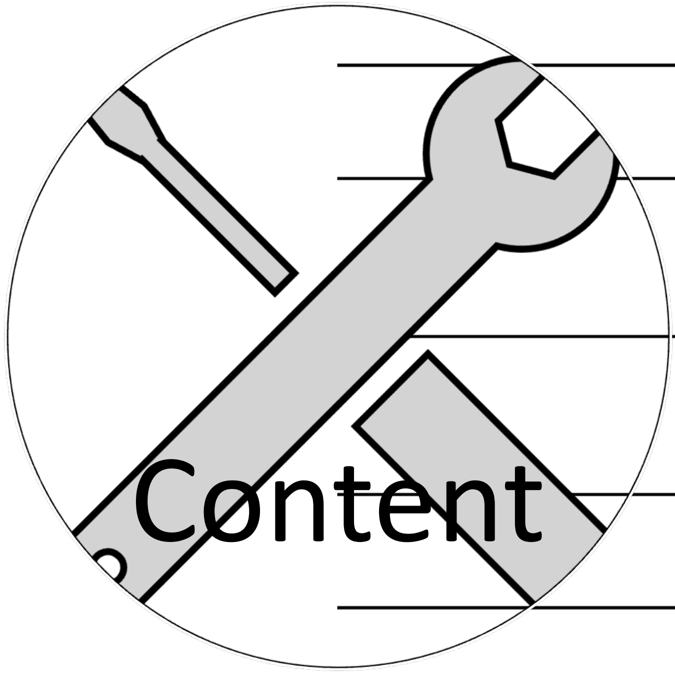
There are no stark architectural differences in these vehicles, except for the naming conventions, and technology used





Source: https://keenlab.tencent.com/en/whitepapers/Mercedes_Benz_Security_Research_Report_Final.pdf

Content



Content

- Updates on Bench 2
- Journey of Bench 3
- Building Challenges
- Comparison of bench 2 and 3 architecture
- **Summary of our learnings**

Bench 3 – Learnings and Challenges (1)

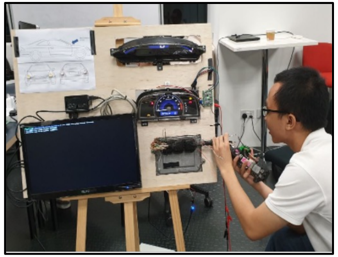
- Through bench 2, it was evident that there are no message signing properties to prevent attacks on the CAN bus such as masquerading as another ECU to send CAN messages
- However, message signing properties are expensive to implement
- with the central gateway, most of the unwanted CAN messages can be filtered away
- In our case with bench 3, for can bus replay attacks, the anti-theft function activates on the infotainment system

Bench 3 – Learnings and Challenges (2)

- Implementation of Anti-theft makes it challenging to build the bench and permanent removal is difficult unless a reflash of a nand chip is done to remove anti-theft – However, this may potentially spoil the board
- Unless root access is gained on the infotainment system and the firmware can be patched – as seen on keen labs research document
- It is important to continuously simulate the ignition signals to remove Level A anti-theft messages

Next Steps

- As we beef up CSQ's continuous efforts to build and understand more Connected Vehicles architectures, we are also in the midst of performing more tests on our ~~three~~ **five** benches!
- Tests can include telematics, Remote attacks, key fob/infotainment/ECU testing, and side channel attacks
- We are also looking into electric vehicles and autonomous vehicles



CSQ Bench 1

CSQ Bench 2

CSQ Bench 3

CSQ Bench 4

CSQ Bench 5

THANK YOU

Questions?