Self driving cars and not so autonomous security

Nicolas Massaviol
Cedric Buxin

Agenda

- What is a modern car nowadays ?

Finding vulnerabilities

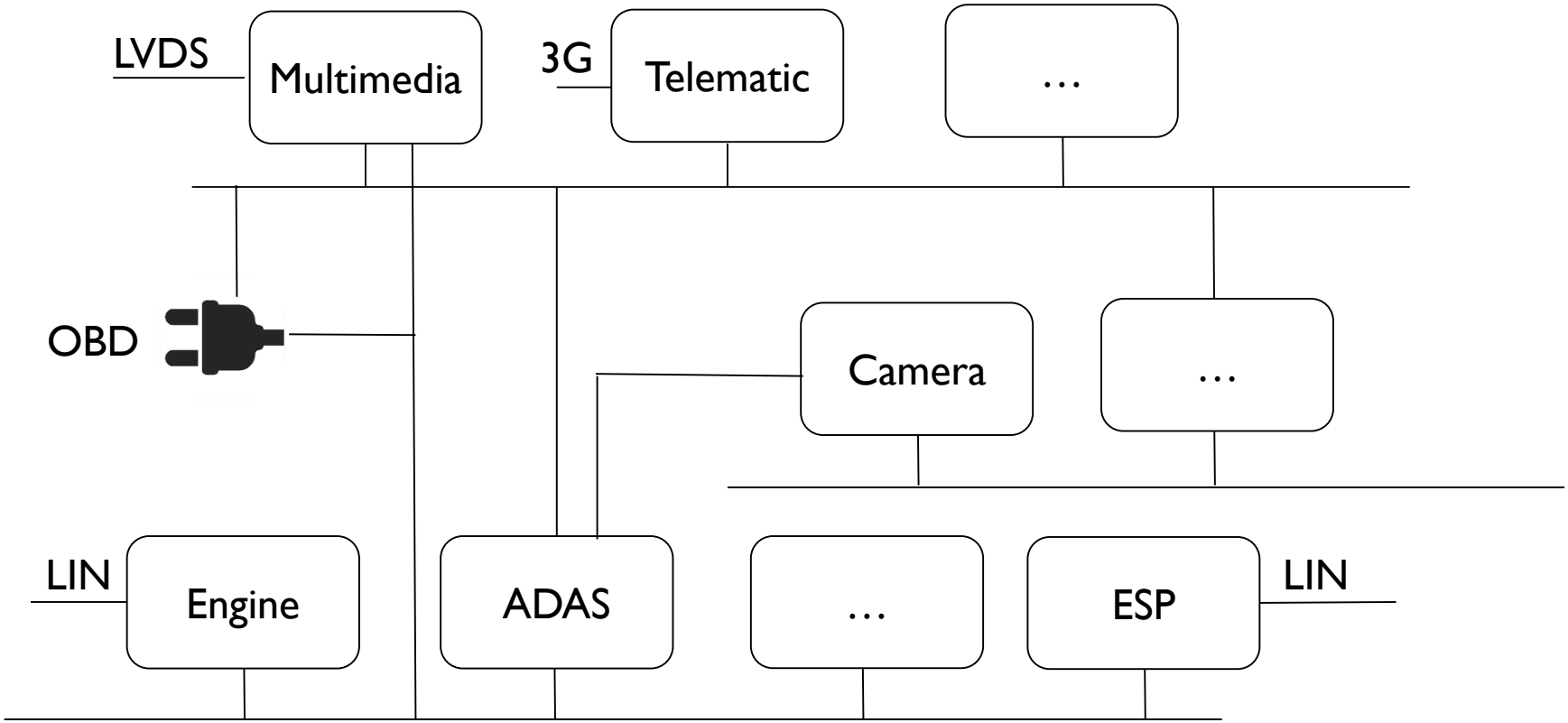
Or not…

Finding backdoors

Autonomous vehicle

toucan system

What is a modern car nowadays ?

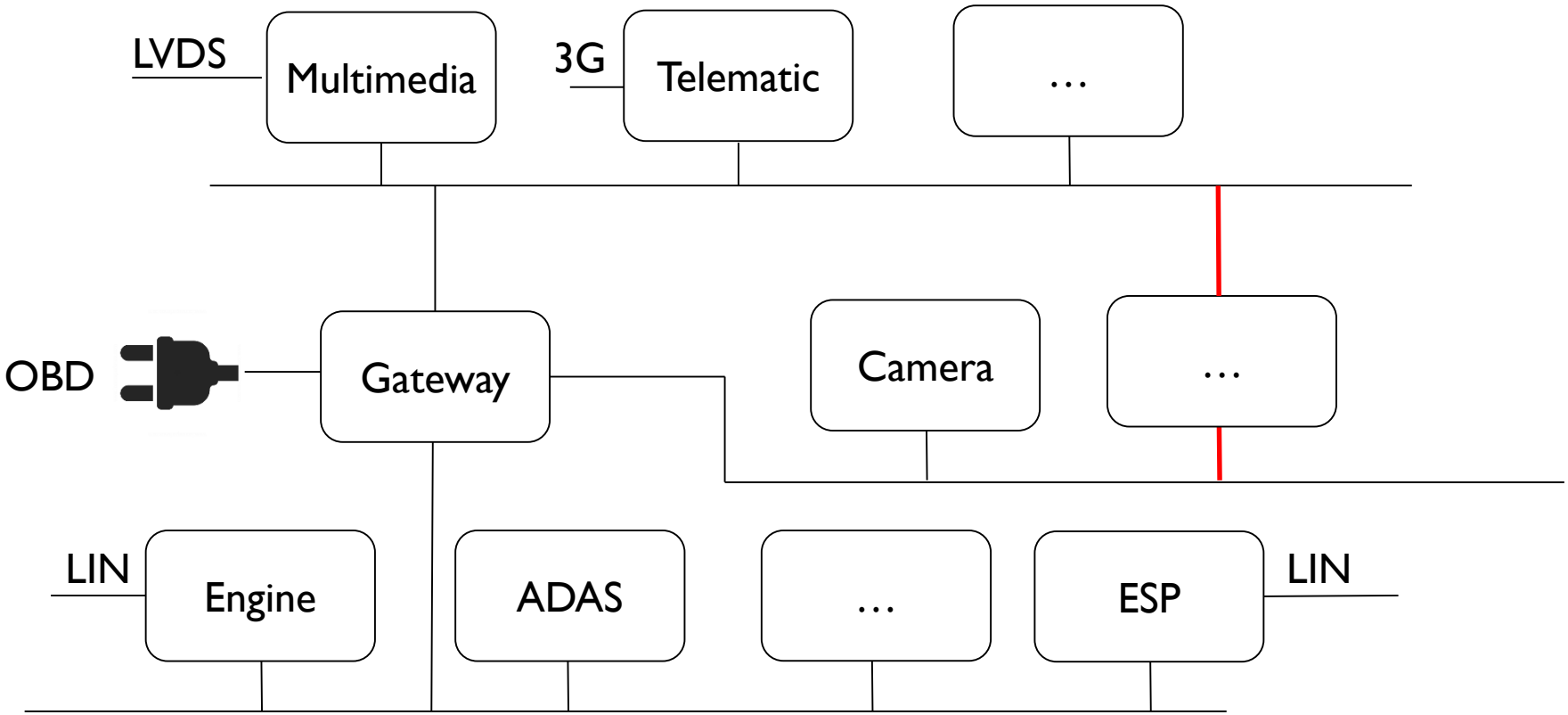


ECU

Electronic control unit : ~30

toucan system

What is a modern car nowadays ?

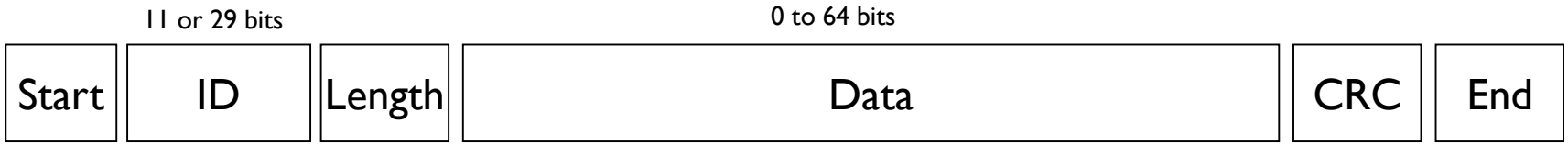


ECU

Electronic control unit : ~30

toucan system

What is a modern car nowadays ?



Ids are not adresses. One ECU : many IDs

e.g. 0x1a9 engine frame :

- 3bits for engine state (turned off / on, turning off, …)
- 8 bits for RPM
- 5 bits reserved

Completely proprietary / opaque. Changes between OEMs, make and model.

What is a modern car nowadays ?

2 kinds of ECUs are interesting from a security point of view

- Highly exposed

Multimedia system, telematic unit, V2X, …

- Highly privileged : Accelerate / brake / steer

Engine, brakes, advanced driver assistance system (ADAS), ESP, …

Agenda

What is a modern car nowadays ?

- Finding vulnerabilities

Or not

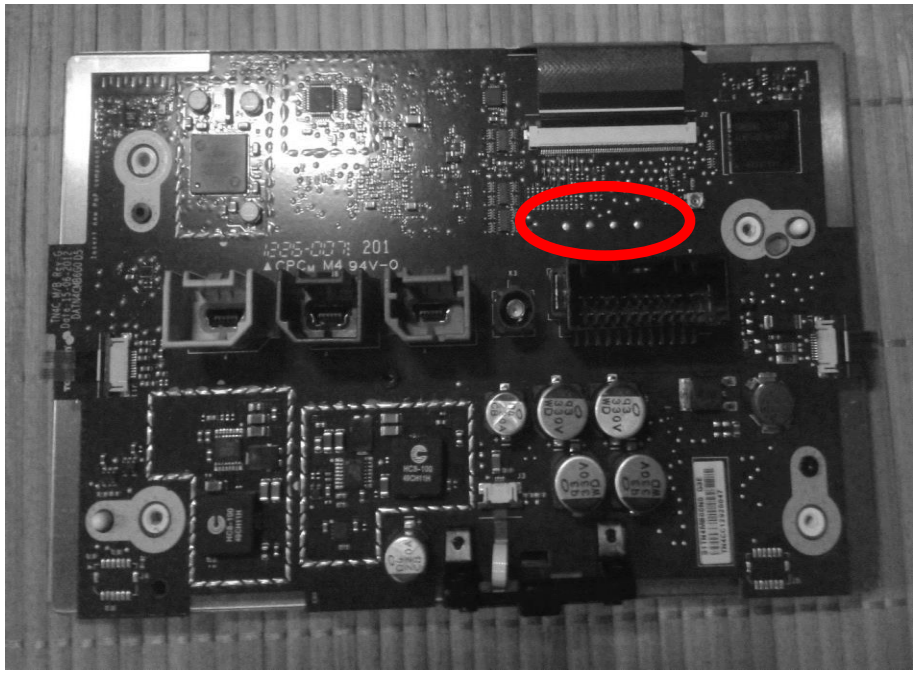
Finding backdoors

Autonomous vehicle

toucan system

Finding vulnerabilities

Debug interfaces



```
-=[ [redacted] DiagSys ]=-

Version    : strasbourg-rel-1191655-jjia
Build date : Feb 20 2013 15:45:33

--- Main menu ---
   1 - CPU
   2 - GPRS
   3 - GPS
   4 - Display
   5 - Bluetooth
   6 - Audio
   7 - Memory
   8 - CAN
   9 - RDS/TMC
  10 - Video
  11 - PSU
  12 - General
  13 - MainCon
  15 - IPOD
  16 - USB
>> 7
```

Classic UART

toucan system

Finding vulnerabilities

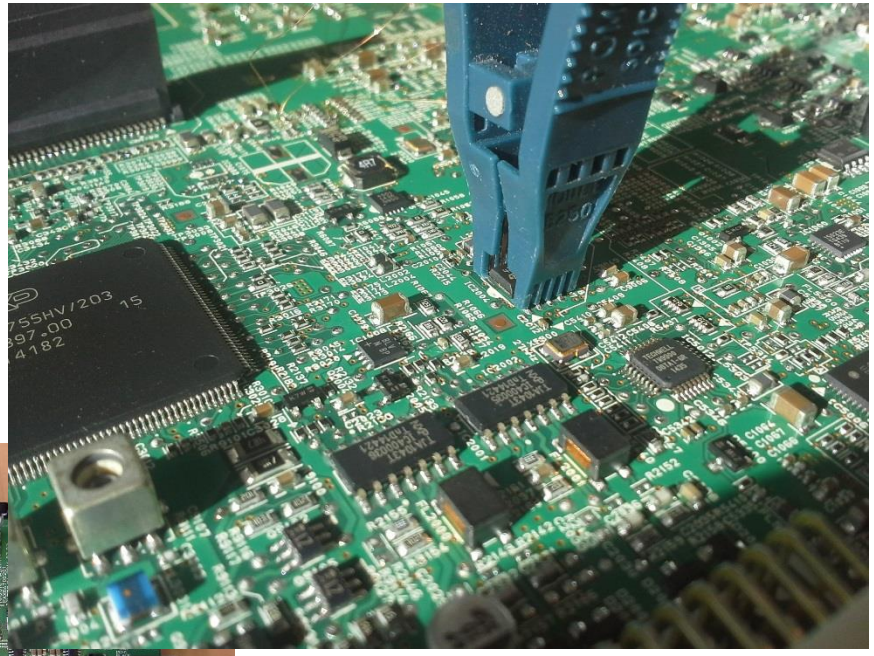
Debug interfaces : JTAG

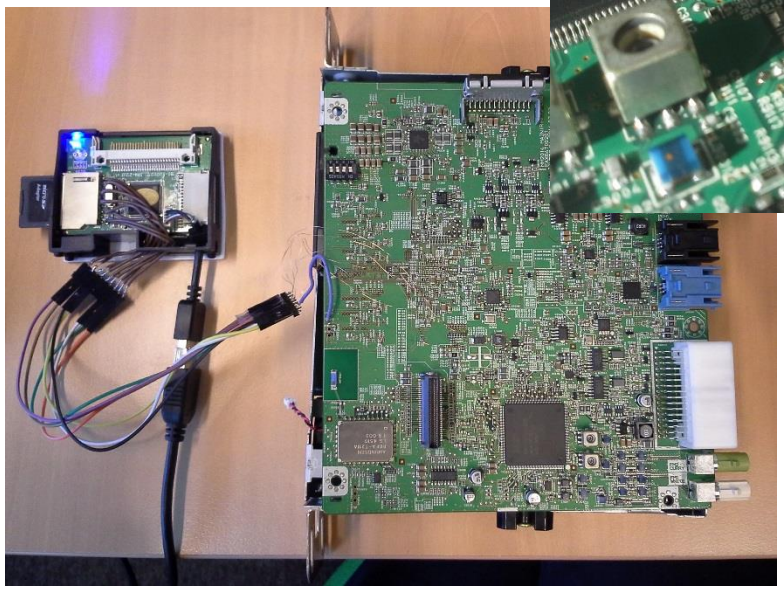
- Depends heavily on the supplier's security awareness
- Usually open
- Sometimes protected by password
- Near impossible to have it locked completely due to shared responsabilities in case of malfunctions

Finding vulnerabilities

Memory dumps

- EEPROMs
- Flash NAND / NOR
- eMMC





toucan system

Finding vulnerabilities

Update files

- Usually not plain text : some « encryption » involved
- Only one implementation using AES-256, with the key properly stored in the target (encrypted with the unique device key)
- Other cases used weak obfuscation, filesystems split, short passwords on zip files, …

Finding vulnerabilities

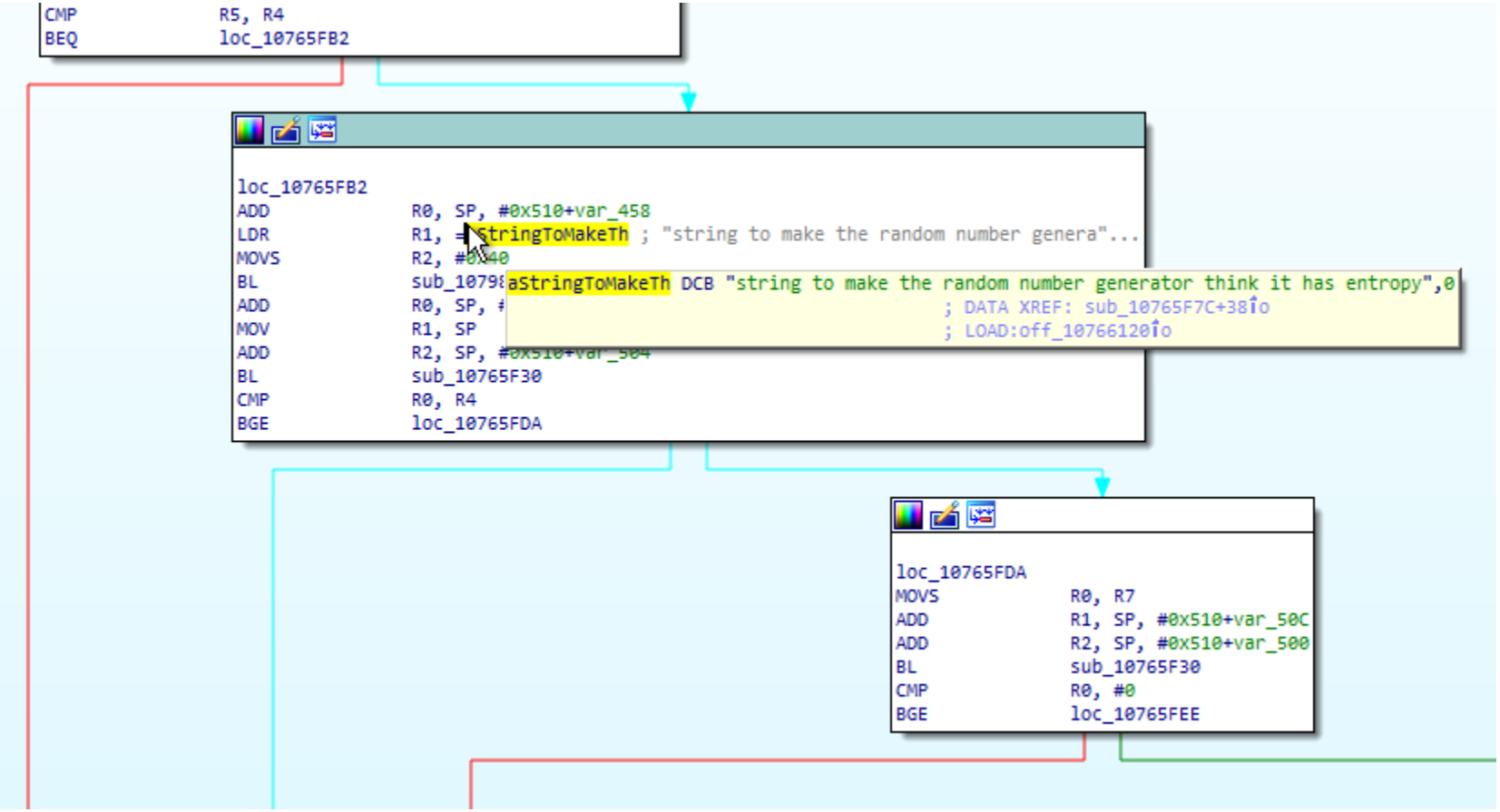
Classic reverse engineering

- ARM based systems, embedded Linux
- Very similar to smartphones

Not so classic reverse engineering

- CAN microcontrollers : v850 (ES/1/2/RH…) / 78K0 / MPC5x / dsPIC /…
- Very few tools and documentation
- 1st step is having a clean disassembly…

Finding vulnerabilities



Finding vulnerabilities

SIERRA WIRELESS | Source

HOME SEARCH COMMUNITY FORUM DEV KITS

5. Software Release Description

5.1. Release Identification

Table 6. Libraries Release Information

Component	Revision
Software Identification	2.2.2.201502061454
Date of generation	2015-02-06 14:54
OpenSSL release	1.0.1c

toucan system

Agenda

What is a modern car nowadays ?

Finding vulnerabilities

- Or not

Finding backdoors

Autonomous vehicle

toucan system

Finding vulnerabilities, or not…

- Multiple IDENTICAL parts is strongly recommended …
- Bricking ECUs is very likely when messing with update files
- Blindly fuzzing the CAN may result in serious injuries !
- Blindly fuzzing the diagnostic services WILL destroy the ECU
- What looks like the same connector may not have the same pinout (careful with power supply…) !
- What looks like an eMMC may not be readable with standard tools
- What looks like a SATA interface may not be readable with standard tools

Finding vulnerabilities, or not…

- Diagnostics functions depend on the vehicle state : wake up / speed = 0 /
- JTAG is not so standard : you will most probably end up with a nice collection of jtag probes
- IDE suites for micro controllers are competing for the least usable softwares ever designed
- Reversing architectures unsupported by IDA will waste more time than you initially expected
- The CAN is very slow…
- Raw NAND reading / writing may be unrelieable

Agenda

What is a modern car nowadays ?

Finding vulnerabilities

Or not

- Finding backdoors

Autonomous vehicle

toucan system

Finding backdoors

« Hidden » menus

Special tap sequence 

Very stealth « crafted » file on usb-stick/sdcard (touch /sdcard/.backdoor …)

Other in-vehicle sequences (not related to multimedia functions:VW…)

Finding backdoors

« Hidden » features

Special USB device using VID/PID opens up network IF with ssh access

Hardware jumpers / pull ups

ADB on special USB port not routed outside the ECU

Finding backdoors

Diagnostics

Set of CAN services (UDS for the most recent ECUs)

- 0x10 sessions
- 0x11 reset
- 0x22 / 0x2E Read / write parameters
- 0x23 / 0x3D Read / write memory by adress

Some use « authentication » : 0x27 Security Access

- Custom crypto !
- One ECU type = 1 key !
- Symmetric keys 16 bits !

Finding backdoors

9.4.5 Message flow example(s) SecurityAccess

9.4.5.1 Assumptions

For the below given message flow examples the following conditions have to be fulfilled to successfully unlock the server if it is in a “locked” state:

— sub-function to request the seed: 0x01 (requestSeed)

— sub-function to send the key: 0x02 (sendKey)

— seed of the server (2 bytes): 0x3657

— key of the server (2 bytes): 0xC9A9 (e.g. 2's complement of the seed value)

The client requests to have a response message by setting the suppressPosRspMsgIndicationBit (bit 7 of the sub-function parameter) to "FALSE" ('0').

Finding backdoors

Diagnostics

0x31 Routines = functions

- Calling convention is standard
- Some are definedby the carmakers
- Some are included by the supplier (...)

0x2F I/O controls

- Turn headlights on/off
- Blow airbag
- Trigger specific actions (depends on the ECU)

Finding backdoors

Stolen vehicle tracking

Resolution 245 July 2007:

"All new vehicles in Brazil, either out of the factory or when imported to the country, within 24 months of the passing of this resolution, in order to be sold on the domestic market, must have antitheft devices.

I - these devices must have the capacity to disable and track the vehicle […]"

Technically : SMS … no authentication planned

Software is the same for a brazilian or a european telematic unit, only configuration changes !

EU is also working on similar features.

Finding backdoors

Remote viewing

All cars equipped with cameras and connectivity are a dream come true for the surveillance business.

Law enforcement and agencies are already investigating their potential to remotely trigger visual capture of the surrounding environment and live feedback.

Finding backdoors

Remote sound capture

Emergency call is already a feature in high end cars : live sound capture over gsm when a crash is detected.

How long (if not already deployed) before the capability is silently offered to governments ?

More important : how much do you trust them to do it securely ?

Agenda

What is a modern car nowadays ?

Finding vulnerabilities

Or not…

Finding backdoors

- Autonomous vehicle

Autonomous vehicle

Level 1 : driver assistance (~2014)

Level 2 : partial automation (~2018) driver attention required

Level 3 : conditional automation (~2020) driver attention not required in some conditions

Level 4/5 : high automation / full automation (~2025)

Autonomous vehicle

Autonomous vehicle

Autonomous ➡ Connected

Remote updates

Remote navigation

Remote actions : lock/unlock, start engine, valet, …

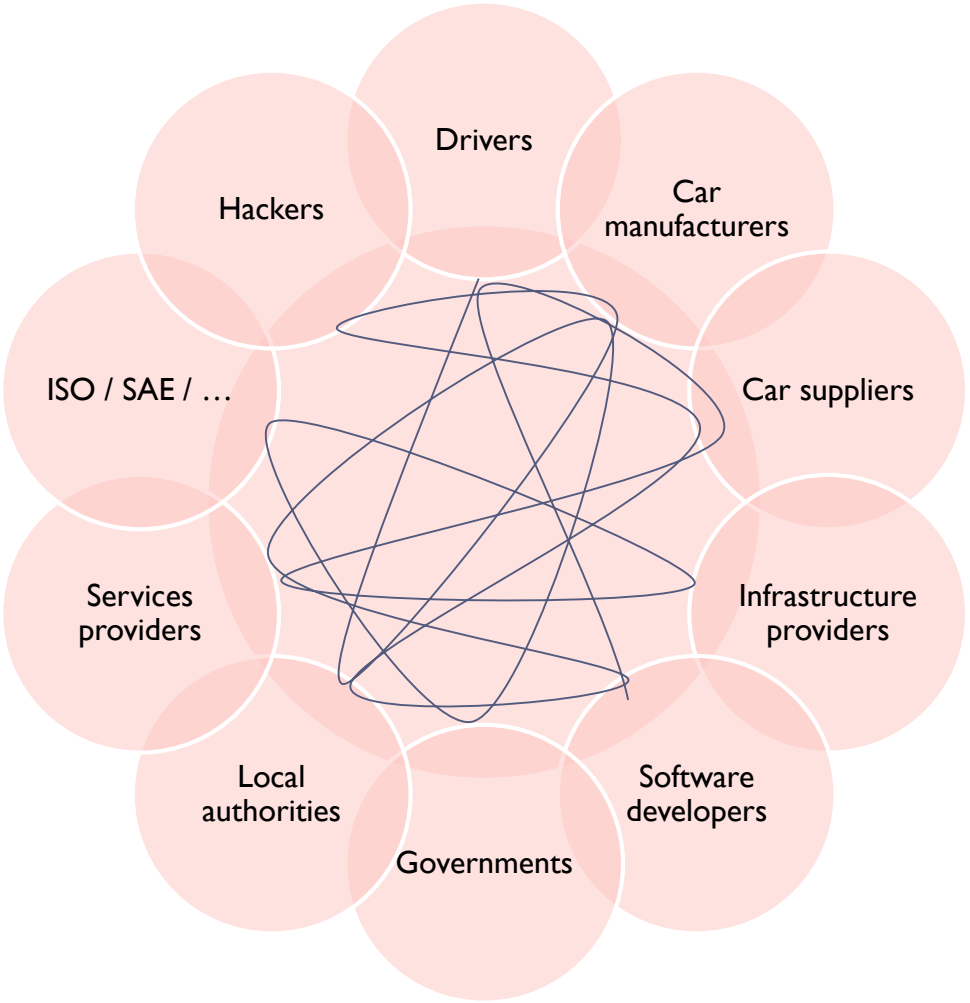
Remote diagnostics

Car to car communication via WiFi

Virtual keys in your smartphone

Facebook / Pokemon go / WiFi hotspot : keep the driver occupied !

Autonomous vehicle : trust model



Autonomous vehicle

Challenges of (not so far) future:

- Energy
- Industrial systems
- Airplanes
- Space