WARNING

The following talk contains disturbing stories from the automotive industry, which can cause discomfort and anger towards the audience. There have already been many instances of fainting and vomiting in conference halls. For those choosing to continue, you have been warned…

/s

HORROR STORIES

FROM THE AUTOMOTIVE INDUSTRY

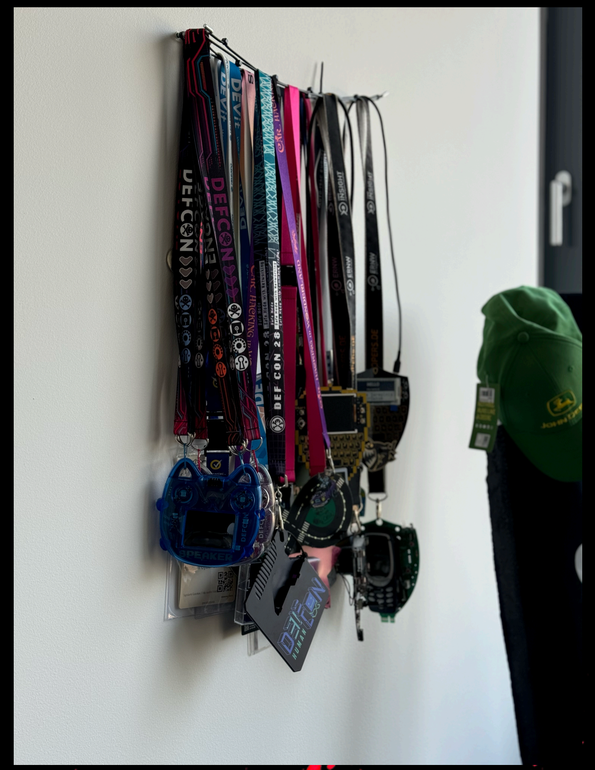
THOMAS SERMPINIS
@CROWTOM

ANDRÉ MAIA
@FIGIS

$Whoami

- Thomas Sermpinis (@cr0wtom)
  - Technical Director - CTO by Day
  - Security Researcher by Night
- André Maia (@figis)
  - Security Researcher | Penetration Tester
  - PhD in Physics
- Hack Everything, Everywhere, All at Once (and Legally)
- *For more: auxilium-labs.com*

AUXILIUM
Pentest Labs



Goals of this talk

- Analyze the state of cybersecurity in the automotive industry
- Present unique (and hopefully interesting) use-cases, result of around 200 pentests and research projects in the industry
- Educate the new, the old and the **bold**
- Endorse and push more hackers to automotive
- Raise and highlight the significance of safety related devices

ΚΕΦΑΛΑΙΟ 0

AUTOMOTIVE SECURITY

The state of automotive cybersecurity

Kevin2600 @Kevin2600 · May 15
Replying to @Kevin2600
Demo video

How Tech-Savvy Thieves Are Stealing Cars By Hacking Through Headlights

by **Nathan Ord** — Saturday, April 08, 2023, 02:37 PM EDT

2 Comments

BECOME A PATRON

Early last year, hackers were replaying remote keyless system codes to unlock and steal Honda or Acura vehicles. This year, criminals of TikTok have been showing people how to break into certain Hyundai and Kia models with some hotwiring. However, criminals are upping their thieving game as car companies come to the rescue with patches and security solutions for vehicles. With this forced advancement come car thefts through attacks on the car's central nervous system called the Controller Area Network (CAN) bus.

uld've let hackers and start cars

t use Sirius XM's connected

/ Security researcher Sam Curry found an exploit affecting the telematics and infotainment systems powered by Sirius XM. Curry says the company has since fixed the issue.

By **Emma Roth**, a news writer who covers the streaming wars, consumer tech, crypto, social media, and much more. Previously, she was a writer and editor at MUO.

Dec 3, 2022 at 11:12 AM MST | 8 Comments / 8 New

Even the most recent models. Image: Honda

By **Mitchell Clark**
Jul 11, 2022 at 6:23 PM MST | 0 Comments / 0 New

s Are Stealing Kias With Just a Cable

ts the Korean cars that use a physical key.

SHED AUG 2, 2022 3:28 PM EDT

NEWS

empts at

The state of automotive cybersecurity

The state of automotive cybersecurity

- UN Regulation No. 155 - general requirements for Vehicle Cybersecurity
  - Provides a set of standards that must be met in order to ensure the safety of road vehicles
  - The regulation requires the operation of a certified cybersecurity management system (CSMS)
  - UN R155 is significant as it provides a set of standards that must be met in order to ensure the safety of road vehicles
- **In summary:** Trying to shape the completely unregulated mess that exists right now
- **Biggest caveat?** Penetration testing is solely based on the Risk Assessment (TARA)

ΚΕΦΑΛΑΙΟ 1

TIER 1 SUPPLIERS

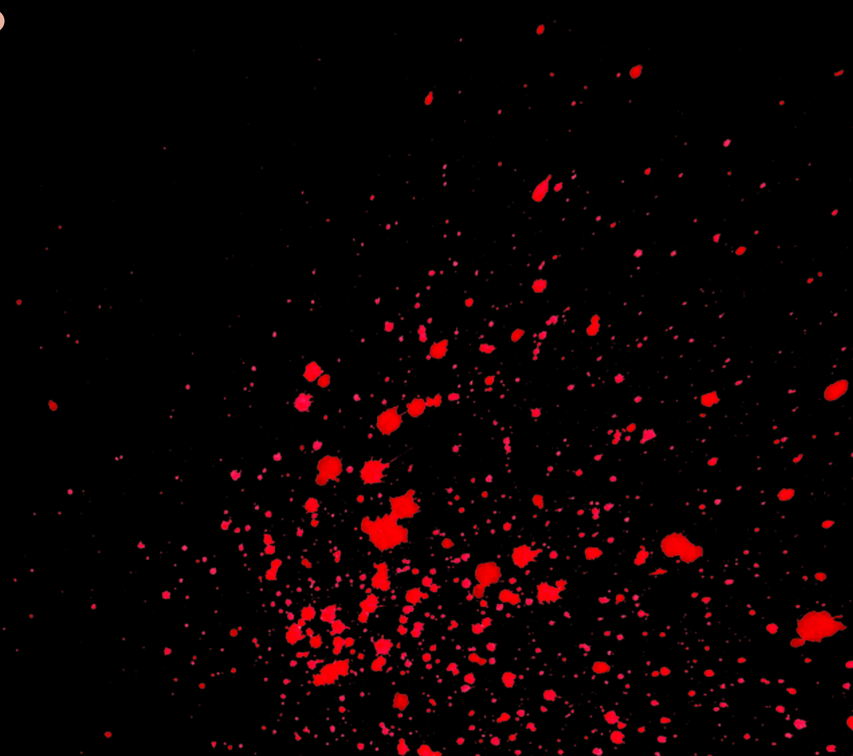
A story of how cybersecurity requirements are designed by OEMs and NOT followed by Tier 1's.

Cyber Security Requitements

- Cyber security requirements are developed and distributed by OEMs
  - A document which specifies **the engineering requirements for cybersecurity risk management** throughout the vehicle life cycle, including the **processes, policies, and standards to comply with the legal framework** and **protect the vehicle from cyber-attacks**

- Tier 1 suppliers should (ideally) comply to those, for correct and “secure" functionality of the supplied components

Is that actually the case though?



Reality check

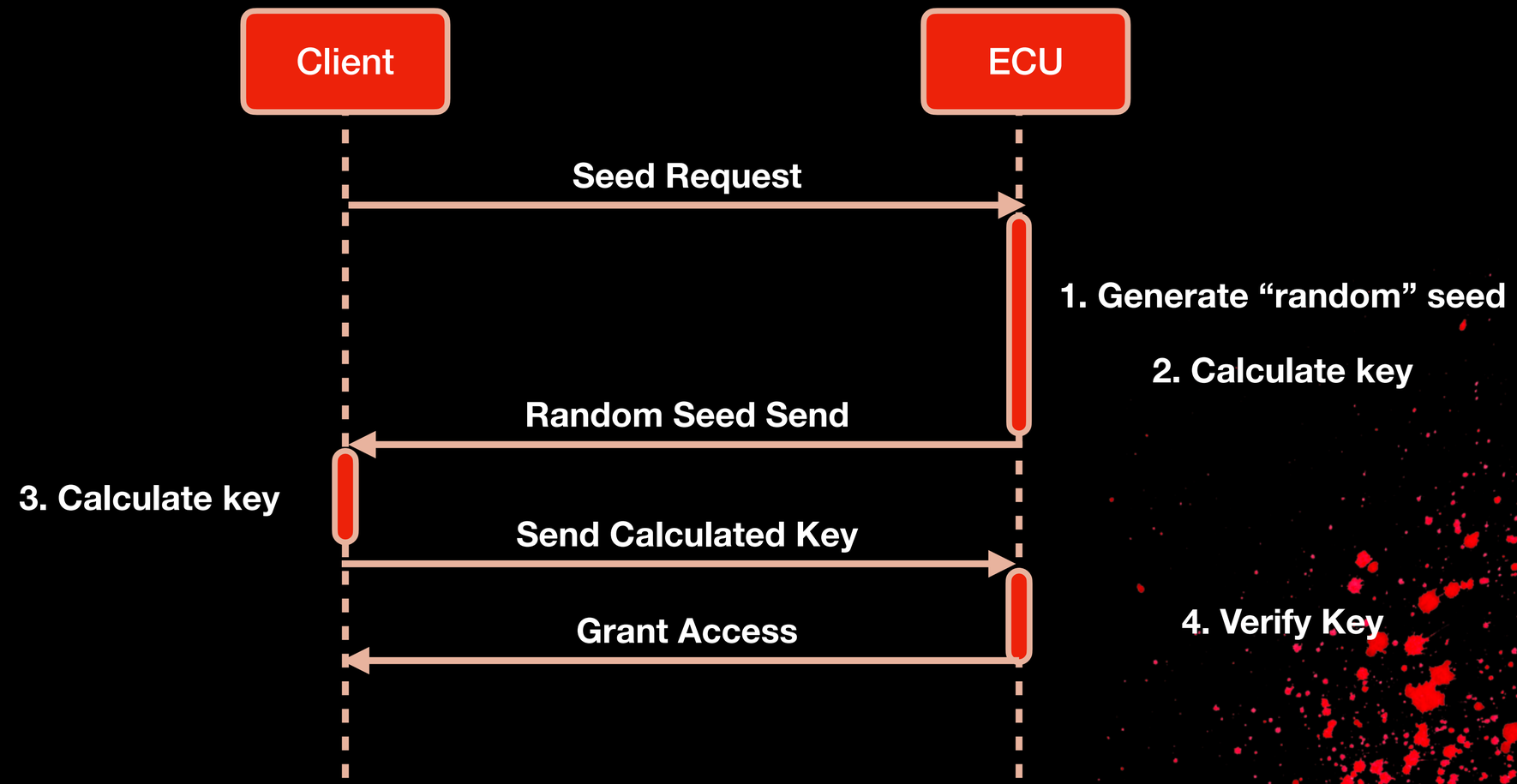
- Several Tier 1's are based in countries with *Low Transparency* ***and*** *Weak Governance.*[1,2]
- *How clear are the Cyber Security Requirements?*
- *Is there a proactive or reactive approach from the OEM or the pentesting supplier?*

1. There is no specific company, entity or government targeted in this sentence.
2. The original bullet-point was referring to ***shady countries***. To avoid any legal implications, speakers used the magic of AI to suggest and use a more formal alternative. /s
3. No language models were used throughout this research and this presentation.

Use Case 1: The path to Game Over

- UDS stands for Unified Diagnostic Services, an application layer protocol for communication between electronic control units in automotive electronics
- Allows diagnostic functions such as reading and erasing fault codes, programming, testing, and monitoring of ECUs
- Consists of several “services" which can be used to perform specific actions
- A really common authentication scheme in UDS is the ***Security Access*** service (0x27)
  - Allows elevated access to authenticated users

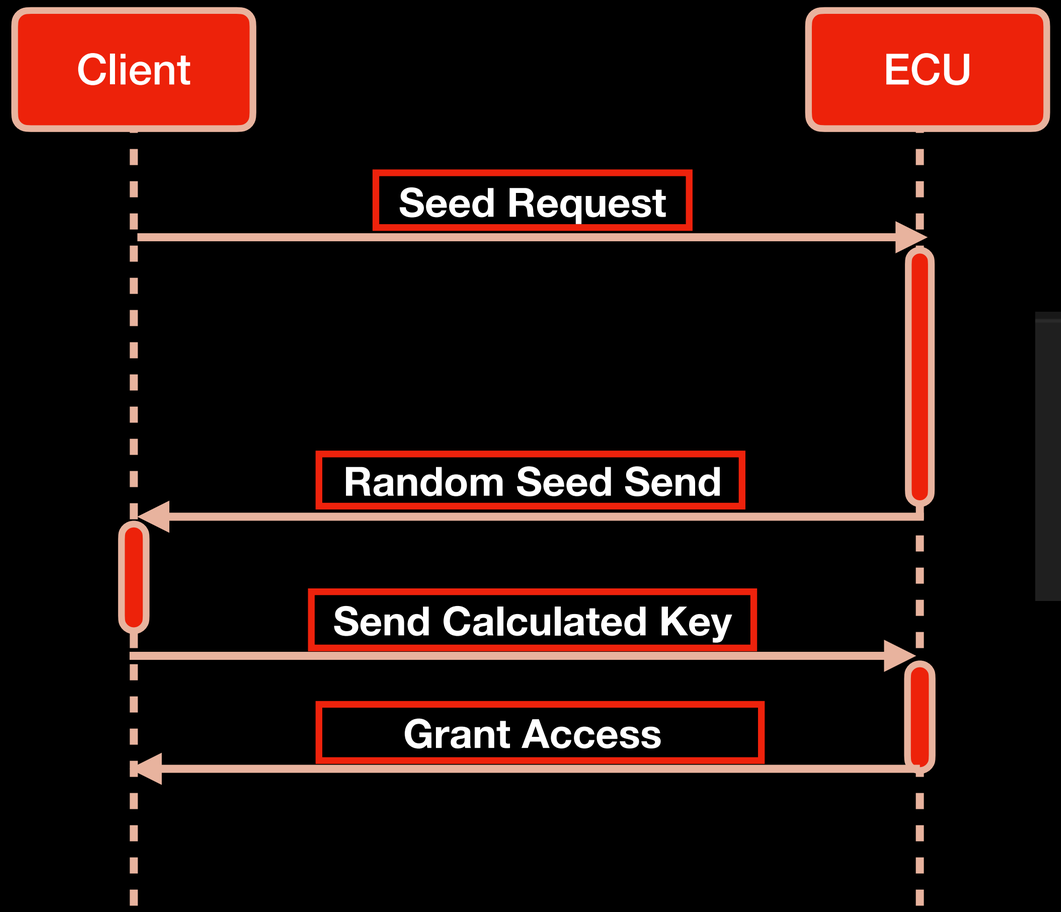
Use Case 1: The path to Game Over



Use Case 1: The path to Game Over

- Loosely developed requirements, can result in:
  1. Sloppy authentication implementations
  2. Weak sources of randomness
  3. **Backdoors implemented outside of the scope of the requirements**
     - e.g. Extra security access sub-service, with extremely weak security

Backdoors, backdoors, backdoors...

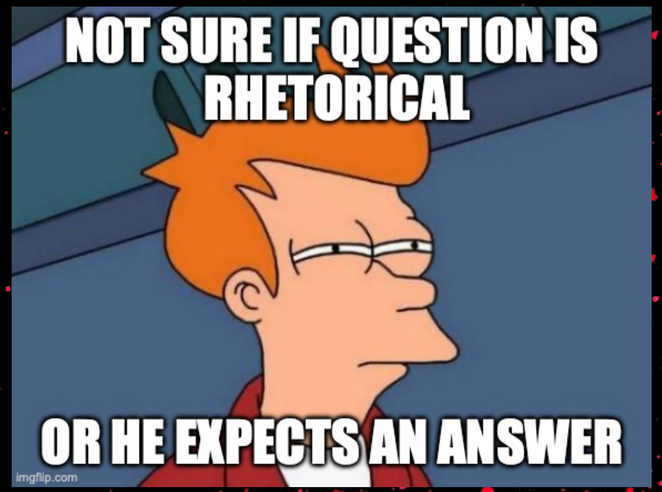



```
can0        760   [8]  02 27 70 00 00 00 00 80
can0        761   [8]  06 67 71 05 23 AA 12 00
can0        760   [8]  06 27 72 00 00 00 00 00
can0        761   [8]  02 67 73 00 00 00 00 00
```

Backdoors

Summary

- While Tier 1 supplied components might follow the OEMs cybersecurity requirements, that doesn't mean we only need to test *"by the book"*
- In most cases:
  - Several misconfigurations existing **outside of the CyberSec Requirements**
  - **OEM doesn't know** (or doesn't want us to know)
  - **Tier 1's did not inform the OEM**
- But why … ?



Solution...

- *For the OEM*: Build more strict Cyber Security Requirements

- *For the pentest suppliers / researchers:*
  - Build a **robust methodology** which will cover a realistic amount of testcases
  - Don’t build it solely based on requirements
  - **Educate** the client (OEM, Tier 1 or anyone applicable)

ΚΕΦΑΛΑΙΟ 2

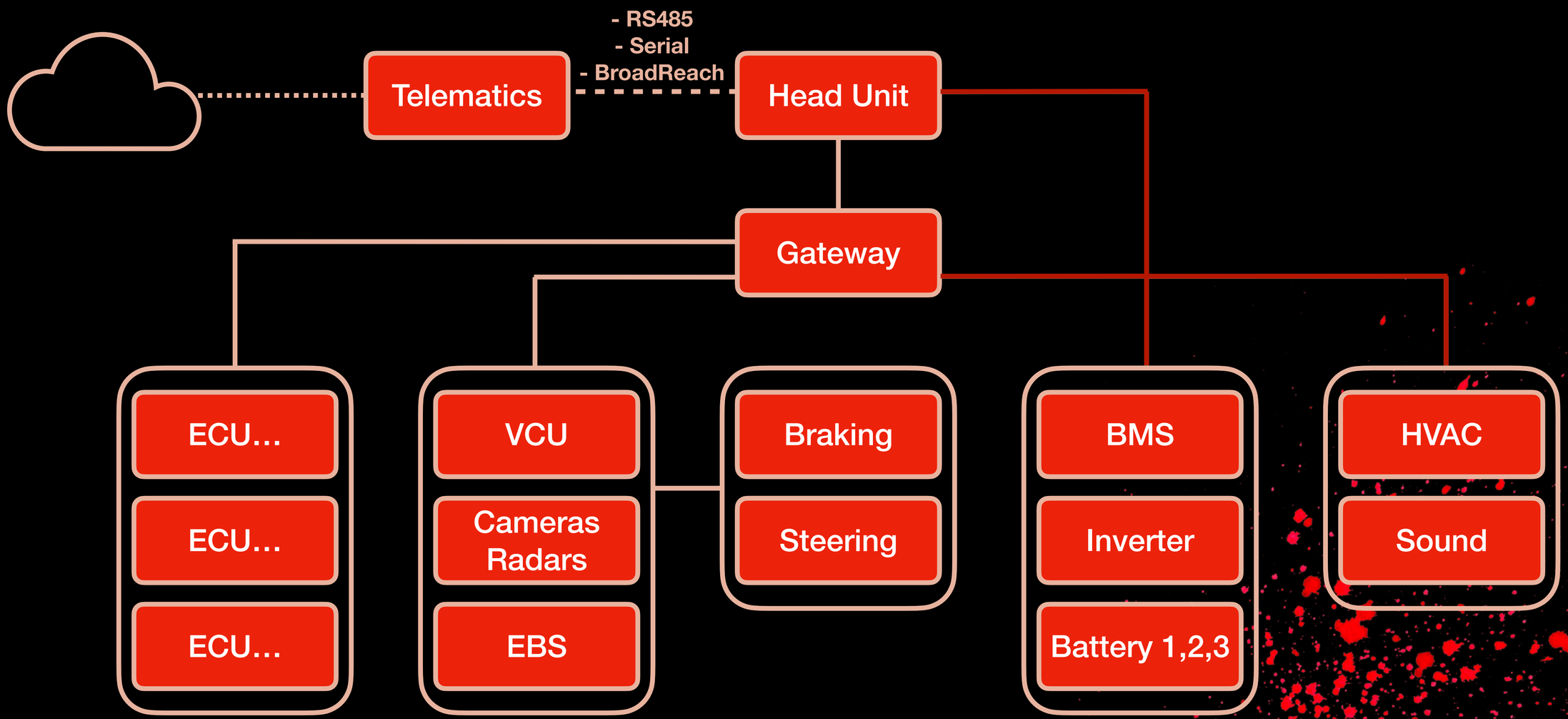
TELEMATICS

A story of how bad architecture can lead to devastating results.

Telematics and Connectivity

- Almost no vehicles ship anymore without a telematics unit
- Secure update procedures became a necessity (they are part of the recent regulations)
- Several running services, including remote vehicle management in most cases (e.g. door unlock, vehicle conditioning, etc.)
- ***TLDR**: Please consider the applicable connectivity while designing the architecture*

Use Case II: The supercar



The tale of the buses

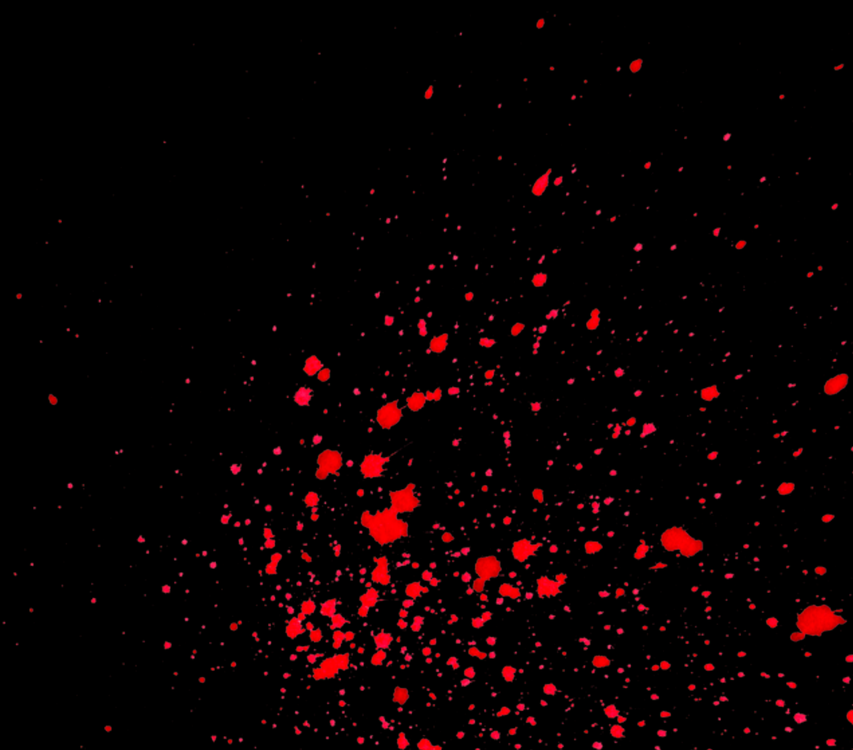
- Interconnected buses can act as a stepping stone in safety critical attacks
- Gateways are commonly used for message filtering and routing
- Bypassing the gateway, results in direct interception and communication of CAN[1] messages
- At this point, target ECUs existing on those buses can be analysed, enumerated, and exploited without the assumed restrictions

1. Or other applicable interfaces and communication protocols

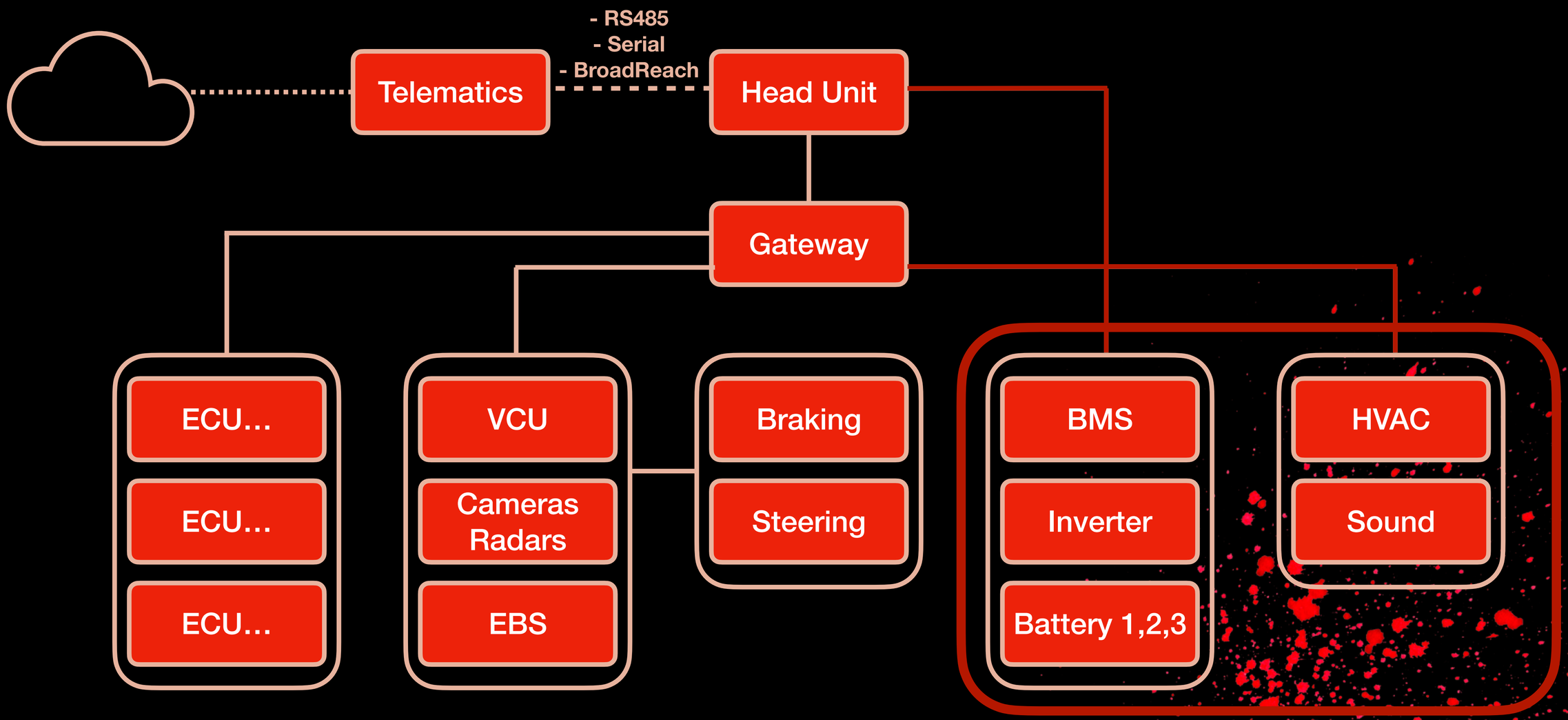
Use Case II: The supercat

- Remember UDS?
- Service 0x11 - ECUReset
- 90% of target ECUs, come with no authentication or pre-condition for hard ECUResets
- This means that any ECU which allows execution of this service, can be immediately interrupted by hard reseting it

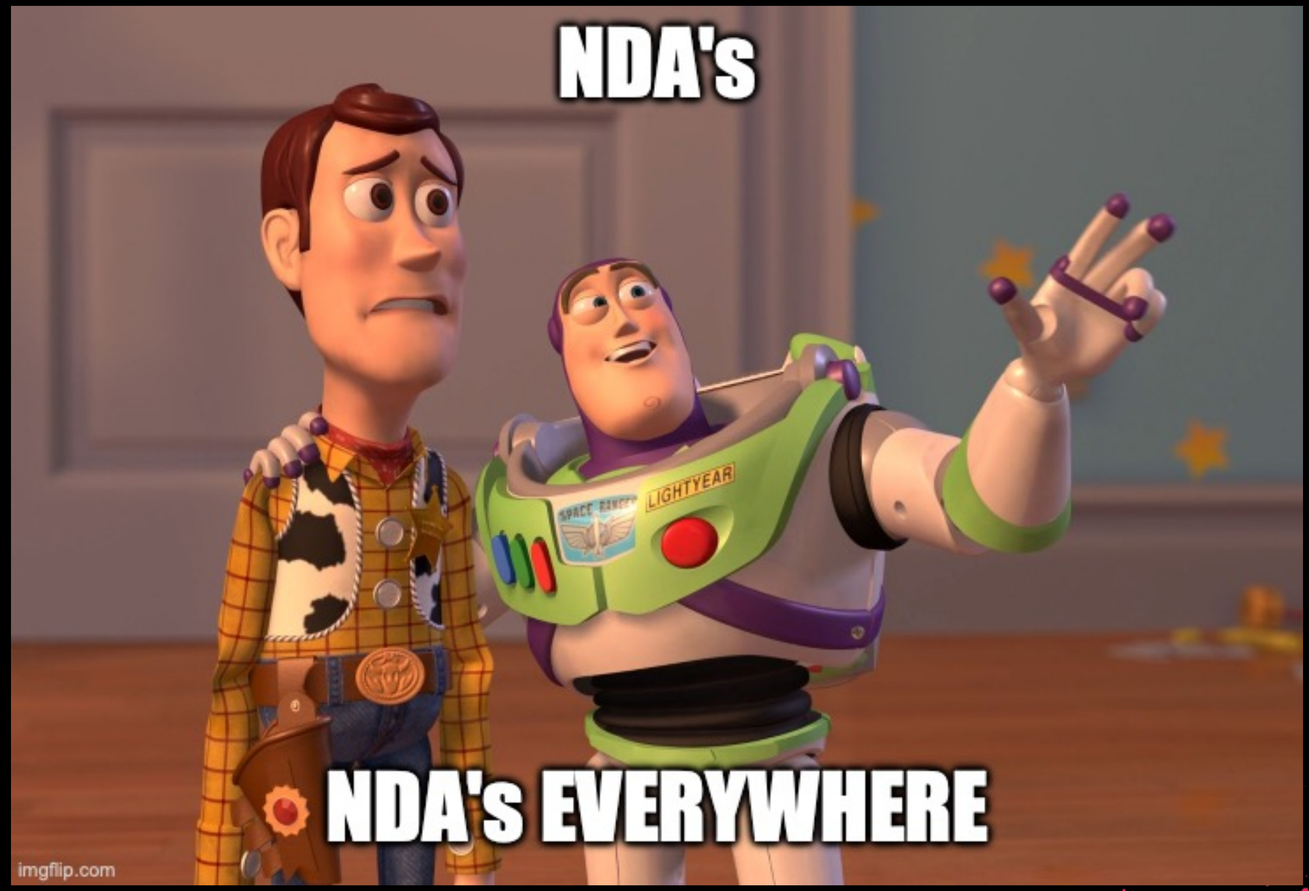
Outcome?



Use Case II: The supercar



Use Case II: The supercar




FIXED
VMware Fusion File Edit View Virtual Machine Window Help
Kali Linux
Sat 10:42
13:42
1 2 3 4
File Actions Edit View Help
cr0wtom@kali-m1: ~/Tools/caringcaribou/tool
(cr0wtom㉿kali-m1)-[~/Tools/caringcaribou/tool]
$ candump can0,705:7ff
Trash
File System
output

The tale of the buses

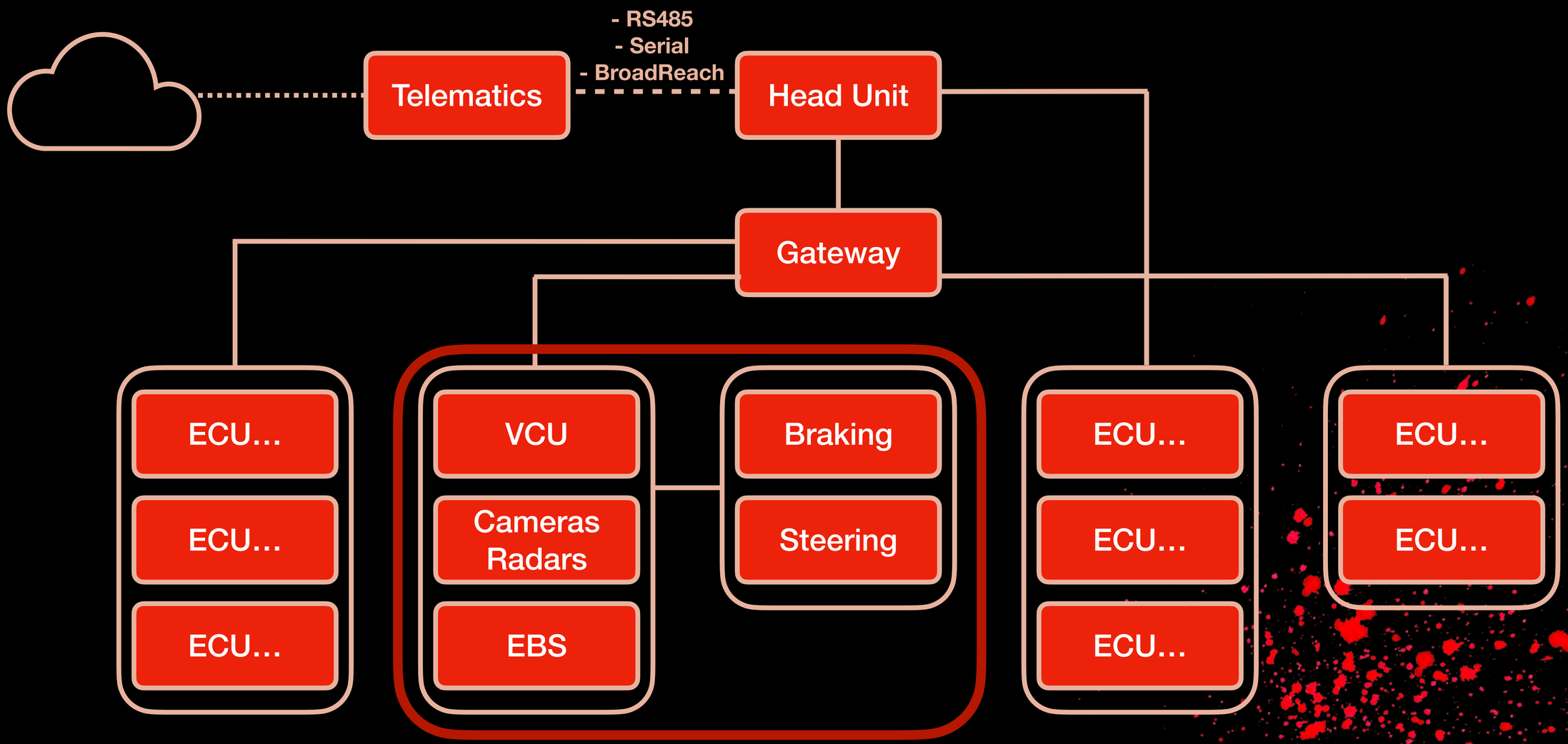
- Automotive architecture, understandably gets more complicated
- More internal buses need to be introduced for proper segmentation of safety critical and non-critical components
- Better design should be considered from the first steps of production

ΚΕΦΑΛΑΙΟ 3

DESIGN CHOICES

...

ECU Reset returns...



ECU Reset returns...

```
└─$ candump can0 | egrep "30F1|F130"
  can0  18DA30F1   [3]  02 11 01
  can0  18DAF130   [8]  02 51 01 FF FF FF FF FF
  can0  18DA30F1   [3]  02 11 01
  can0  18DAF130   [8]  02 51 01 FF FF FF FF FF
```

ECU Reset returns...

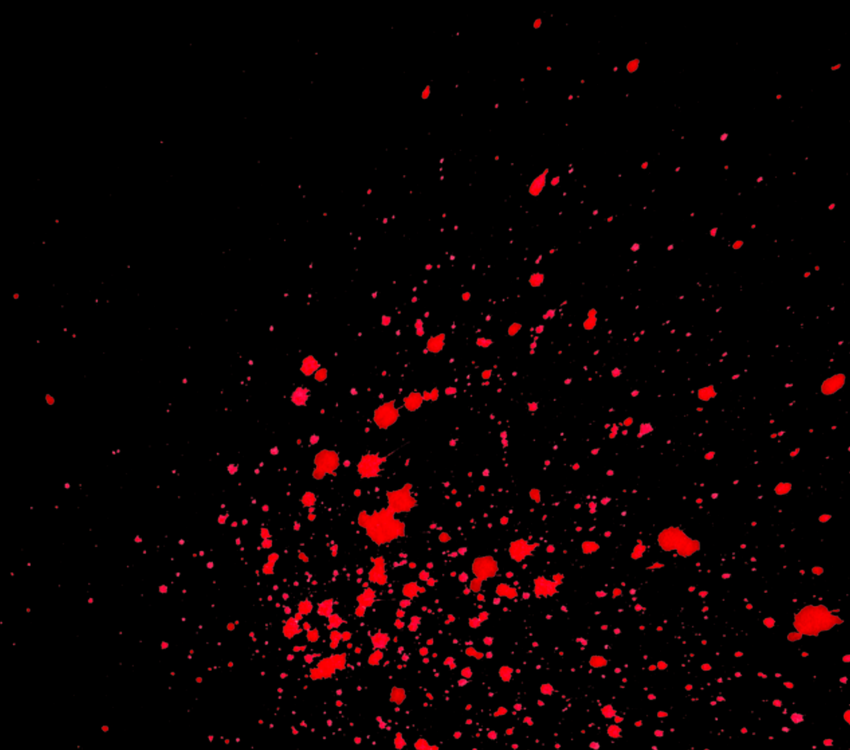
Is it Hard....

- Other than architecture, there are several points during the design of a vehicle that need to be considered

- The specific physical space of the components, wiring and connections is a - multifunctional issue with several restrictions

- Manufacturers need to make sure that everything is secure, isolated and inaccessible to external users

What if it’s not?



External Points of Connectivity

- Several external components are directly connected to internal buses
  - e.g. radars, lidars, lights
- Recent Toyota hack proved that this can have devastating results
- Bad design choices and bad architecture are not a good combination
  - External access to internal busses is a really common “misconfiguration”

Source: https://www.thedrive.com/news/shadetree-hackers-are-stealing-cars-by-injecting-code-into-headlight-wiring


ΕΛΠΑ
ΕΠΙΠΛΑ

Source: https://www.youtube.com/watch?v=9rsIoDEERoM

External Points of Connectivity

- Separates direct current into specified components
- Several reasons behind the inclusion of those isolators
  - Both security and safety related
- Encountered during pentests mainly on buses, trucks and boats
- Should it be accessible in an unrestricted manner though … ?

Source: Alibaba

ΚΕΦΑΛΑΙΟ 4

BOOTLOADERS

A story of how the old is becoming new again.

SecureBoot

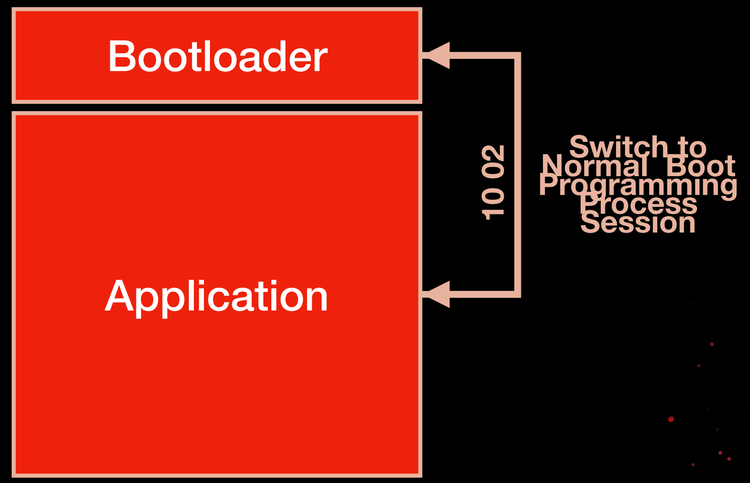
- Depending on the target architecture and system, the bootloader is implemented accordingly
- ECU bootloaders are usually used for:
  - Re-programming
  - Initialisation of application section of memory
  - Read and write *from* and *to* sensitive parts of memory
- **Understandably** security measures must be taken to restrict unauthenticated access to the bootloader

Unfortunately, not so many manufacturers restrict access to the bootloader…

The reality

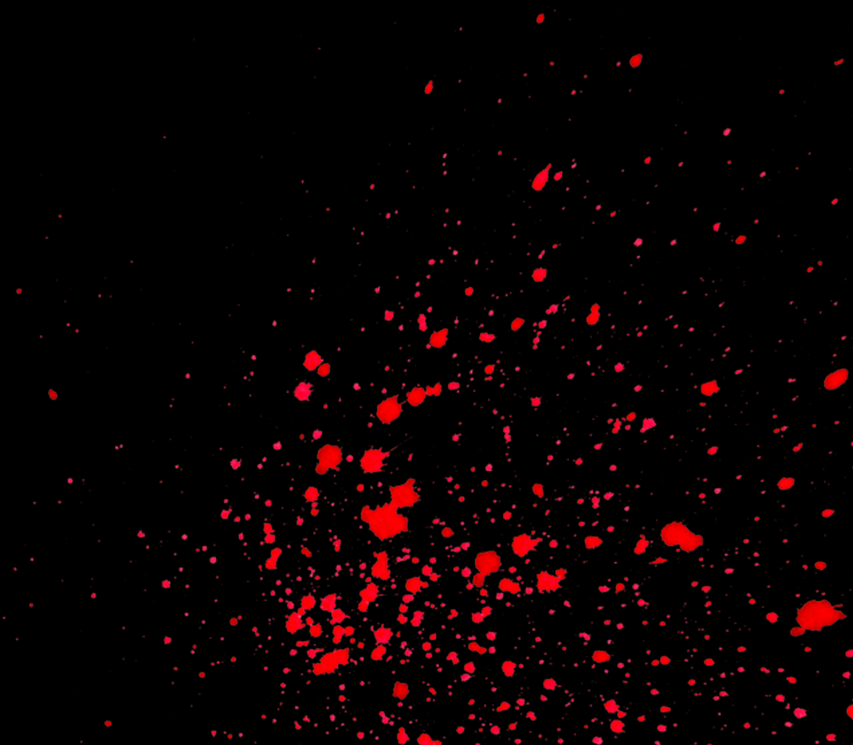
- Even if we can obtain access to the bootloader, sensitive services are restricted to unauthenticated users
  - Request Download (0x34) / Request Upload (0x35)
  - Transfer Data (0x36)
- Most of the ECUs use the “bootloader” section (or UDS programming session) to perform secure update of the target
- Authentication sub-service for re-programming is different from the sub-service used in application mode for other restricted tasks

The reality

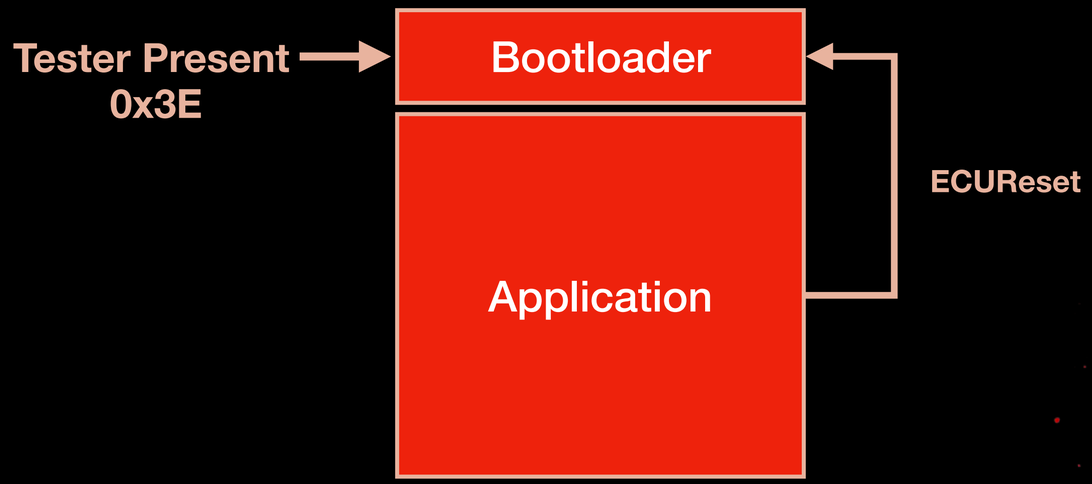

Bootloader
Application
10 02
Switch to Normal Boot Programming Process Session

The hard truth

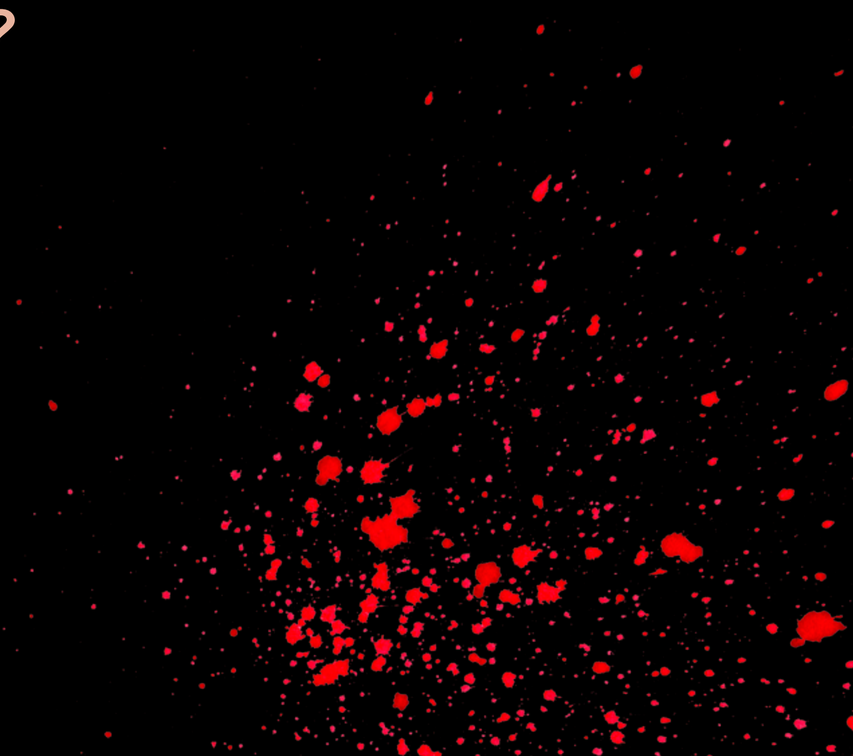
- UDS Diagnostic Session Control for Programming session (10 02) is most of the times accessible to unauthenticated users
- What happens if it’s not?
- Remember ECUReset?



The hard truth

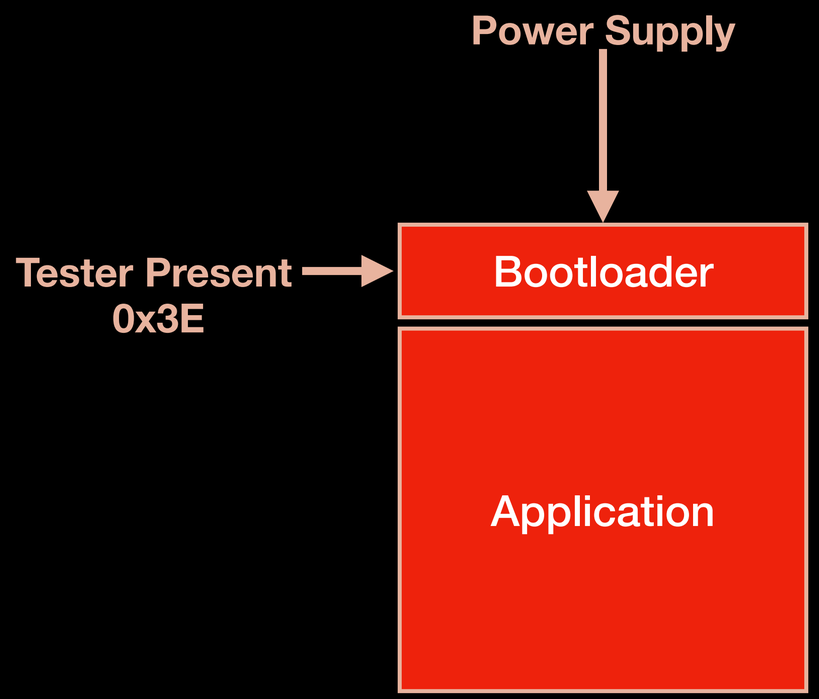


ECUReset restricted, you say?



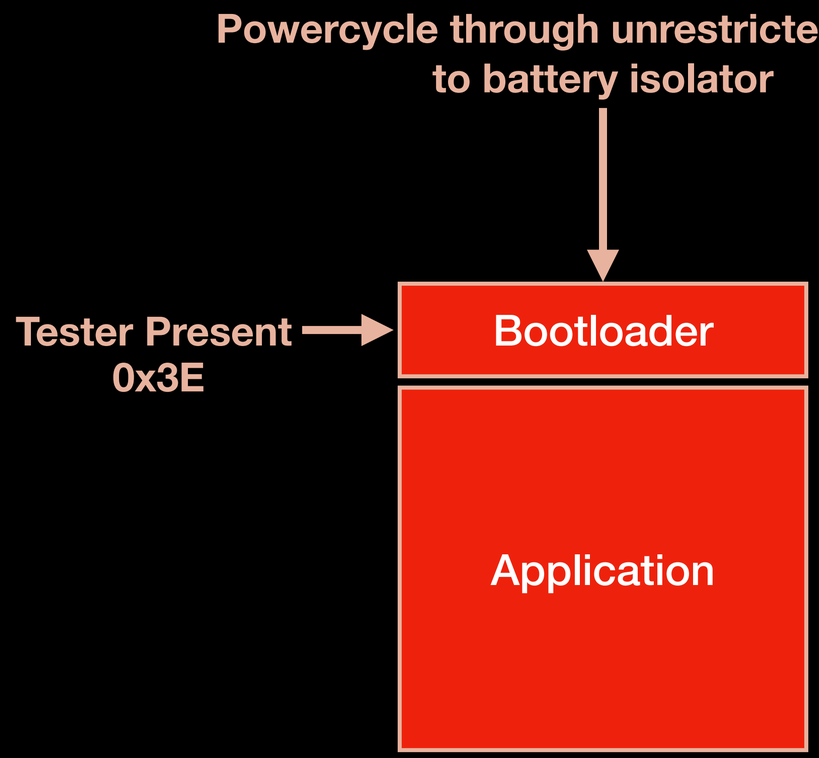

I SEE NO PROBLEM
imgflip.com

The hard truth



The hard truth

The hard truth



Bypasses in front of your eyes

- As mentioned, battery isolator can be used to clear errors from ECUs
- ECUs are mainly powered by the internal 12V battery
  - In EVs, from the AC Inverter, which is supplied by the vehicles batteries
- Isolating the power source, technically turns off the ECUs
- By supplying power again, we initiate the boot process and everything that comes after that

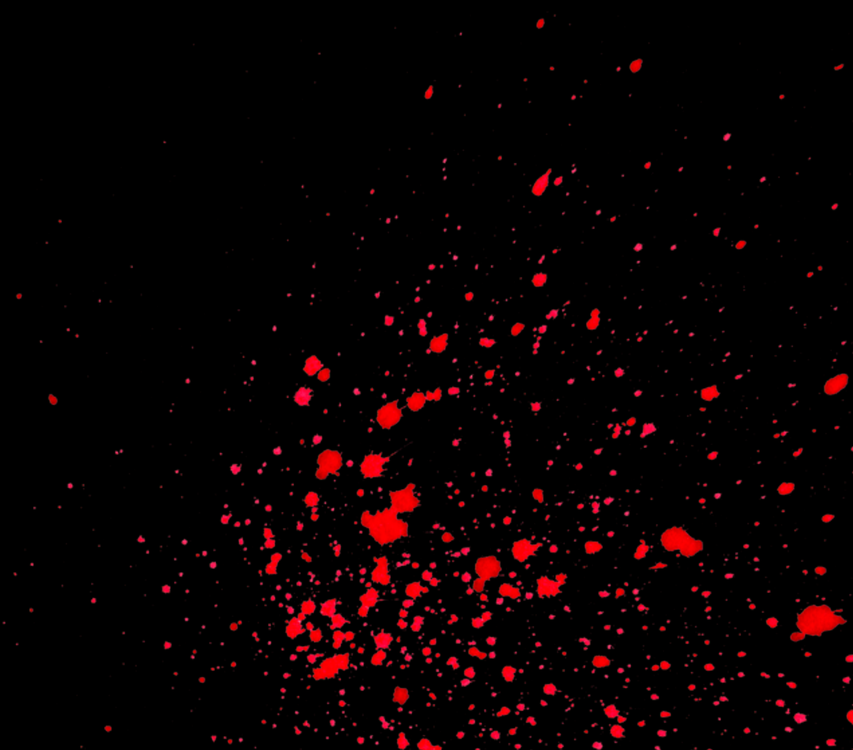
What about the hidden bypasses...

- TROOPERS22 - UDS Fuzzing and the Path to Game Over

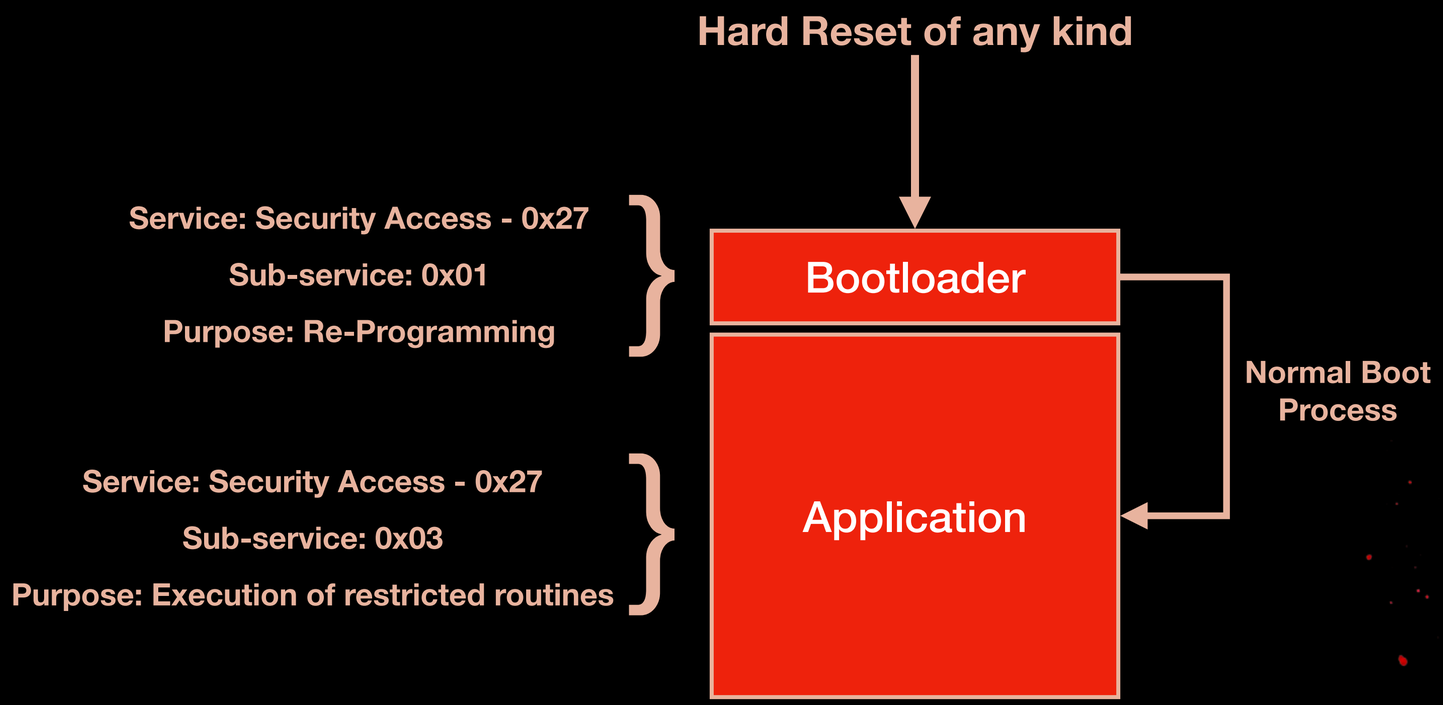
- Security access seed randomness based on system clock and old vulnerabilities becoming new again

- Manufacturers start realising and mitigating this issue
  - Especially big OEMs and Tier 1s

But did they actually realise?



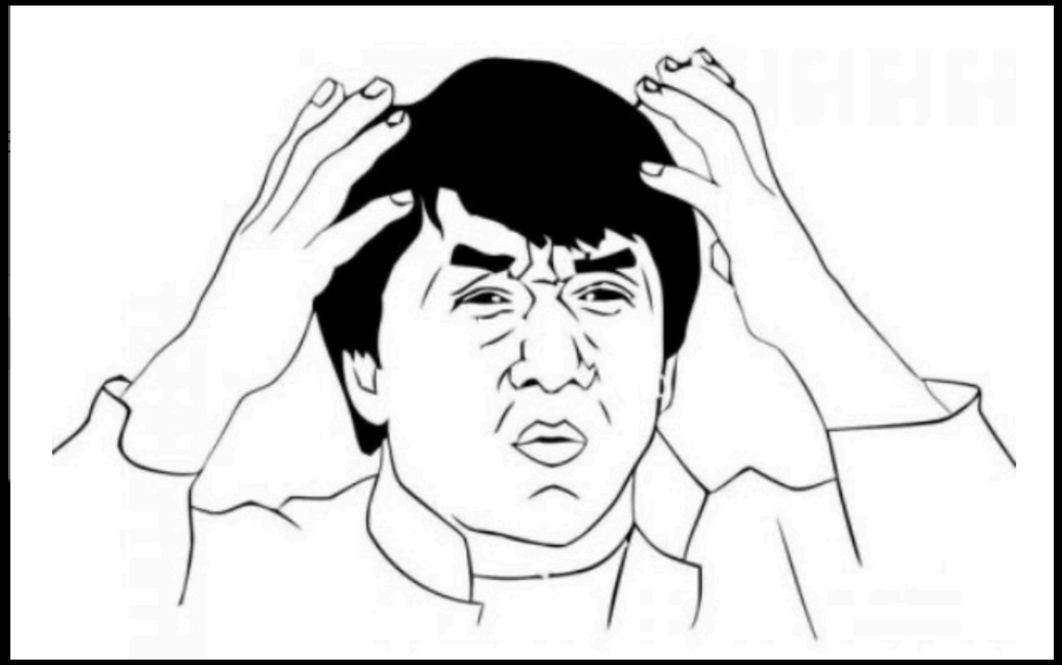
The Hard Truth



Seed Source of Randomness:

System Clock HSM

The Hard Truth



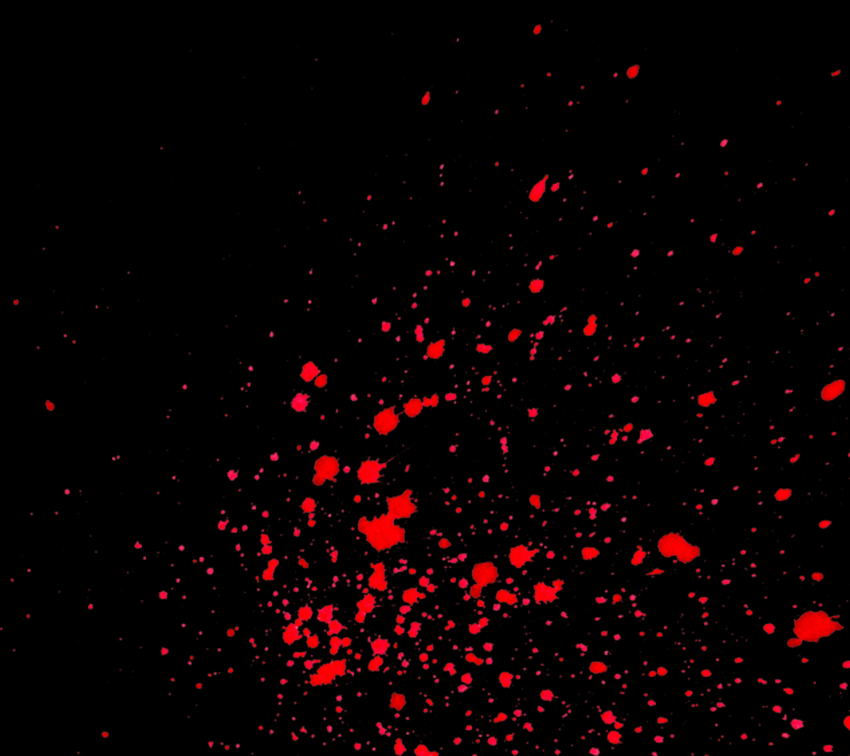
The Hard Truth

- Things which are protected on the application layer, can be usually unprotected on the bootloader
  - Forgotten?
  - Separate development teams?
  - Externally sourced, so different code base?
- It’s worth testing all available services and sub-services, under all available layers

ΚΕΦΑΛΑΙΟ 5

SEEDS^2

The story of the duplicates once again.



UDS Fuzzing

- CaringCaribou and seed_randomness_fuzzer module
- Mostly modular with several developed modules
- Main advantage is the ease of use
- Main disadvantage is the inability to easily alter the low level layers of the project

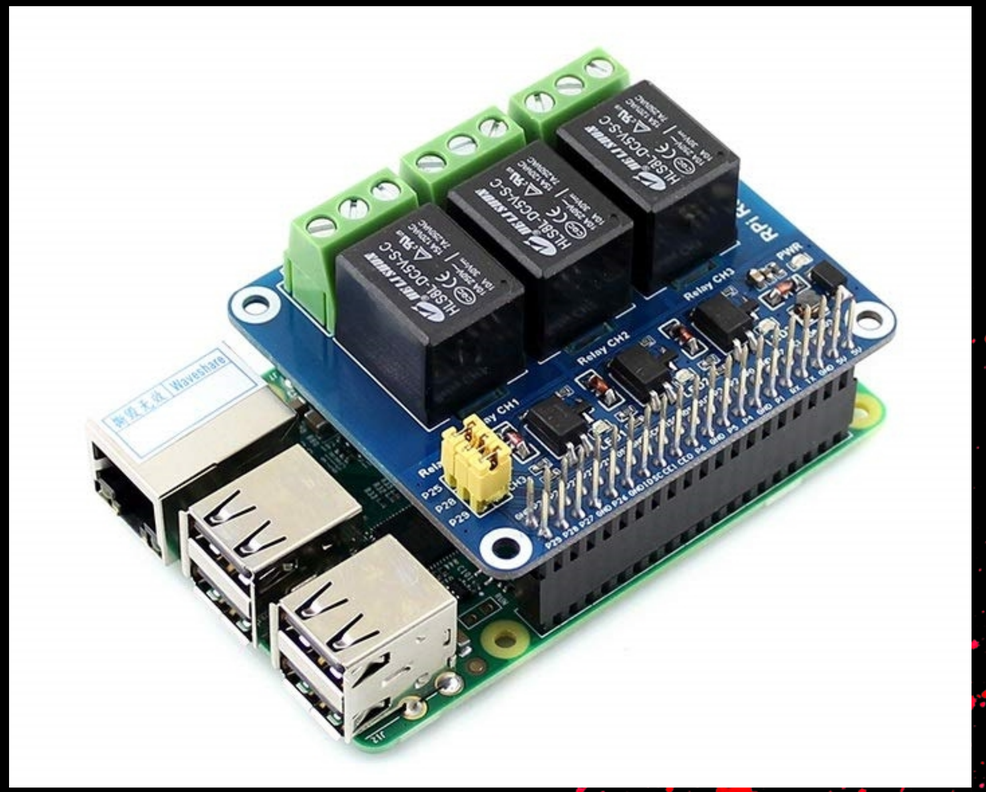
Use Case IV: Hydrogen Combustion ATV

- Safety critical components need to be easily isolated from batteries

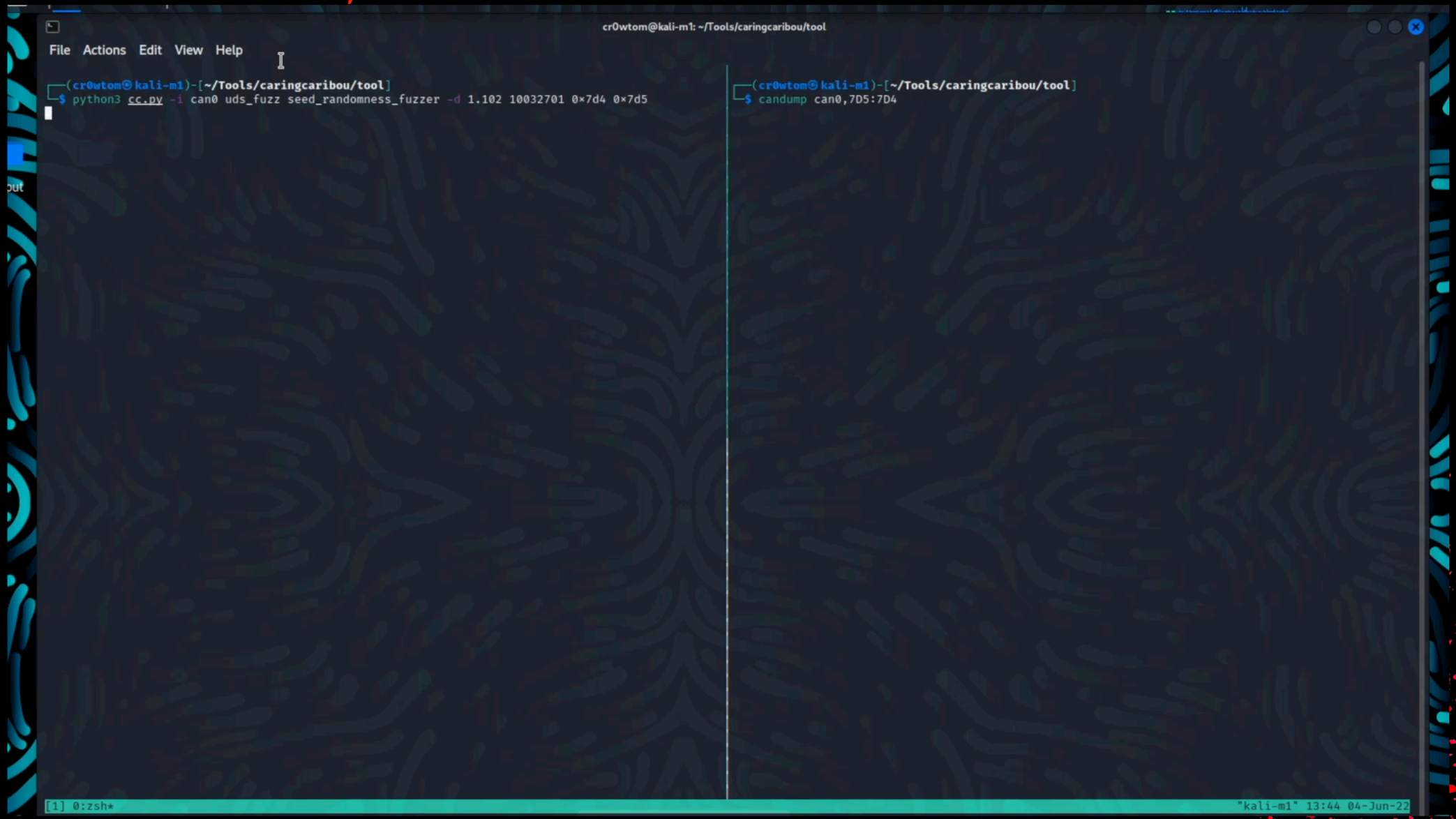
- After enumerating:
  - ECUReset is not available in any diagnostic session
  - The available Security Access is not backdoored or vulnerable to weak seed randomness
  - No other misconfigurations discovered during initial enumeration

Use Case IV: Hydrogen Combustion ATV

+



Use Case IV: Hydrogen Combustion ATV



Results

- Having a relay as the source of the powercycle, can result in more accurate results from last year

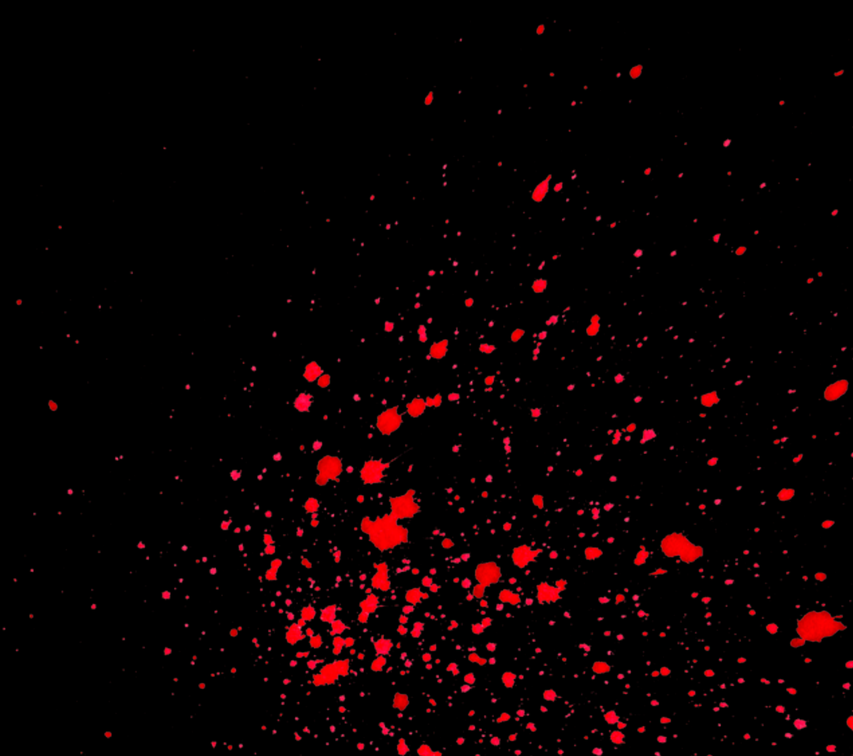
- With around 20% of duplicate seeds out of 1k samples, we can be relatively confident that the target is sourcing the randomness on the system clock

- In most cases, it’s easier to intercept a seed and pre-calculated key pair from the bootloader accessible sub-session than from the application layer
  - Used for re-programming purposes

ΚΕΦΑΛΑΙΟ 6

XCP

From chaos in diagnostics to calibration



Enough about UDS…

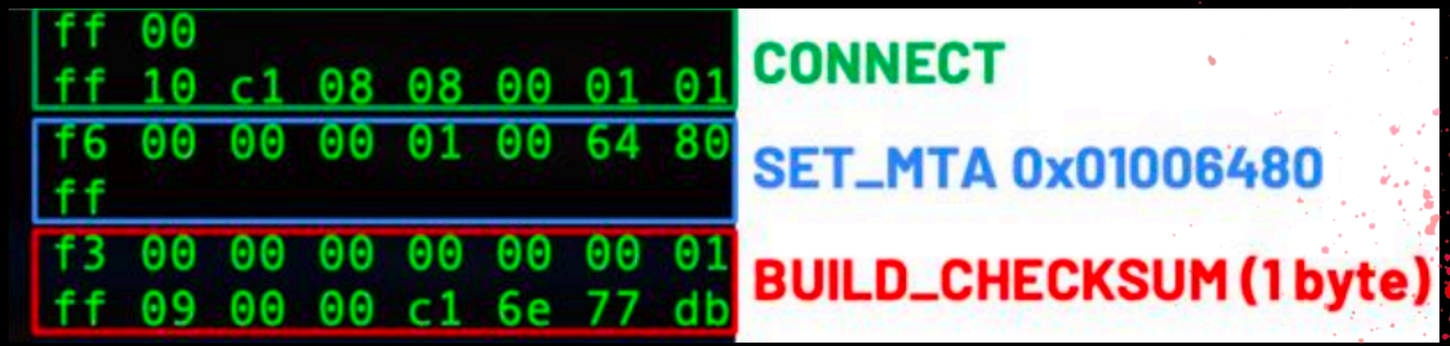
- Universal Measurement and Calibration Protocol (XCP)
  - Connecting calibration systems to ECUs
  - Enables read and write access to variables and memory contents
  - Supports programming of flash memory
  - It also supports a seed/key type of security access, but…

Interesting XCP services

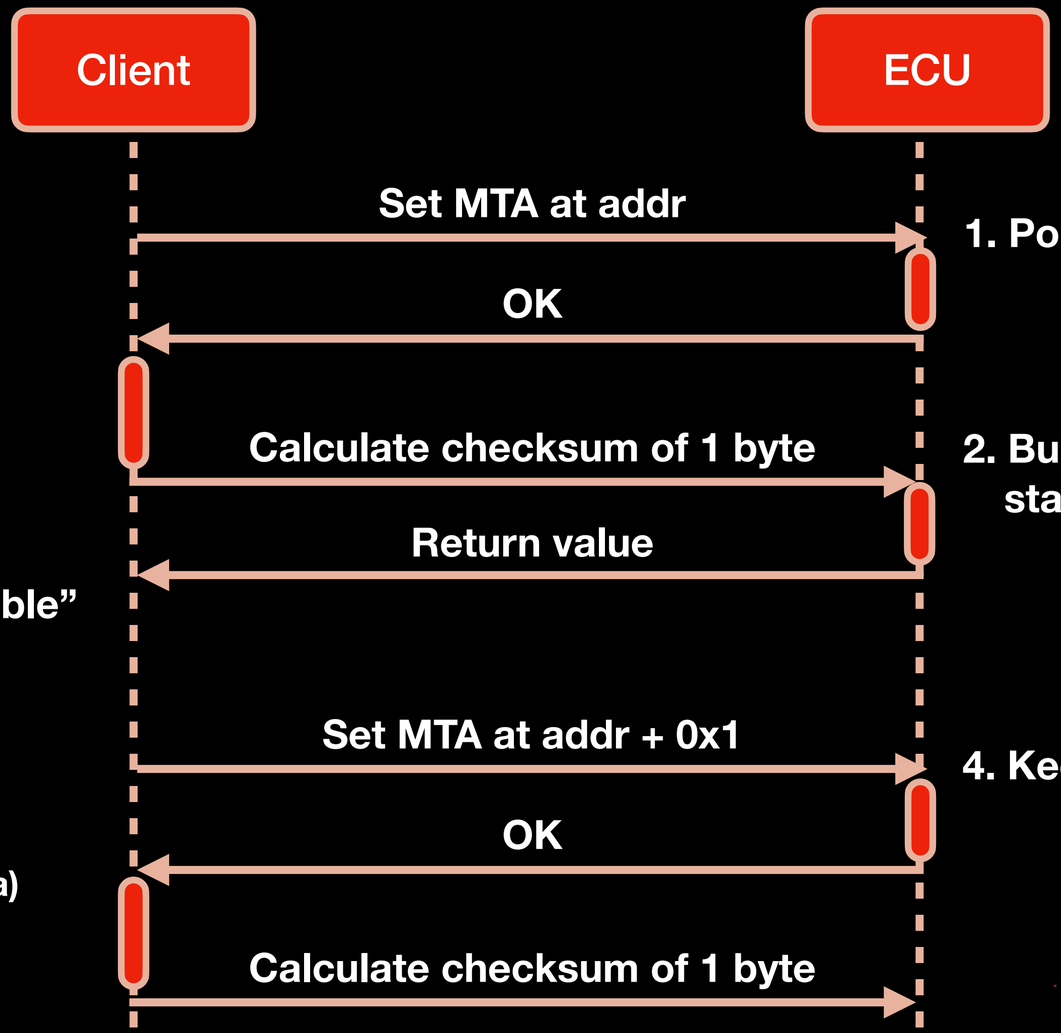
Command	PID
CONNECT	0xFF
DISCONNECT	0xFE
GET_STATUS	0xFD
SYNCH	0xFC
GET_COMM_MODE_INFO	0xFB
GET_ID	0xFA
SET_REQUEST	0xF9
GET_SEED	0xF8
UNLOCK	0xF7
SET_MTA	0xF6
UPLOAD	0xF5
SHORT_UPLOAD	0xF4
BUILD_CHECKSUM	0xF3
TRANSPORT_LAYER_CMD	0xF2
USER_CMD	0xF1
SHORT_DOWNLOAD	0xED
DOWNLOAD	0xF0

Interesting XCP services

- CRC32 (4-byte output)
- 12 typical CRC32 algorithms (*crccalc*)
- XCP typically follows AUTOSAR standard
- Applicable to custom implementations, with some more effort required



Dumping memory via checksum



1. Point to specific memory address

2. Build checksum of 1 byte starting at specified address

3. Get contents of memory address from CRC “rainbow table”

4. Keep going…

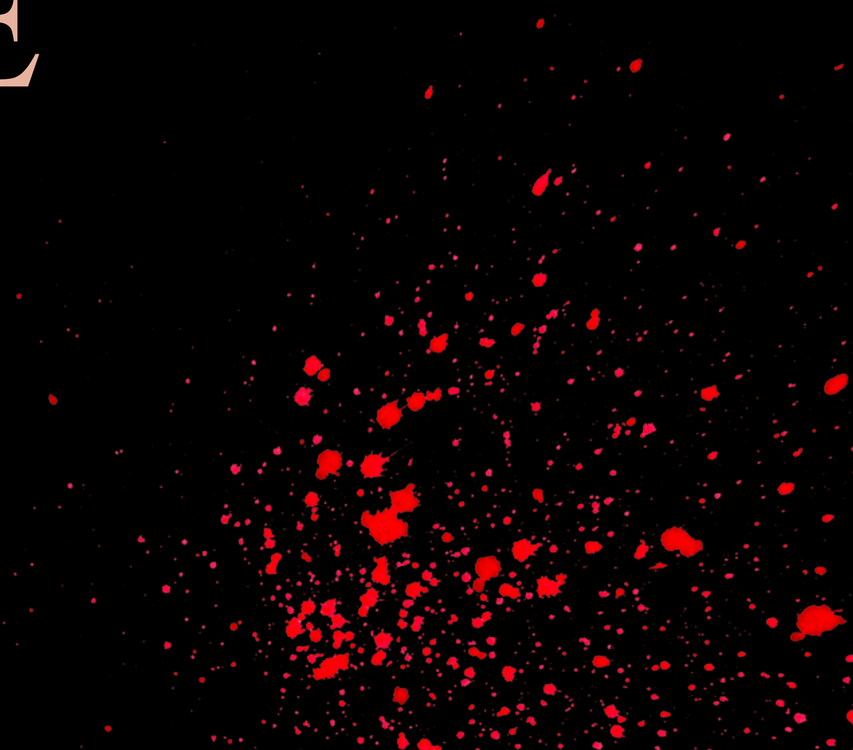
(In collaboration with Diego Ledda)

Dumping memory via checksum

```
[*] Running the crc_test module
0x18
0x21
0x6
0xe0
```

```
01006480 18 21 06 e0     e_stwu      r1,local_20(r1)
01006484 00 80           se_mflr     r0
```

EPILOGUE



For the community

- While CC might not be the best tool out there, it can help newcomers start
  - A project which also helped us start

- Several new automations from my side to help the project move forward:
  - Write Data by Identifier fuzzer
  - Auto module, for complete automation of the UDS enumeration
  - Support for new CAN interfaces with proprietary drivers under python-can
  - Different padding (and no padding) support

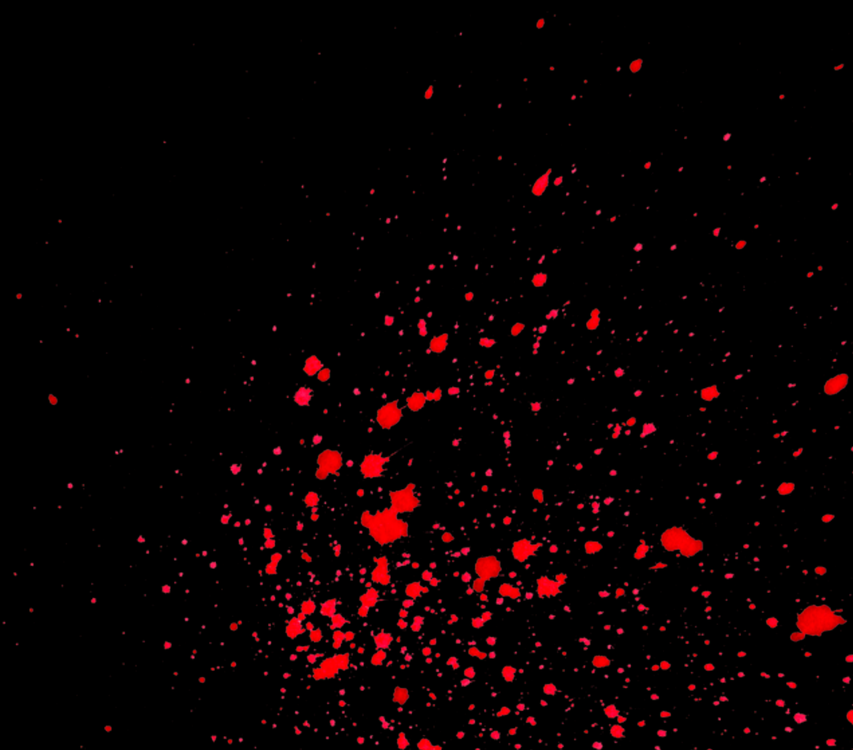
Pentesting VS Research

- While reversing firmwares and getting hardware access is fun, scope is usually extremely limited
- We are tasked to find efficient ways to perform more testing, in a result driven environment
- Automation of tasks is usually the main priority of the testing
- Direct result is the extension of our methodology and testcases

Clients VS Pentesters

- Automotive clients need to understand our methodology and testcases
- Abstract results are not always a good way forward
- Education is the key to a better collaboration with developers as there is no clear standard and methodology available online, in contrast to mature industries like web, infra, API, etc.

Do they even care?



THE END

THANK YOU FOR YOUR ATTENTION

Thomas Sermpinis | André Maia
cr0wsplace.com