PCAUTOMOTIVE

Top 10 Security Issues in Modern Vehicles

Escar Europe 2023

Danila Parnishchev

Head of Security Assessment, PCAutomotive

info@pcautomotive.com

www.linkedin.com/company/pcautomotive

https://twitter.com/PC_Automotive

Who am I

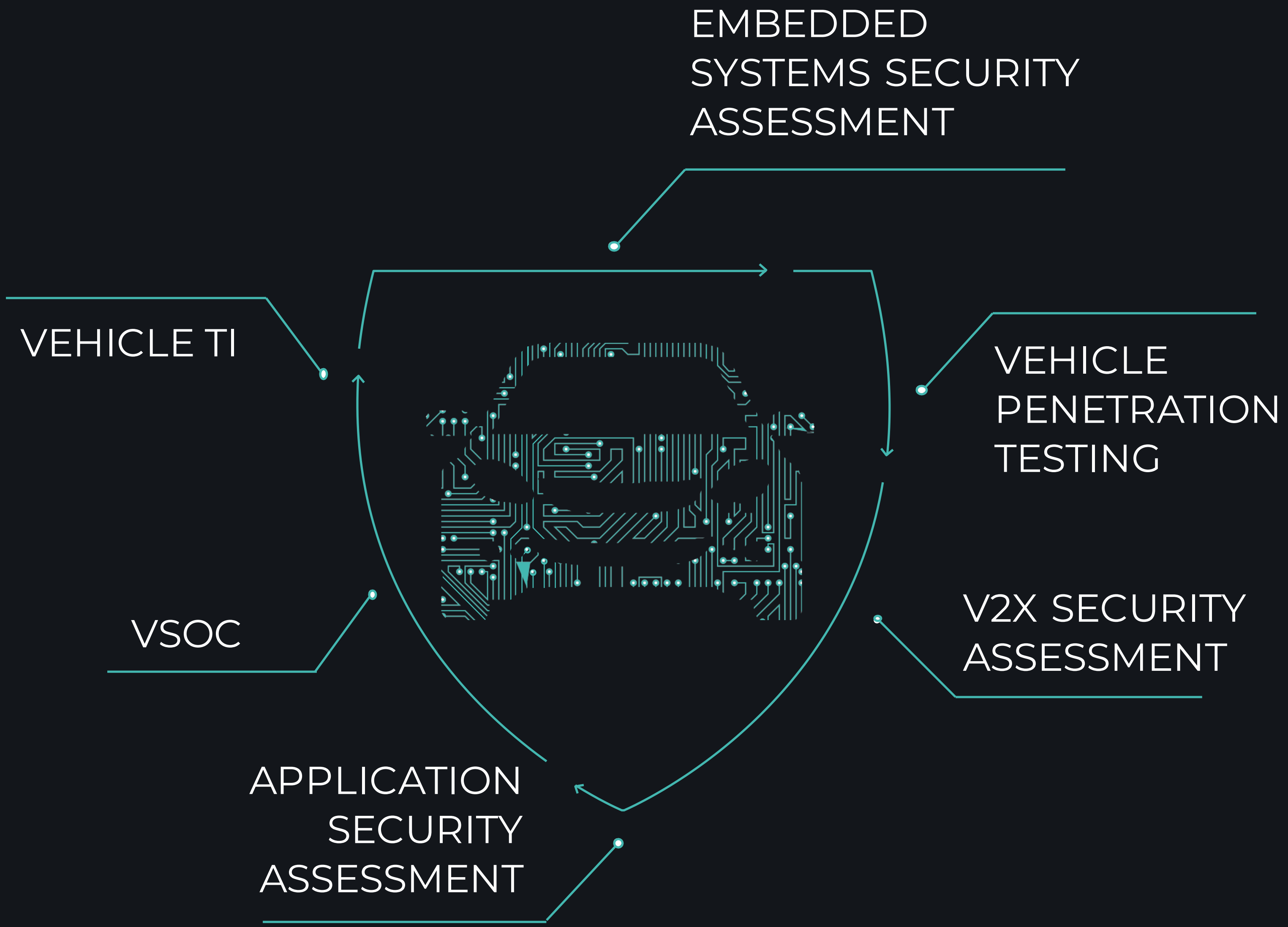
- 8 years in security research
- Favourite targets – embedded devices
  - Network / payment / ICS / transportation

Pwn everything!

Danila Parnishchev

@zero_wf

PCAutomotive – our focus



EMBEDDED SYSTEMS SECURITY ASSESSMENT

VEHICLE TI

VEHICLE PENETRATION TESTING

VSOC

V2X SECURITY ASSESSMENT

APPLICATION SECURITY ASSESSMENT

Automotive lab

Br^{35}eaking Ba^{56}d…

…automotive ECUs

Automotive garage

Fixing…

…security flaws

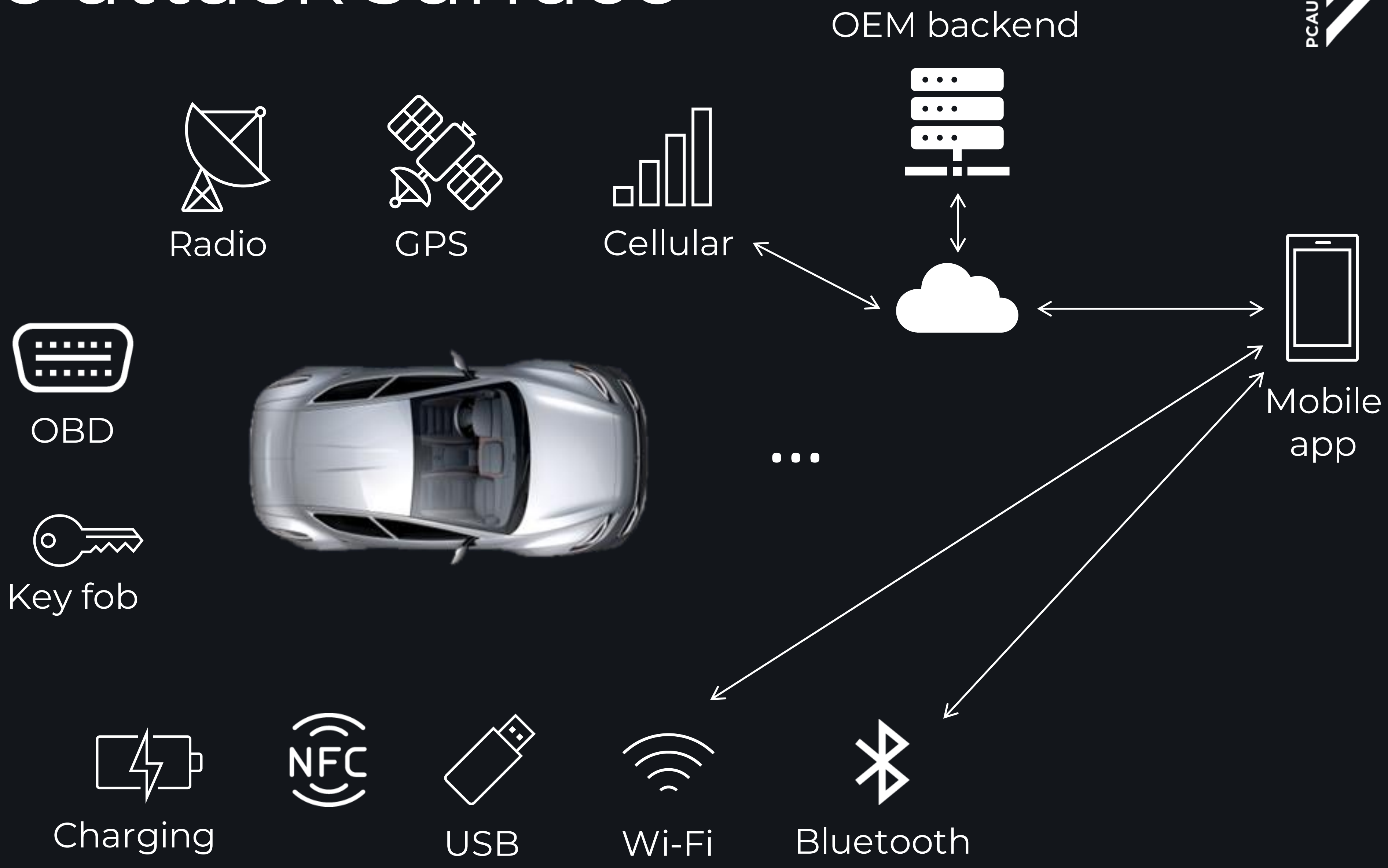
Goal of the talk

- Give practical overview of the 10 issues and the ways of solving them
- Experience is based on
  - 7 full vehicle security analysis done by our specialists from 2018 to 2023
  - Other’s public research & inspiration

1 IVI protocol impl. flaws

Vehicle attack surface

That’s a lot



Attack surface – infotainment

- Infotainment unit brings wireless vectors to the attack surface
- It has control over many peripherals
  - Microphones
  - Main display (HMI)
  - Audio system
  - …
- It’s probably the most attractive entry point for would-be attackers

Bluetooth

Radio

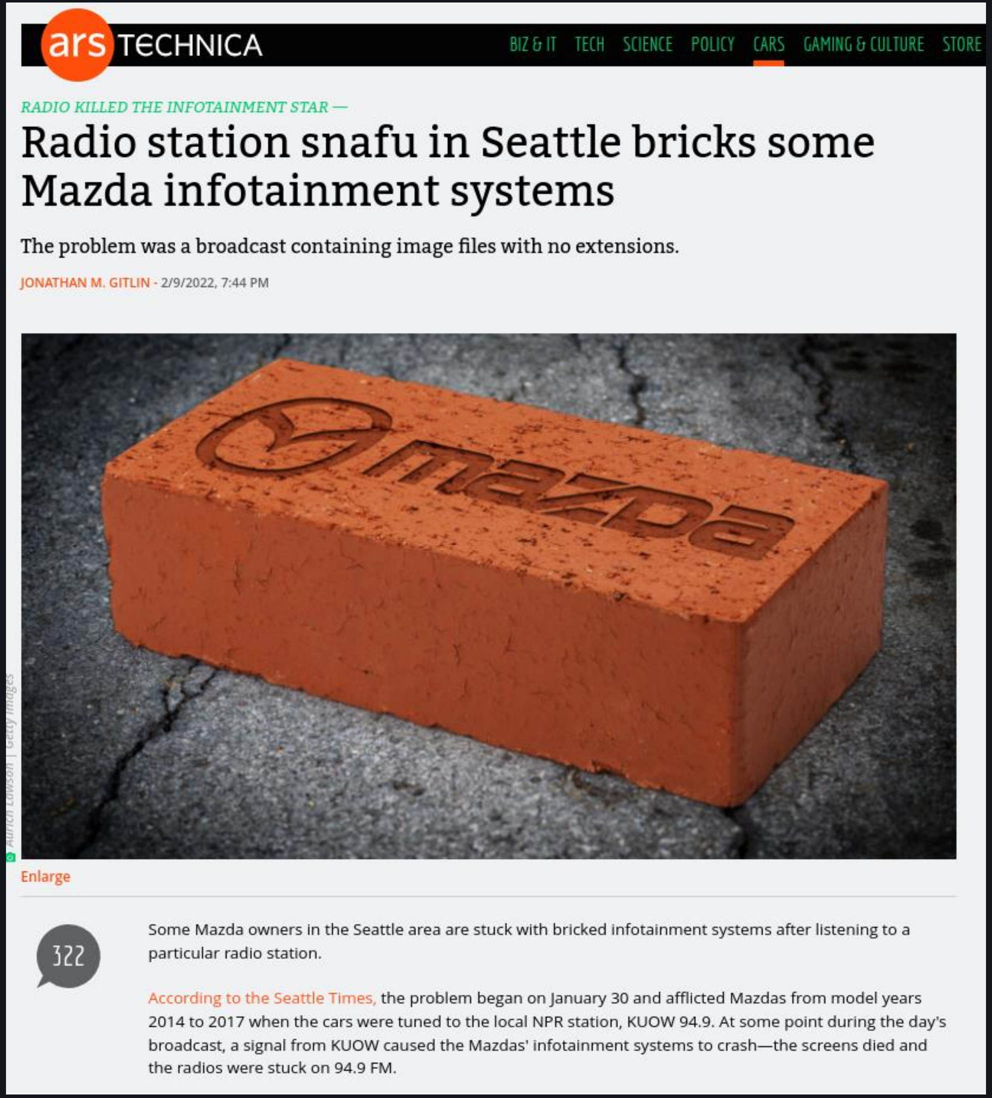
Wi-Fi

USB

Infotainment ECU

Yes, radio is also a vector

- Digital radio sends pictures and text to the car
- Pictures -> parsers ->…
  …vulnerabilities



RADIO KILLED THE INFOTAINMENT STAR —

Radio station snafu in Seattle bricks some Mazda infotainment systems

The problem was a broadcast containing image files with no extensions.

JONATHAN M. GITLIN - 2/9/2022, 7:44 PM

Aurich Lawson | Getty Images

Enlarge

Some Mazda owners in the Seattle area are stuck with bricked infotainment systems after listening to a particular radio station.

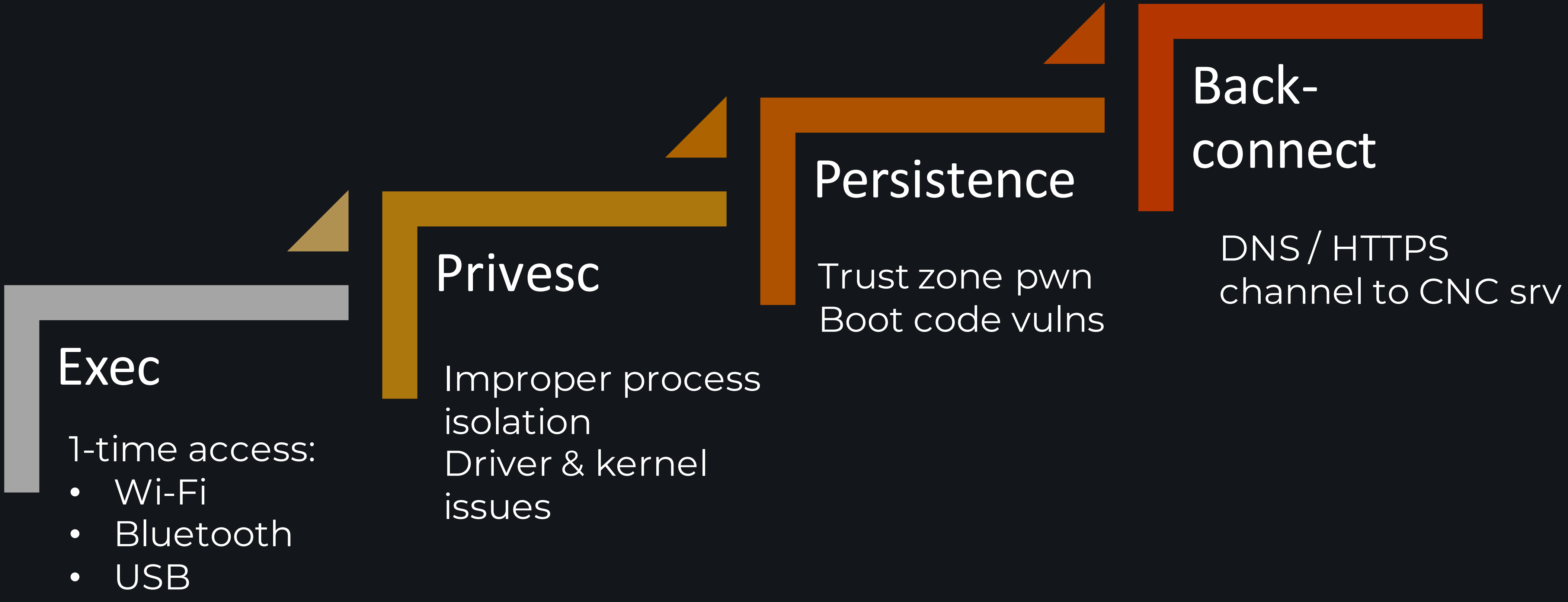
According to the Seattle Times, the problem began on January 30 and afflicted Mazdas from model years 2014 to 2017 when the cars were tuned to the local NPR station, KUOW 94.9. At some point during the day's broadcast, a signal from KUOW caused the Mazdas' infotainment systems to crash—the screens died and the radios were stuck on 94.9 FM.

Infiltration

- Wi-Fi & Bluetooth
  - Baseband chip vulnerabilities
  - Vulnerabilities in protocol stacks
  - Media file format parsers
- USB
  - Driver bugs
  - File format parser flaws:
    - Media
    - Map updates
    - Firmware updates
  - Firmware signature flaws

Exploitable overflows are still common

Lateral movement on the IVI



Exec

1-time access:

- Wi-Fi
- Bluetooth
- USB

Privesc

Improper process isolation
Driver & kernel issues

Persistence

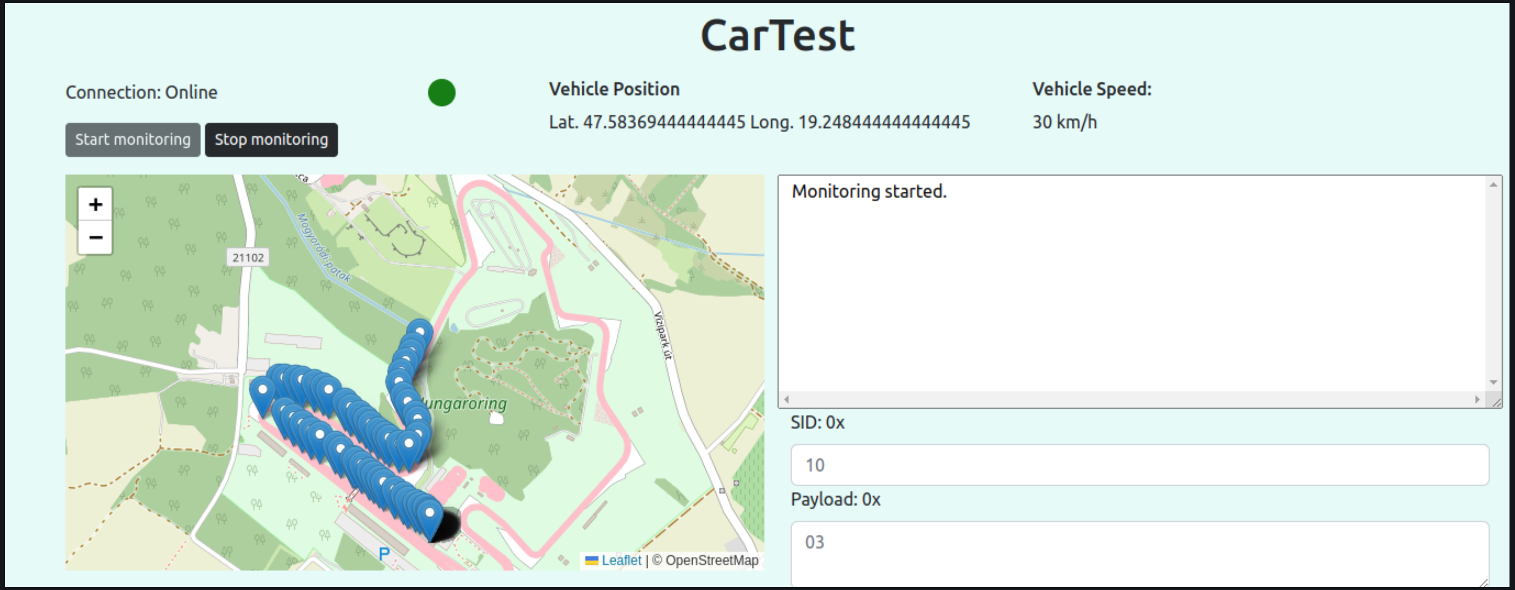
Trust zone pwn
Boot code vulns

Back-connect

DNS / HTTPS channel to CNC srv

1 – Impact

- Code execution on the infotainment
  - Display
  - Sound system
  - Microphone – no more private singing in traffic jams
  - Location tracking
  - User data compromise



CarTest

Connection: Online

Vehicle Position

Lat. 47.58369444444445 Long. 19.248444444444445

Vehicle Speed:

30 km/h

Monitoring started.

SID: 0x

10

Payload: 0x

03

1 – Counter-measures

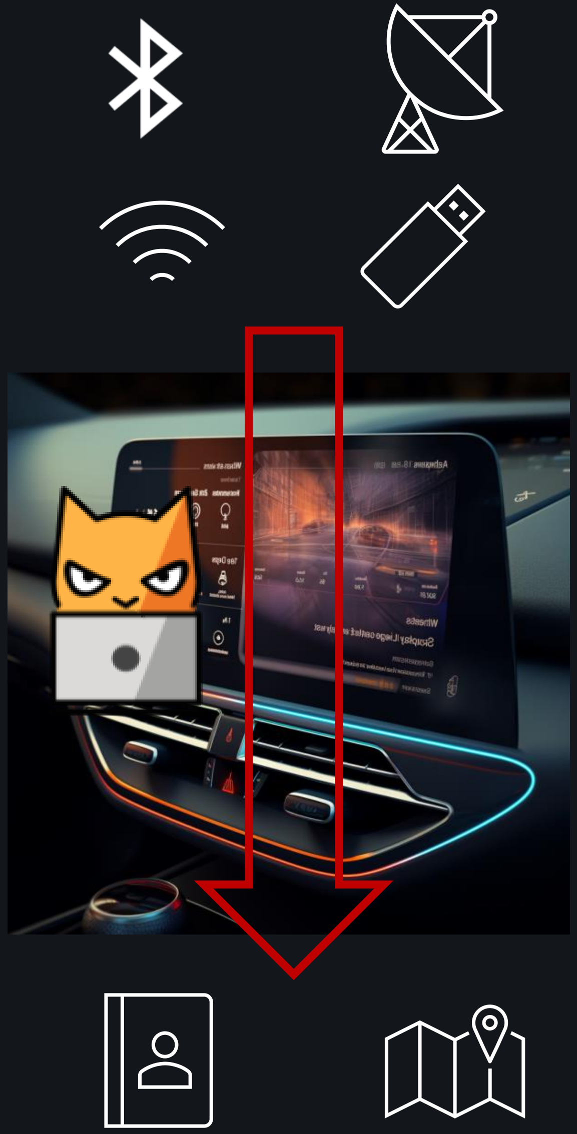
- Preventing
  - **Fuzz** format & protocol parsers
  - Run Bluetooth and Wi-Fi services as **low-privilege** or even **containerized** services
  - Pay attention to **inter-process communication** – it can undermine privilege separation
  - **Manual security analysis** of external interfaces, fw update process, supply chain (chips, boot loaders, protocol stacks, …)
- Monitoring
  - Security logs collection and analysis on IVI as part of **VSOC**

2 Protection of user data

Types of user data on the IVI

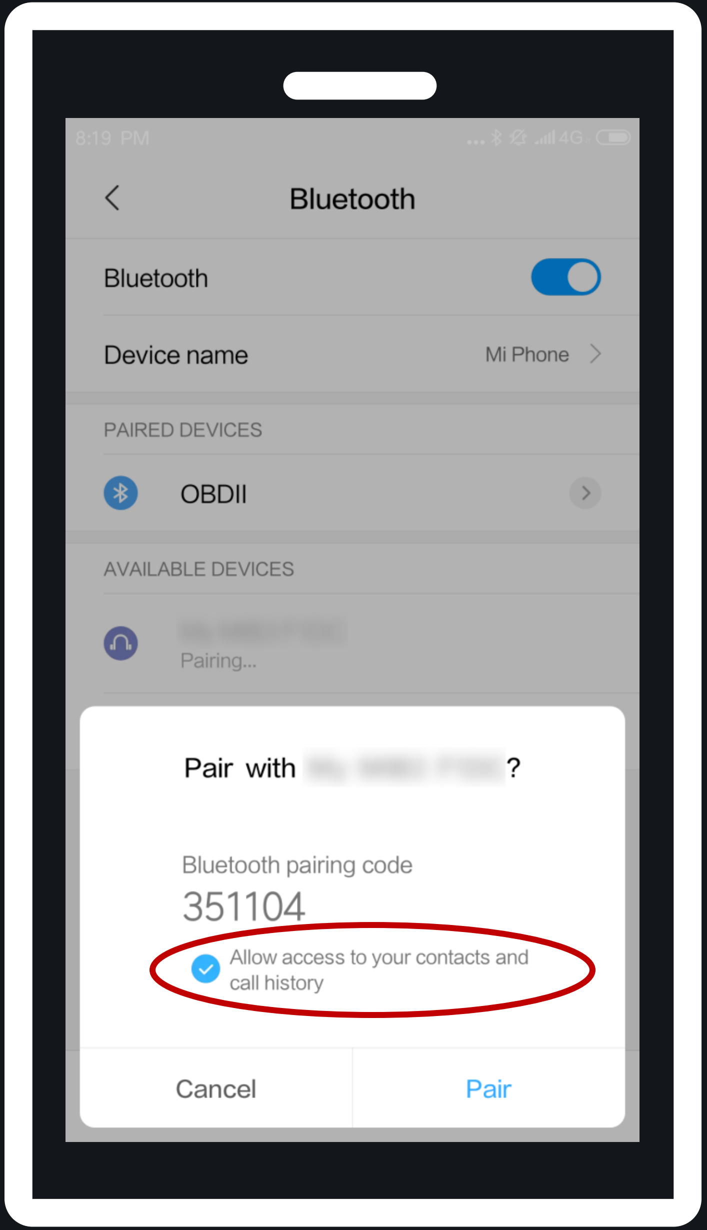
- Valuable user data
  - Phonebook & call history
  - Favourite locations & trip history

- Can be compromised:
  - Via external interfaces
  - Via physical access (memory dump)



The synchronization problem

Is our contact data well-protected when stored on the IVI?
Research shows that **not always**



8:19 PM

Bluetooth

Bluetooth

Device name Mi Phone

PAIRED DEVICES

OBDII

AVAILABLE DEVICES

[redacted]
Pairing...

Pair with [redacted]?

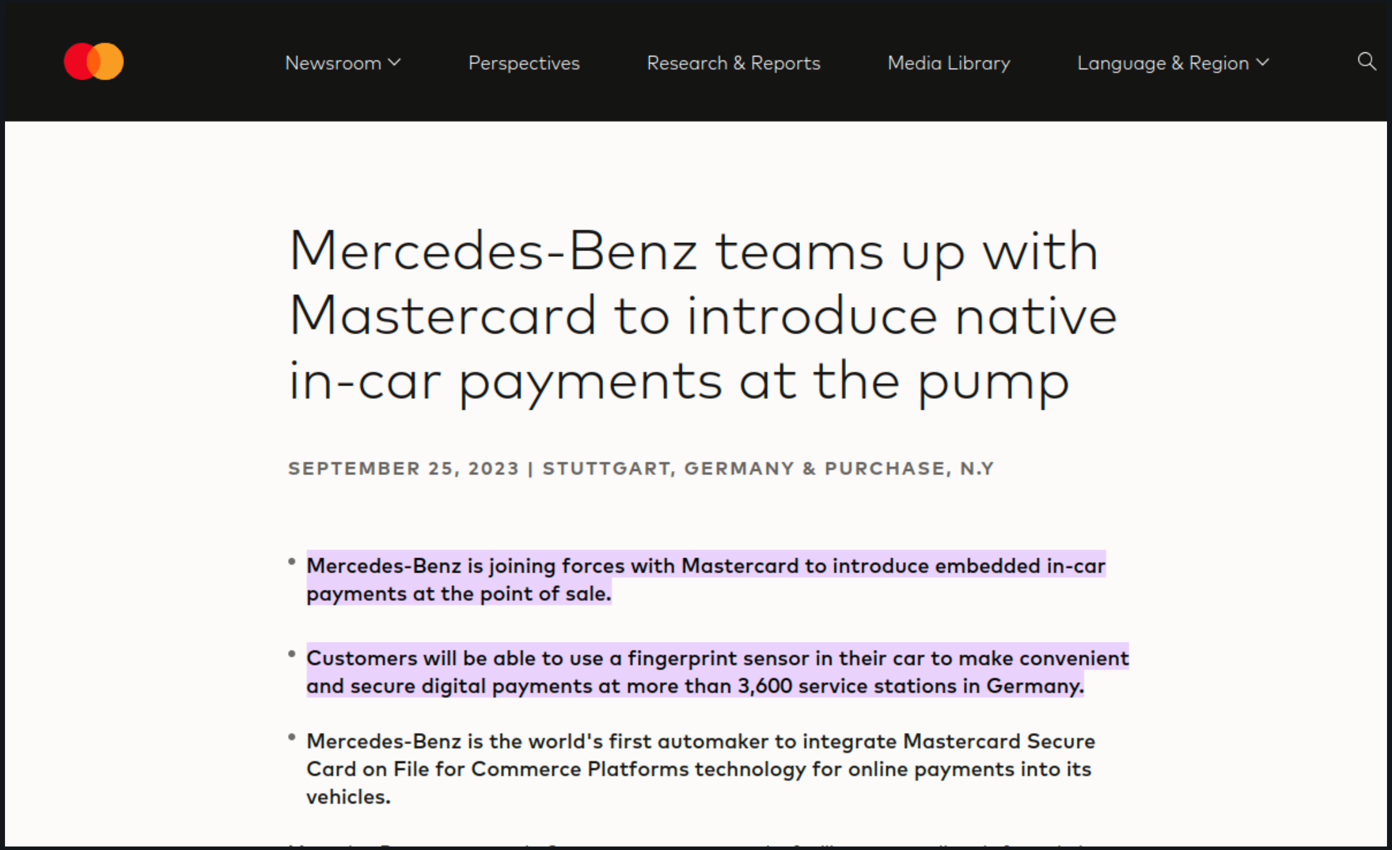
Bluetooth pairing code
351104

☑ Allow access to your contacts and call history

Cancel | Pair

Next: payments and subscriptions

- Vendors already offer subscriptions for their cars
  - IVI online
  - Connected services
  - Telemetry
  - …
  - Heated seats?
- Next: in-car payments



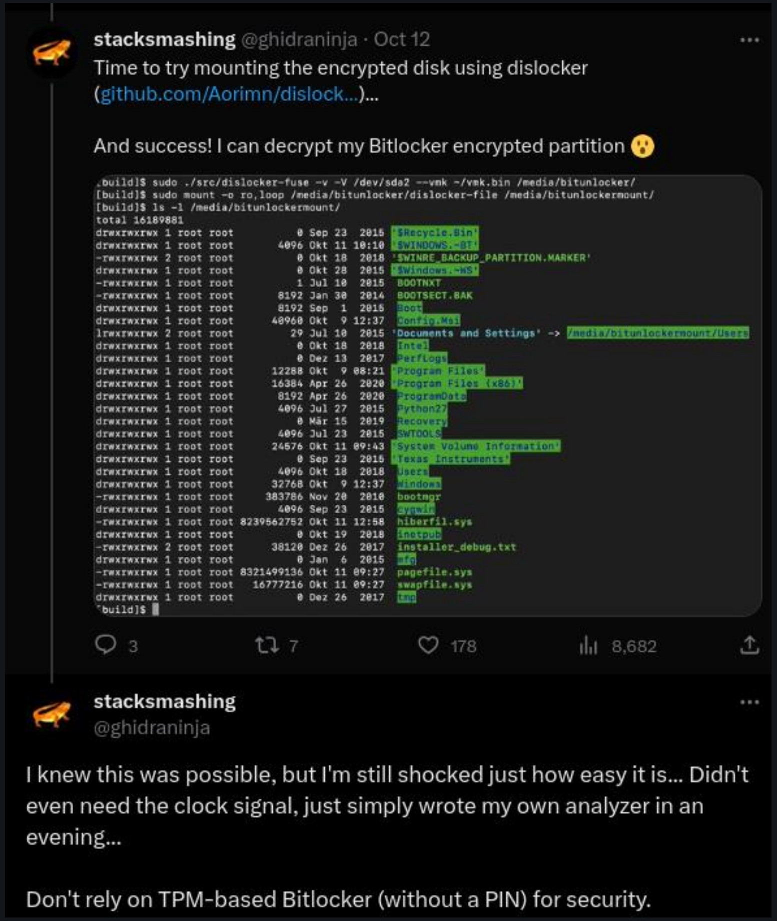
Mercedes-Benz teams up with Mastercard to introduce native in-car payments at the pump

SEPTEMBER 25, 2023 | STUTTGART, GERMANY & PURCHASE, N.Y

- Mercedes-Benz is joining forces with Mastercard to introduce embedded in-car payments at the point of sale.
- Customers will be able to use a fingerprint sensor in their car to make convenient and secure digital payments at more than 3,600 service stations in Germany.
- Mercedes-Benz is the world's first automaker to integrate Mastercard Secure Card on File for Commerce Platforms technology for online payments into its vehicles.

2 – Impact & counter-measures

- Impact: user data stolen
- Counter-measures:
  - Encryption of user data
  - TrustZone for storing decryption keys – not a silver bullet!
    - TZ apps must have proper input validation from the OS layer
  - TPM – not a silver bullet!
    - The hardware bus can be sniffed



stacksmashing @ghidraninja · Oct 12

Time to try mounting the encrypted disk using dislocker (github.com/Aorimn/dislock...)...

And success! I can decrypt my Bitlocker encrypted partition 😮

```
.build]$ sudo ./src/dislocker-fuse -v -V /dev/sda2 --vmk ~/vmk.bin /media/bitunlocker/
[build]$ sudo mount -o ro,loop /media/bitunlocker/dislocker-file /media/bitunlockermount/
[build]$ ls -l /media/bitunlockermount/
total 16189881
drwxrwxrwx 1 root root          0 Sep 23  2015 '$Recycle.Bin'
drwxrwxrwx 1 root root       4096 Okt 11 10:10 '$WINDOWS.~BT'
-rwxrwxrwx 2 root root          0 Okt 18  2018 '$WINRE_BACKUP_PARTITION.MARKER'
drwxrwxrwx 1 root root          0 Okt 28  2015 '$Windows.~WS'
-rwxrwxrwx 1 root root          1 Jul 10  2015  BOOTNXT
-rwxrwxrwx 1 root root       8192 Jan 30  2014  BOOTSECT.BAK
drwxrwxrwx 1 root root       8192 Sep  1  2015  Boot
drwxrwxrwx 1 root root      40960 Okt  9 12:37  Config.Msi
lrwxrwxrwx 2 root root         29 Jul 10  2015 'Documents and Settings' -> /media/bitunlockermount/Users
drwxrwxrwx 1 root root          0 Okt 18  2018  Intel
drwxrwxrwx 1 root root          0 Dez 13  2017  PerfLogs
drwxrwxrwx 1 root root      12288 Okt  9 08:21 'Program Files'
drwxrwxrwx 1 root root      16384 Apr 26  2020 'Program Files (x86)'
drwxrwxrwx 1 root root       8192 Apr 26  2020  ProgramData
drwxrwxrwx 1 root root       4096 Jul 27  2015  Python27
drwxrwxrwx 1 root root          0 Mär 15  2019  Recovery
drwxrwxrwx 1 root root       4096 Jul 23  2015  SWTOOLS
drwxrwxrwx 1 root root      24576 Okt 11 09:43 'System Volume Information'
drwxrwxrwx 1 root root          0 Sep 23  2015 'Texas Instruments'
drwxrwxrwx 1 root root       4096 Okt 18  2018  Users
drwxrwxrwx 1 root root      32768 Okt  9 12:37  Windows
-rwxrwxrwx 1 root root     383786 Nov 20  2010  bootmgr
drwxrwxrwx 1 root root       4096 Sep 23  2015  cygwin
-rwxrwxrwx 1 root root 8239562752 Okt 11 12:58  hiberfil.sys
drwxrwxrwx 1 root root          0 Okt 19  2018  inetpub
-rwxrwxrwx 2 root root      38120 Dez 26  2017  installer_debug.txt
drwxrwxrwx 1 root root          0 Jan  6  2015  mfg
-rwxrwxrwx 1 root root 8321499136 Okt 11 09:27  pagefile.sys
-rwxrwxrwx 1 root root   16777216 Okt 11 09:27  swapfile.sys
drwxrwxrwx 1 root root          0 Dez 26  2017  tmp
[build]$
```

stacksmashing
@ghidraninja

I knew this was possible, but I'm still shocked just how easy it is... Didn't even need the clock signal, just simply wrote my own analyzer in an evening...

Don't rely on TPM-based Bitlocker (without a PIN) for security.

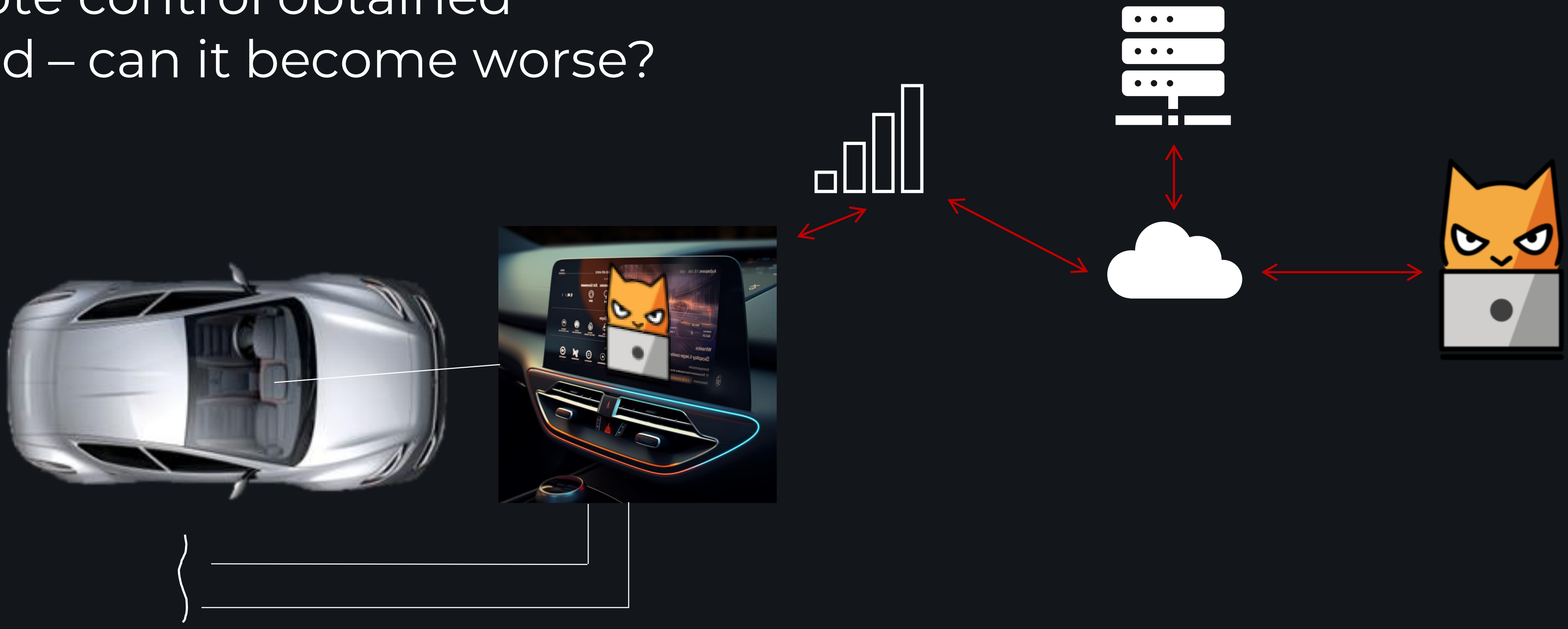
Know your security tools! They don't protect by themselves out-of-the-box!

https://x.com/ghidraninja/status/1712514241842884656

3 System isolation on IVI

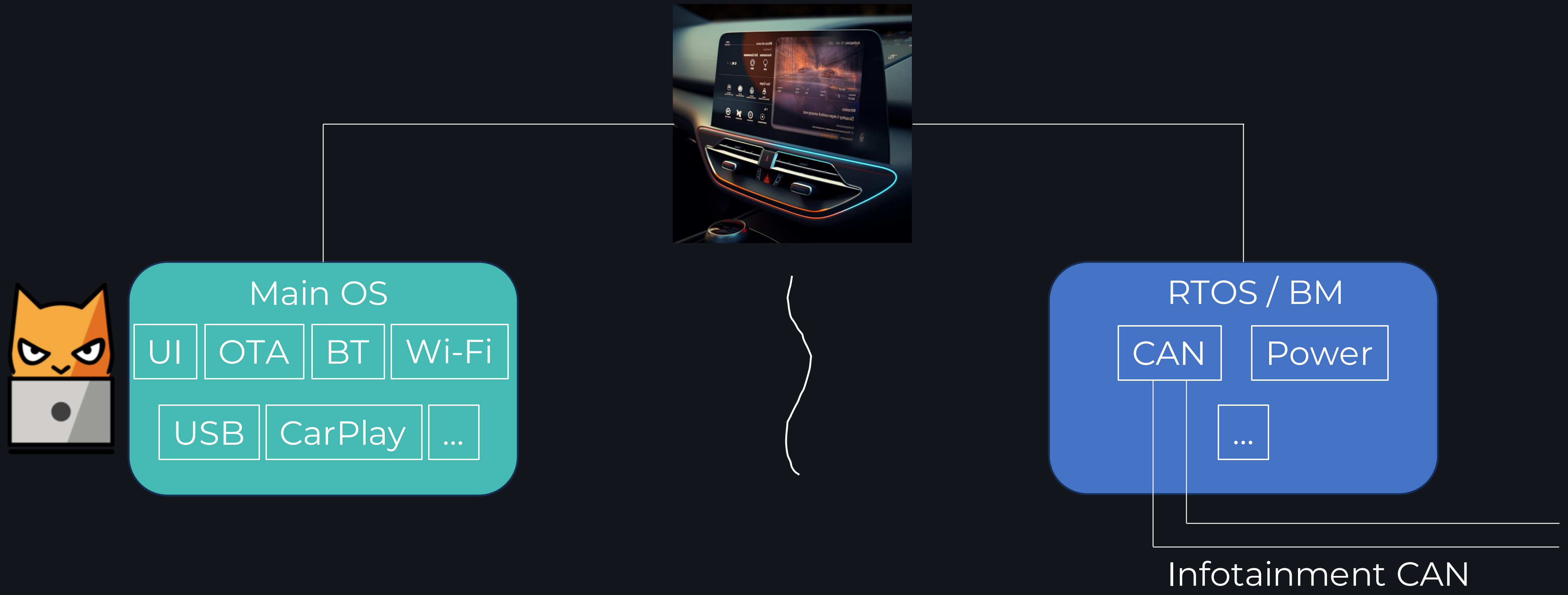
Assume-breach approach

- Remote control obtained
- All bad – can it become worse?



IVI internals

- Remote control obtained
- All bad – can it become worse?
- No – we have system isolation



Main OS

UI | OTA | BT | Wi-Fi

USB | CarPlay | ...

RTOS / BM

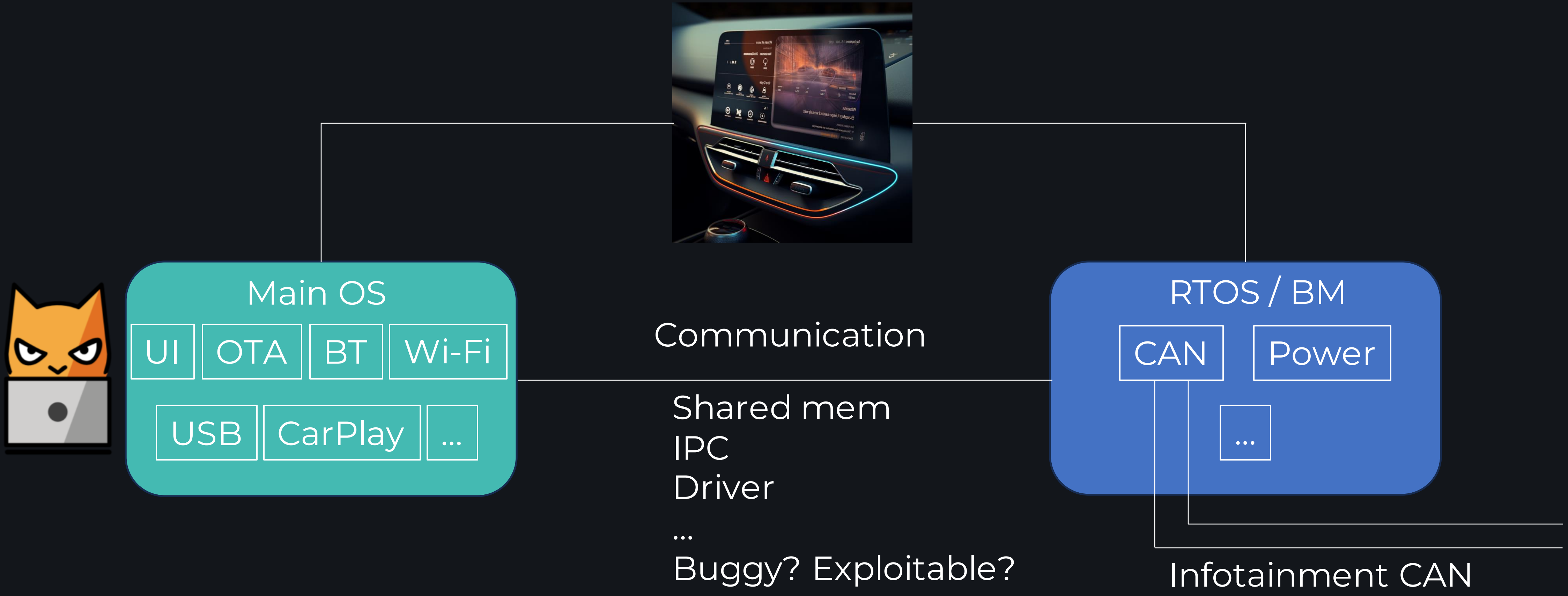
CAN | Power

...

Infotainment CAN

IVI internals

- Remote control obtained
- All bad – can it become worse?
- No – we have system isolation
- Do we?



Main OS

UI | OTA | BT | Wi-Fi

USB | CarPlay | ...

Communication

Shared mem
IPC
Driver
...
Buggy? Exploitable?

RTOS / BM

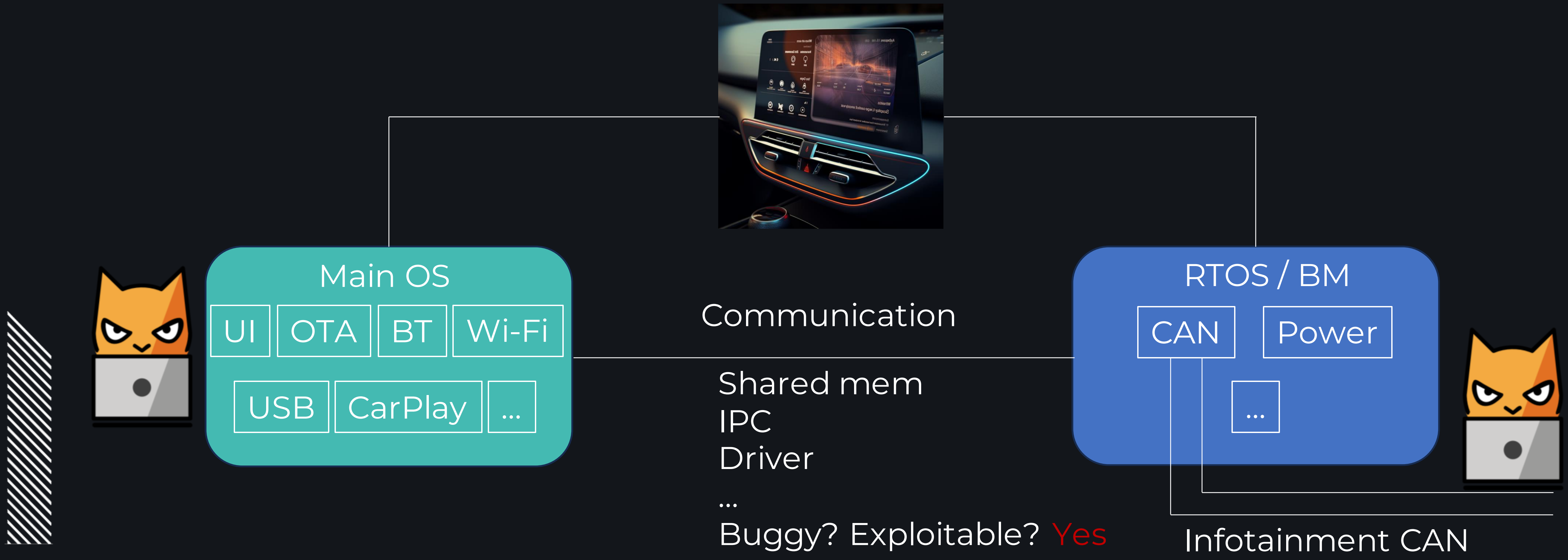
CAN | Power

...

Infotainment CAN

IVI internals

- Remote control obtained
- All bad – can it become worse?
- No – we have system isolation
- Do we? No



Main OS

UI | OTA | BT | Wi-Fi

USB | CarPlay | ...

Communication

Shared mem
IPC
Driver
...
Buggy? Exploitable? Yes

RTOS / BM

CAN | Power

...

Infotainment CAN

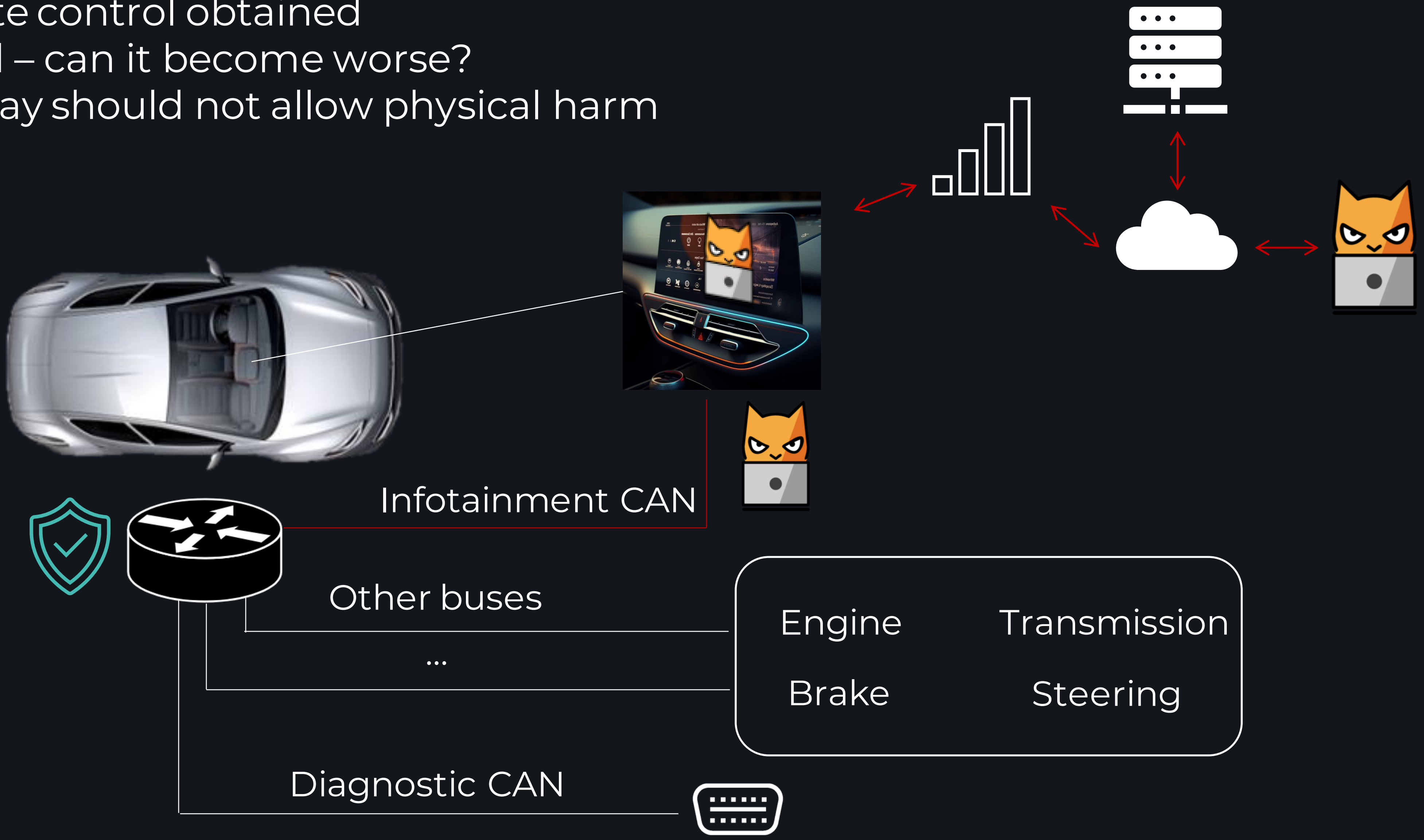
3 – Impact & counter-measures

- Impact – attackers gets into at least 1 CAN domain
- Counter-measures:
  - Evaluation of interfaces between RTOS and Main OS
  - Fuzzing
  - Design of firmware update process is important
    - Can the main CPU reflash the RTOS?
    - Are there signatures?
    - Are they well-implemented?

4 Network segmentation

Assume-breach approach

- Remote control obtained
- All bad – can it become worse?
- Gateway should not allow physical harm



Infotainment CAN

Other buses

...

Diagnostic CAN

Engine

Transmission

Brake

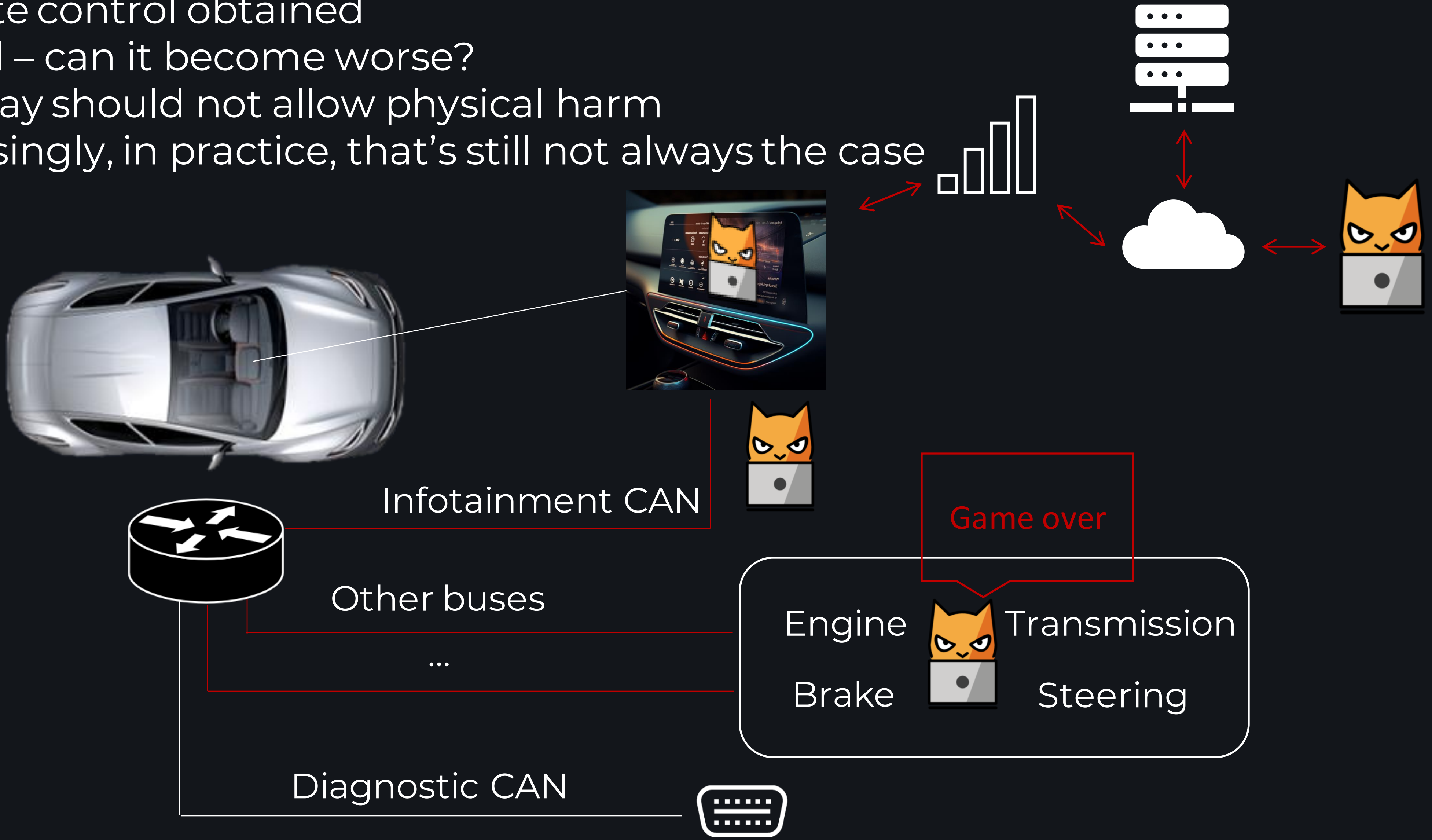
Steering

Vehicle gateway

- Interconnects different physical buses
- Filters unnecessary traffic – firewalling function
- Controls diagnostic restrictions
- The gateway is the last resort between a would-be attacker and physical impact

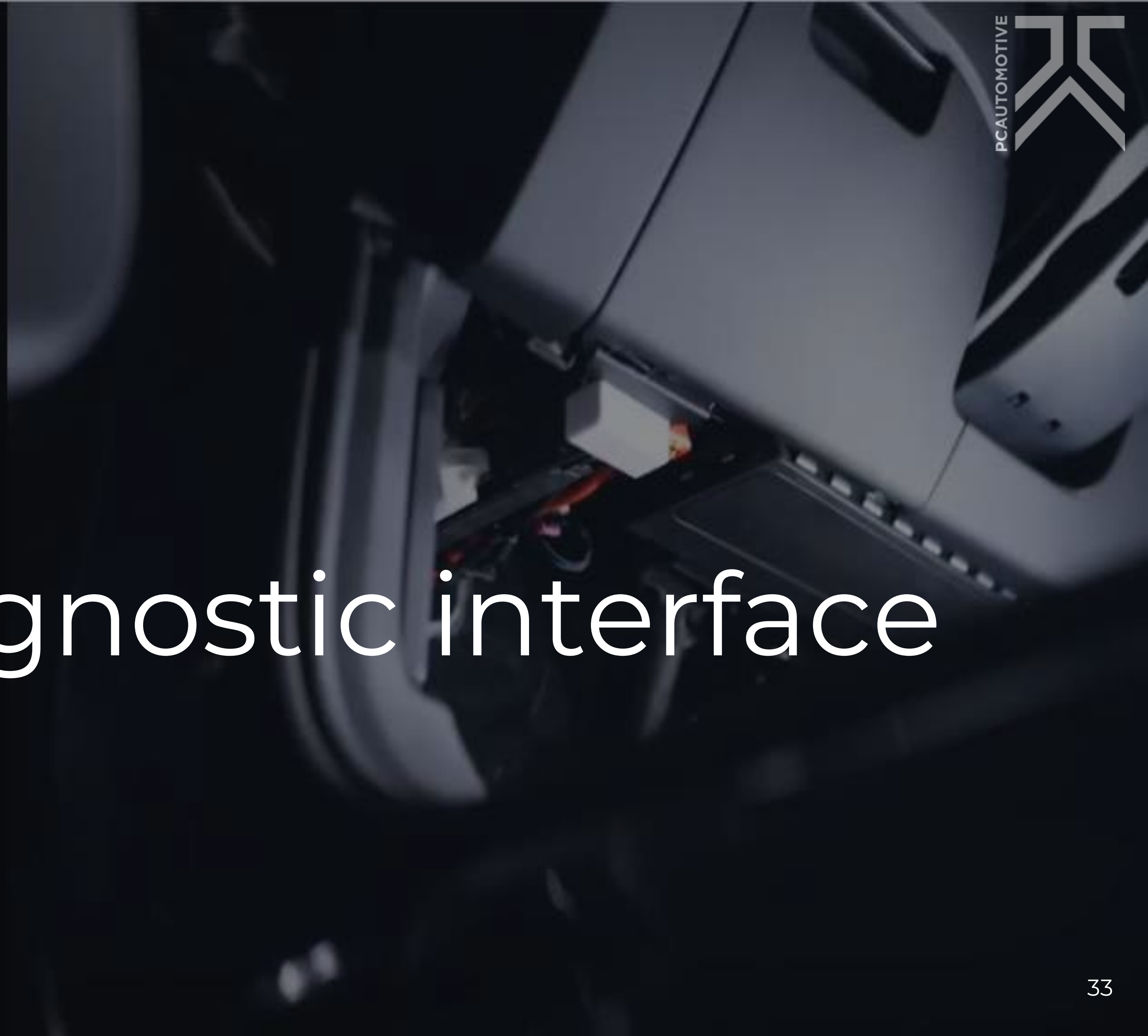
Gateway problems

- Remote control obtained
- All bad – can it become worse?
- Gateway should not allow physical harm
- Surprisingly, in practice, that’s still not always the case



4 Impact & counter-measures

- Poor segmentation = BIG safety problems, which is hard/impossible to fix after vehicle release
- Counter-measures:
  - Implement gateway firewalling feature – if you haven't already
  - Test that the traffic forwarding really corresponds to the programmed rules
  - If diagnostic of the car from IVI is a must, apply other restrictions
    - Trunk opening
    - Speed limitation



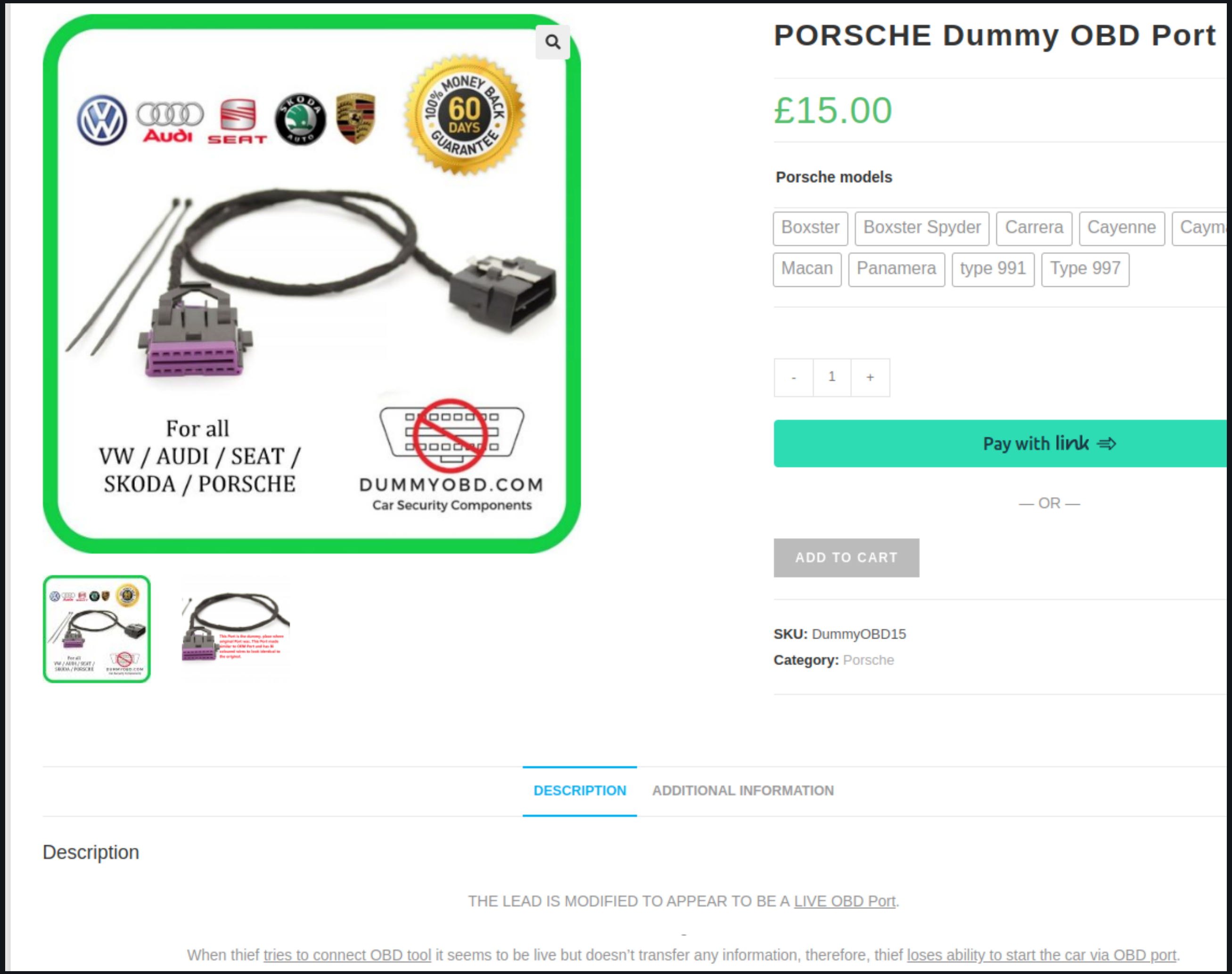
5 & 6 Diagnostic interface

Diag interface

- OBD includes diagnostic CAN bus (plus sometimes other buses)
- To test major car functions
  - Opening/closing doors and windows
  - lights, horn, wipers, washers, …
  - Folding mirrors
- Firmware update
- Quite sensitive functions – must be protected

Diag interface - example

- Diag port sealer
- To prevent car theft



PORSCHE Dummy OBD Port

£15.00

Porsche models

Boxster | Boxster Spyder | Carrera | Cayenne | Caym
Macan | Panamera | type 991 | Type 997

SKU: DummyOBD15

Category: Porsche

Description

THE LEAD IS MODIFIED TO APPEAR TO BE A LIVE OBD Port.

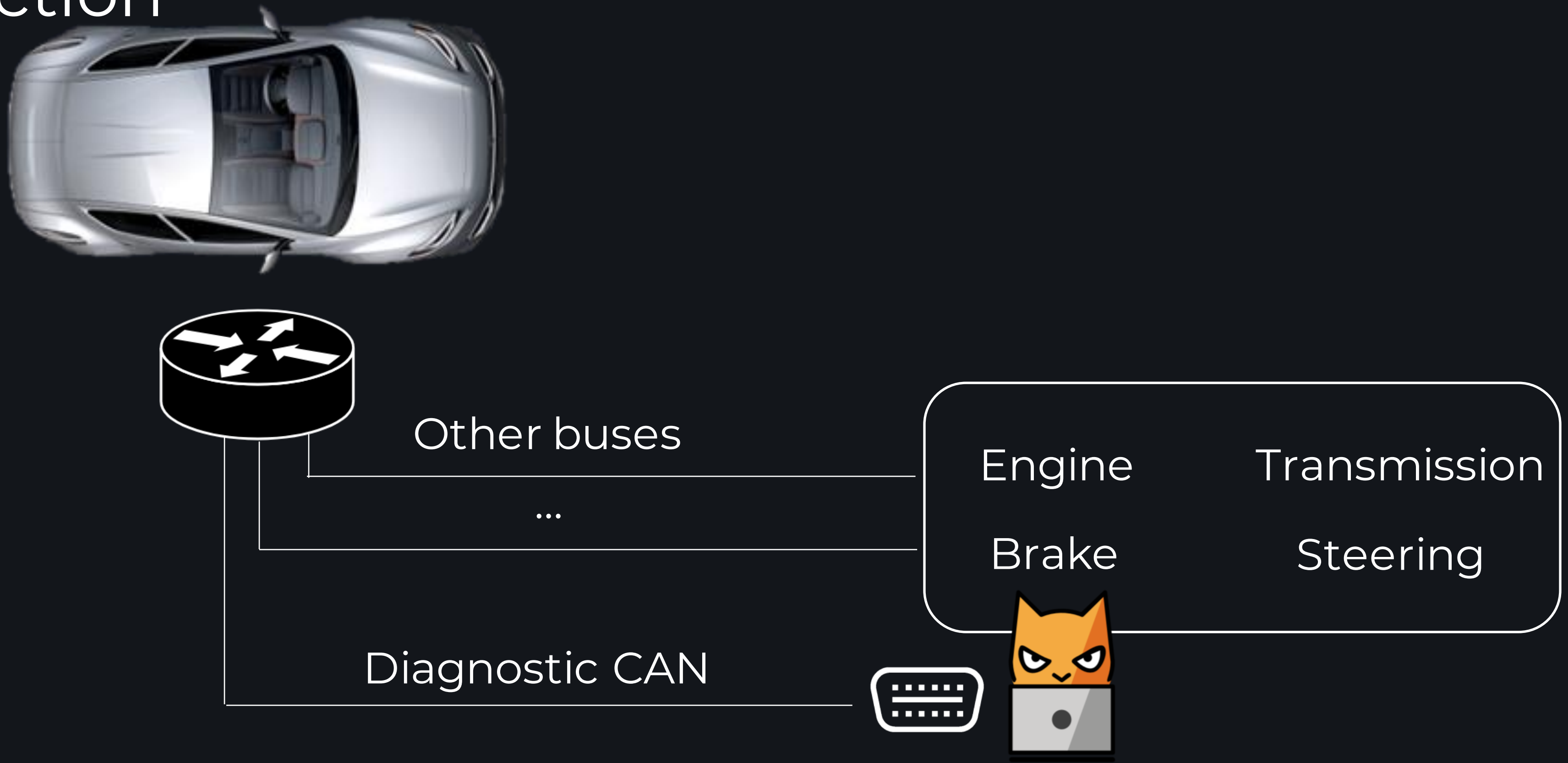
-

When thief tries to connect OBD tool it seems to be live but doesn't transfer any information, therefore, thief loses ability to start the car via OBD port.

https://www.dummyobd.com/shop/porsche-dummy-obd-port/

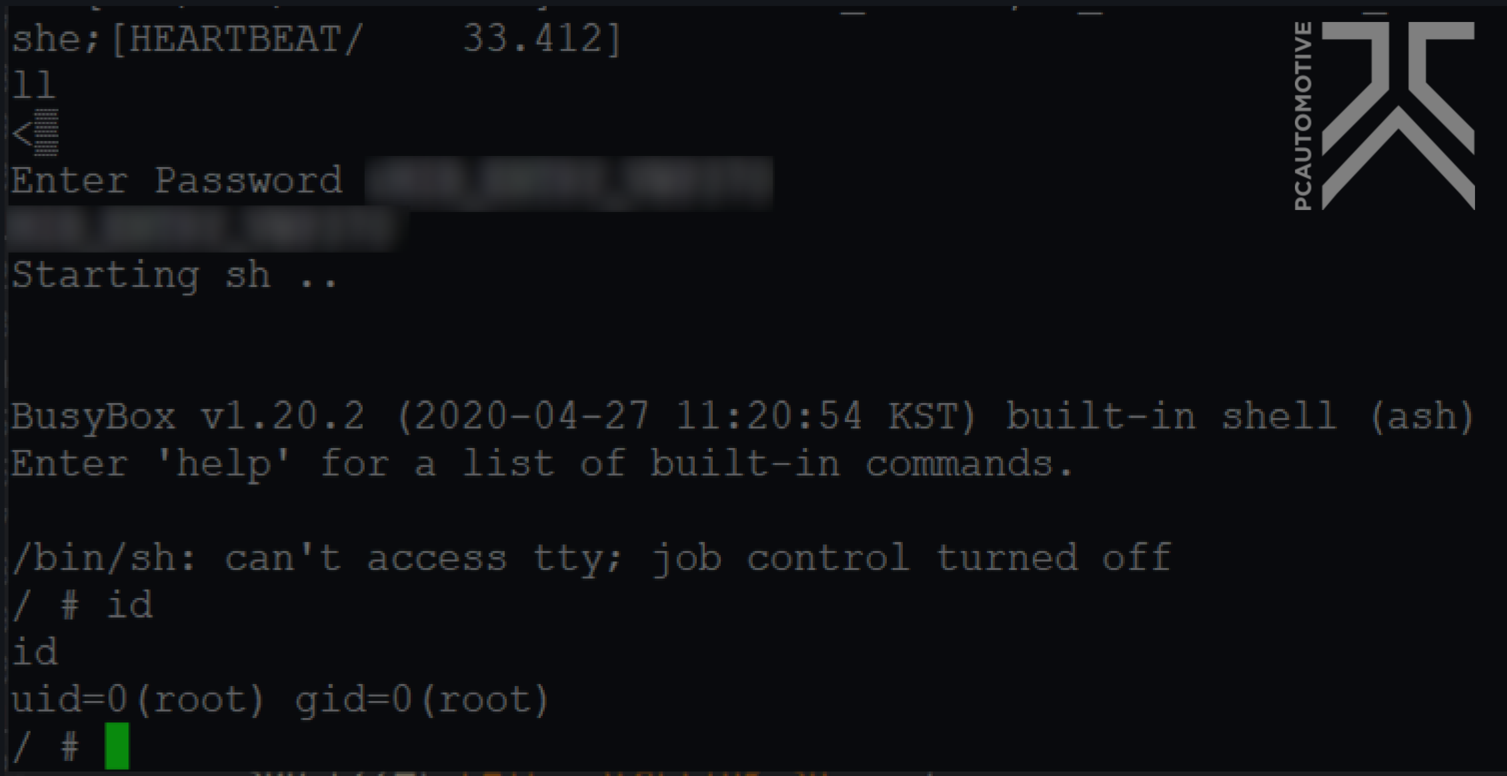
Diag interface

- This attack path requires physical access to the car
- We don't always watch our cars
- Car sharing services are affected by poor diag protection



Existing protections

- UDS authentication for critical functions – frequently appears weak
- Physical protection – trunk opening before diag functions become available
- Speed limitation – no diag at high speed

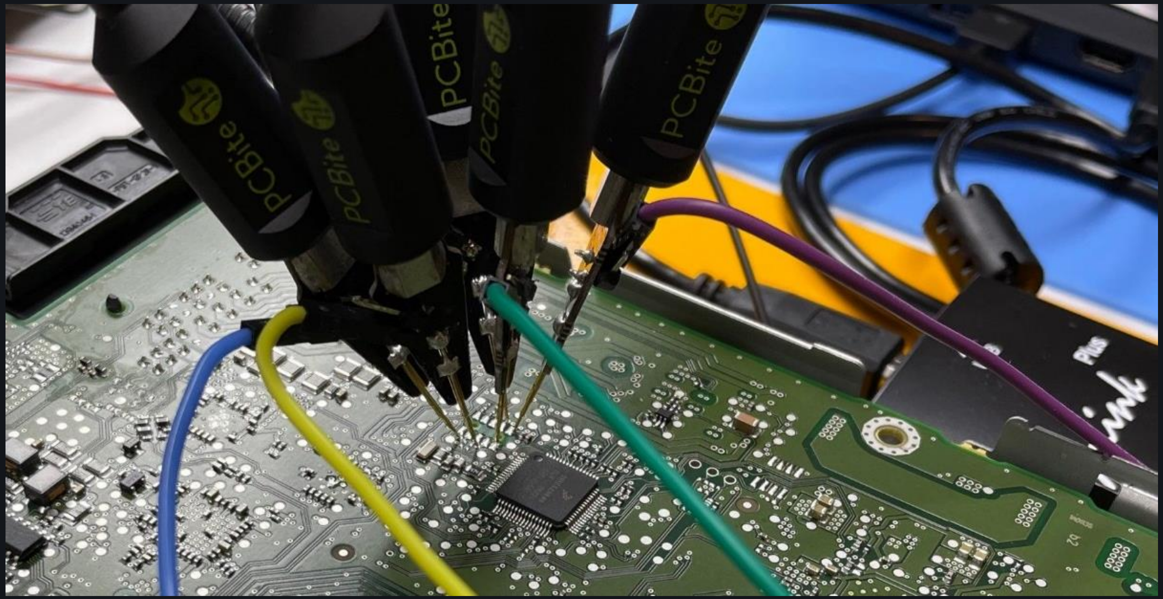


```
she;[HEARTBEAT/    33.412]
ll
<
Enter Password [redacted]
[redacted]
Starting sh ..


BusyBox v1.20.2 (2020-04-27 11:20:54 KST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

/bin/sh: can't access tty; job control turned off
/ # id
id
uid=0(root) gid=0(root)
/ # 
```

7 & 8 Debug features

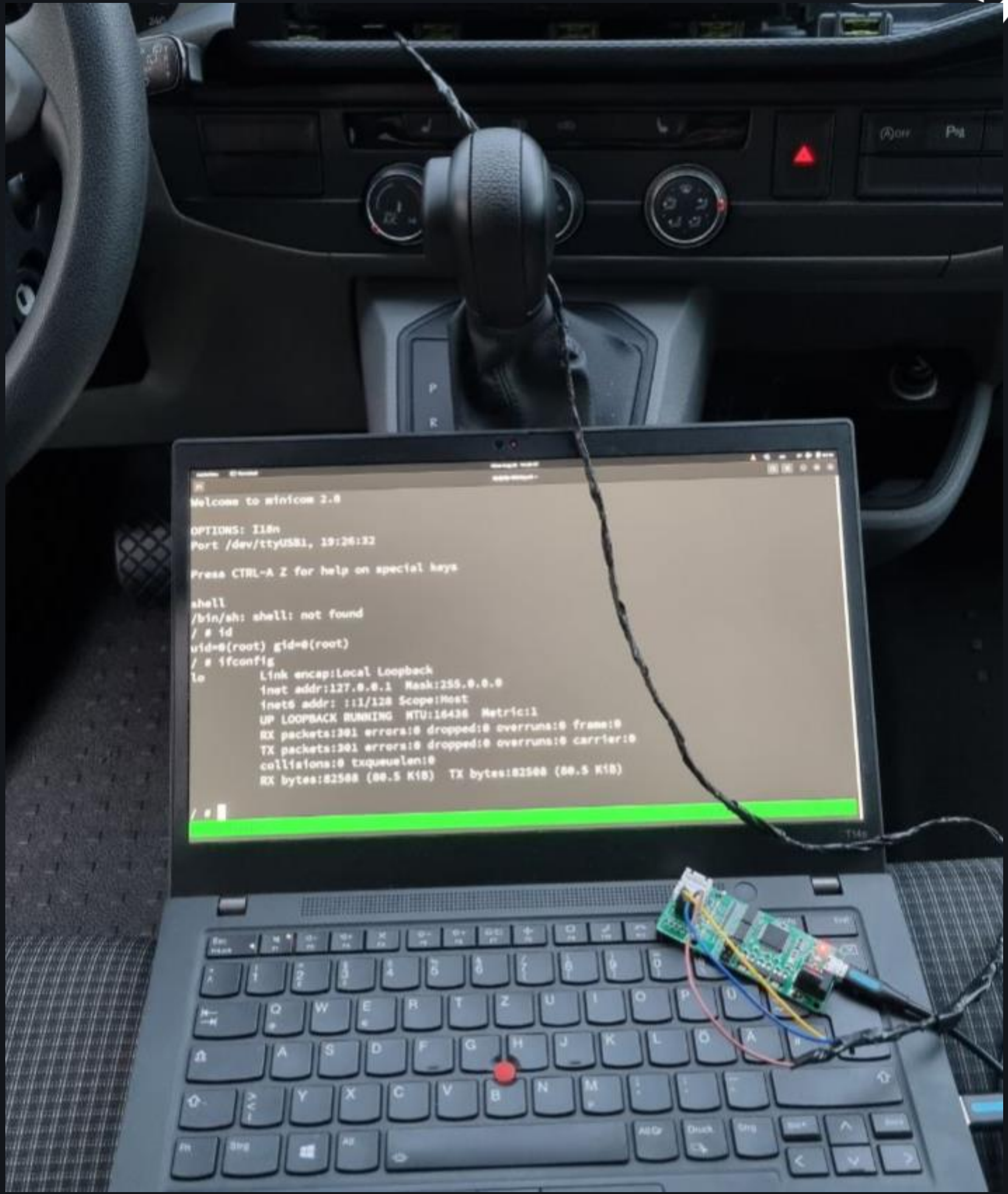
Unlocked debugging interfaces

- Challenges of black-box analysis (& thus, real hacking):
  - Obtain relevant FW & SW images
  - Obtain debug access to the target – very useful for PoC exploitation
- Debugging interfaces left in release products significantly eases those tasks



Unlocked debugging interfaces

- Root shell = easy debug and enjoyable security testing
- ~~Please don't lock it!~~



```
Welcome to minicom 2.8

OPTIONS: I18n
Port /dev/ttyUSB1, 19:26:32

Press CTRL-A Z for help on special keys

shell
/bin/sh: shell: not found
/ # id
uid=0(root) gid=0(root)
/ # ifconfig
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:301 errors:0 dropped:0 overruns:0 frame:0
          TX packets:301 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:82588 (80.5 KiB)  TX bytes:82588 (80.5 KiB)

/ #
```

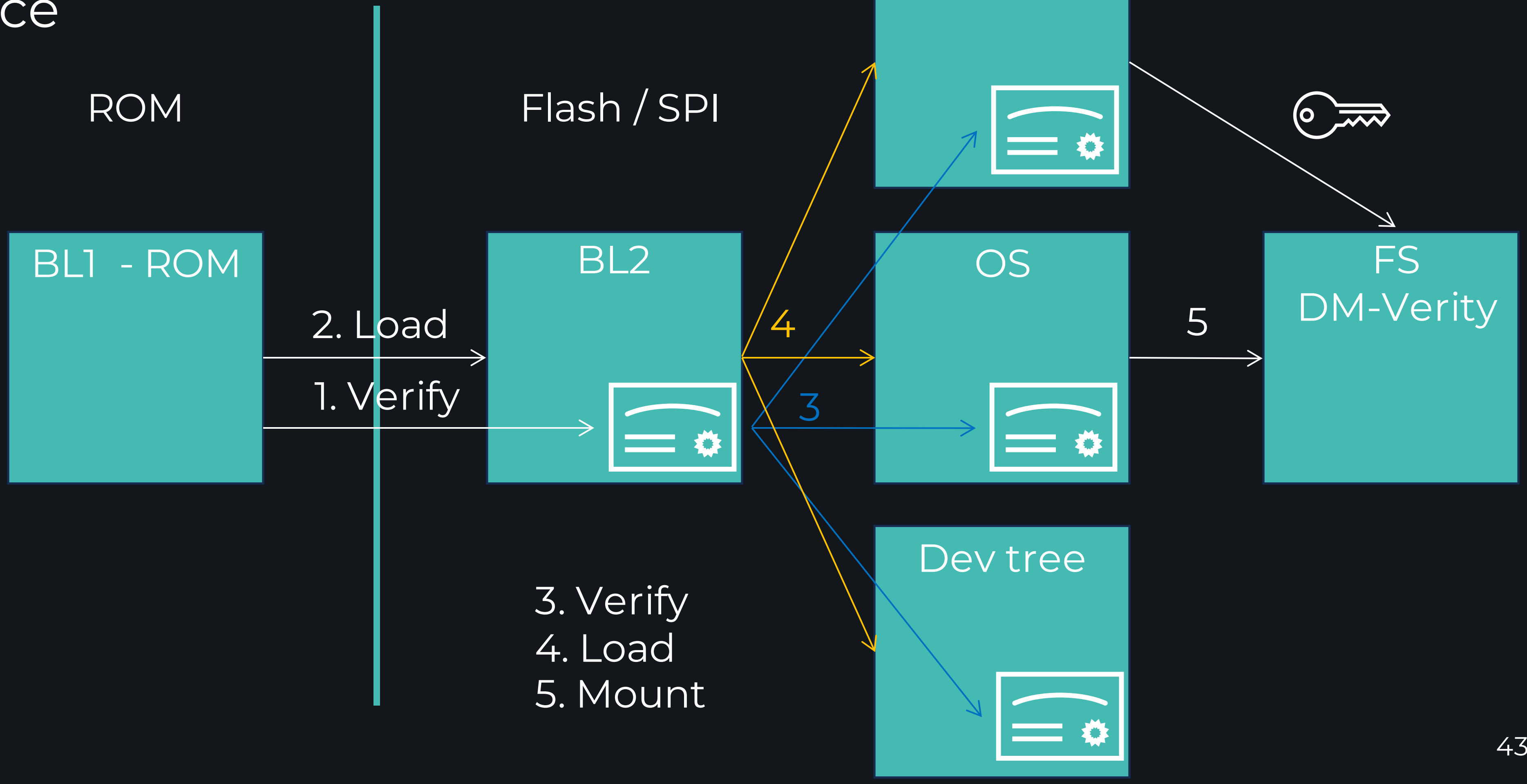
Impact & counter-measures

- Impact:
  - Ease intelligence gathering, exploit debugging, lateral movement for adversaries
  - Unauthorized chip tuning
  - Bypass of paid services
- Counter-measures:
  - Proper hardware enumeration
  - SMART usage of protection mechanisms provided by HW chip manufacturers
  - Remove or lock software debugging mechanisms
    - UART shells
  - Hardcoded password is not a lock!

9 & 10 Crypto impl. flaws

Secure boot

- Security feature that blocks
  - Flashing malicious FW
  - Persistence



3. Verify
4. Load
5. Mount

Firmware signatures

- Secures OTA and local (USB, OBD) updates
- Crypto signature (certificate) is attached to the update image, like in the secure boot case
- Only developers have a private key to sign
- Devices incorporate public key to verify
- Public keys need to be stored securely (TrustZone, TPM)

- Common flaws:
  - Incomplete coverage – some files are not signed
  - Manipulations prior to signature verification – unpacking, parsing, so on

Impact & counter-measures

- Impact: firmware forgery, same as for 7 & 8 or even worse
- Mitigations:
  - Implement secure boot if you haven’t already!
  - Implement signature-based updates if you haven’t already!
  - Verify signature of an image before manipulating it
    - Parsing
    - Unpacking
  - Ensure that the whole software image is covered by signature verification!
  - Fuzz your custom certificate parsers!

Final thoughts

- Thanks to researchers publishing their work results and following responsible disclosure!
- Thanks to manufacturers and vendors who handles security reports openly!
- Do verification & validation of your products and components!
- For practical example of our recent findings, see our talk at Secure Our Streets 2023:
  - Slides https://sos.asrg.io/wp-content/uploads/2023/09/Danila-Parnishchev_Presentation.pdf
  - Recording https://youtu.be/GK9s4y-0GpE?si=rzVyTuFZuPwvQczu

PCAUTOMOTIVE

THANK YOU
FOR YOUR ATTENTION!

E: info@pcautomotive.com
A: 1031 Budapest, Záhony u. 7. C ép.

WWW.PCAUTOMOTIVE.COM