Stepping Stone to Car Hacking

The Realistic Threat Model

Movie

TROOPERS

MAKE THE WORLD A SAFER PLACE

ENIGMATOS

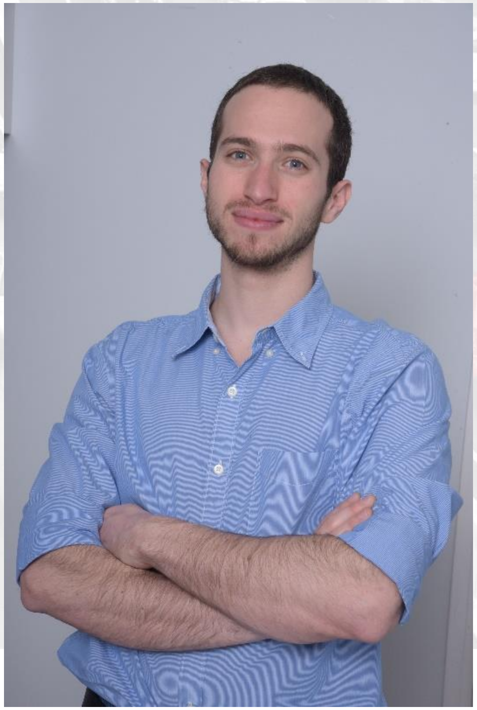
Automotive Cyber Security

Who We Are

Enigmatos - Automotive Cyber Security

Liran Zwickel - Security researcher

Yannay Livneh - Security researcher

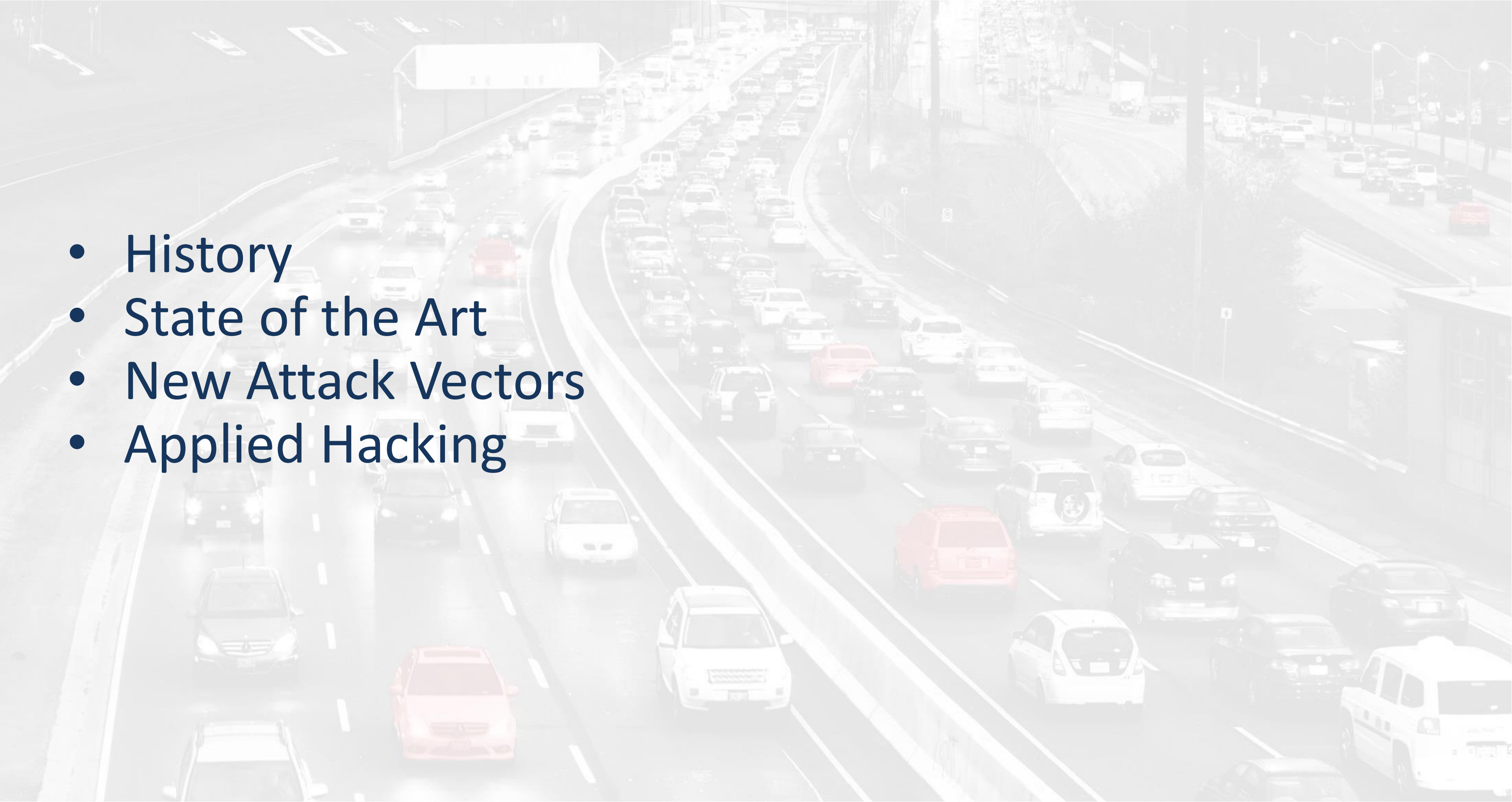


Alex Fok – CTO

ENIGMATOS

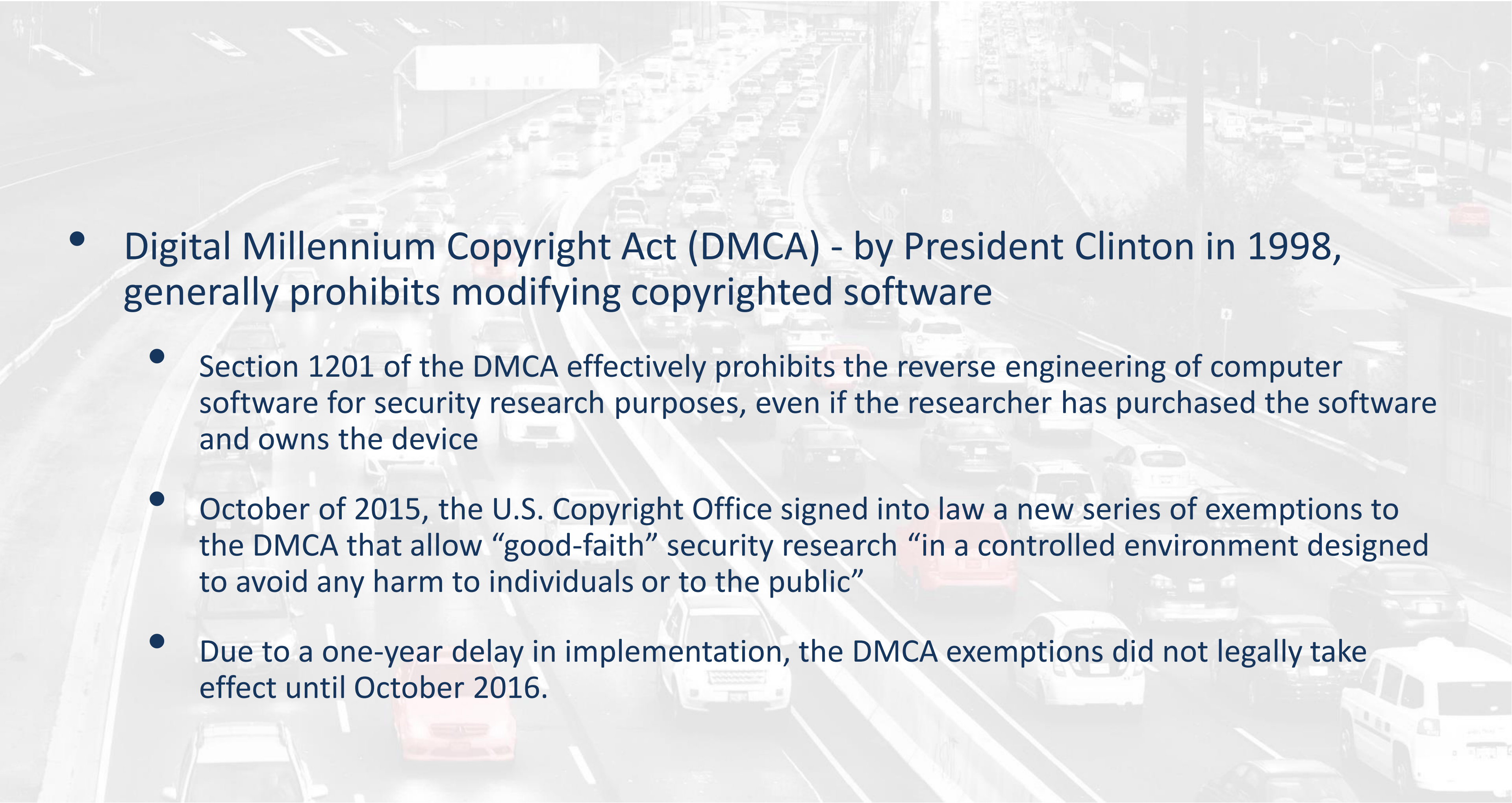
Automotive Cyber Security

Agenda



- History
- State of the Art
- New Attack Vectors
- Applied Hacking

Legal Aspects of Automotive Cyber Research



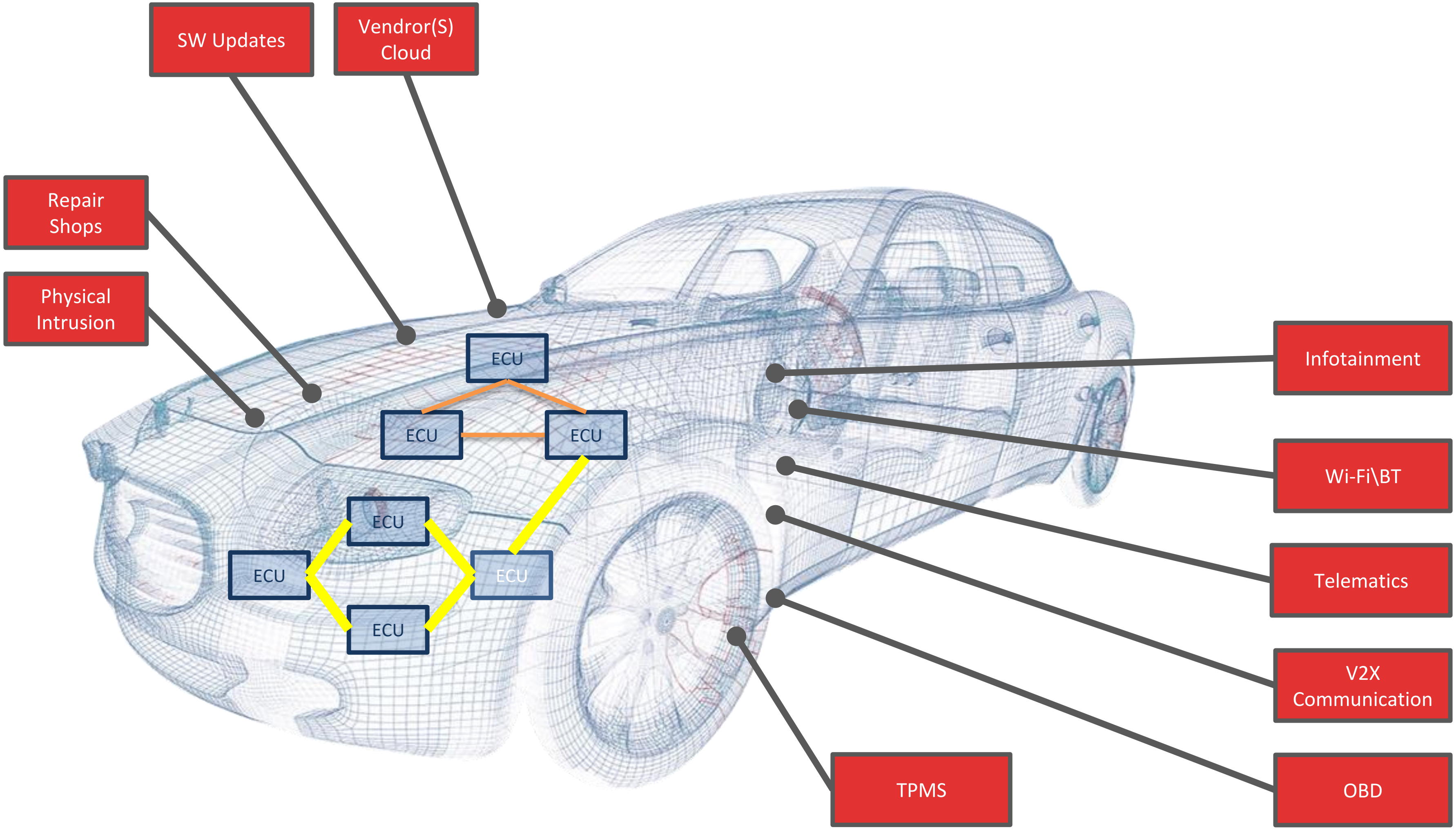
- Digital Millennium Copyright Act (DMCA) - by President Clinton in 1998, generally prohibits modifying copyrighted software
  - Section 1201 of the DMCA effectively prohibits the reverse engineering of computer software for security research purposes, even if the researcher has purchased the software and owns the device
  - October of 2015, the U.S. Copyright Office signed into law a new series of exemptions to the DMCA that allow “good-faith” security research “in a controlled environment designed to avoid any harm to individuals or to the public”
  - Due to a one-year delay in implementation, the DMCA exemptions did not legally take effect until October 2016.

Automotive Cyber Challenges

- The number of known incidents is low
- Updates Distribution Expensive
- Long life cycle => low computation power
- Physical access protection is poor
- Lack of standardization

ENIGMATOS
Automotive Cyber Security

Attack Vectors



ENIGMATOS
Automotive Cyber Security

AUTOMOTIVE CYBER SECURITY CHALLENGE

Complete control through cellular. Chrysler had to recall 1.4 M vehicles (2015)

Ability to lock and unlock car as well as access to personal data through WiFi (2016)

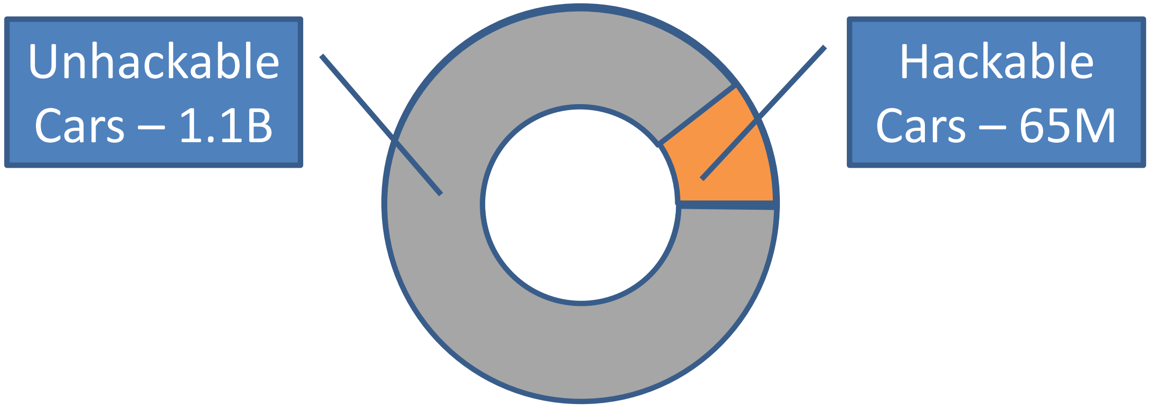
Autopilot & multiple car systems hacked through WiFi (2016)

Connected

Connected and Intelligent

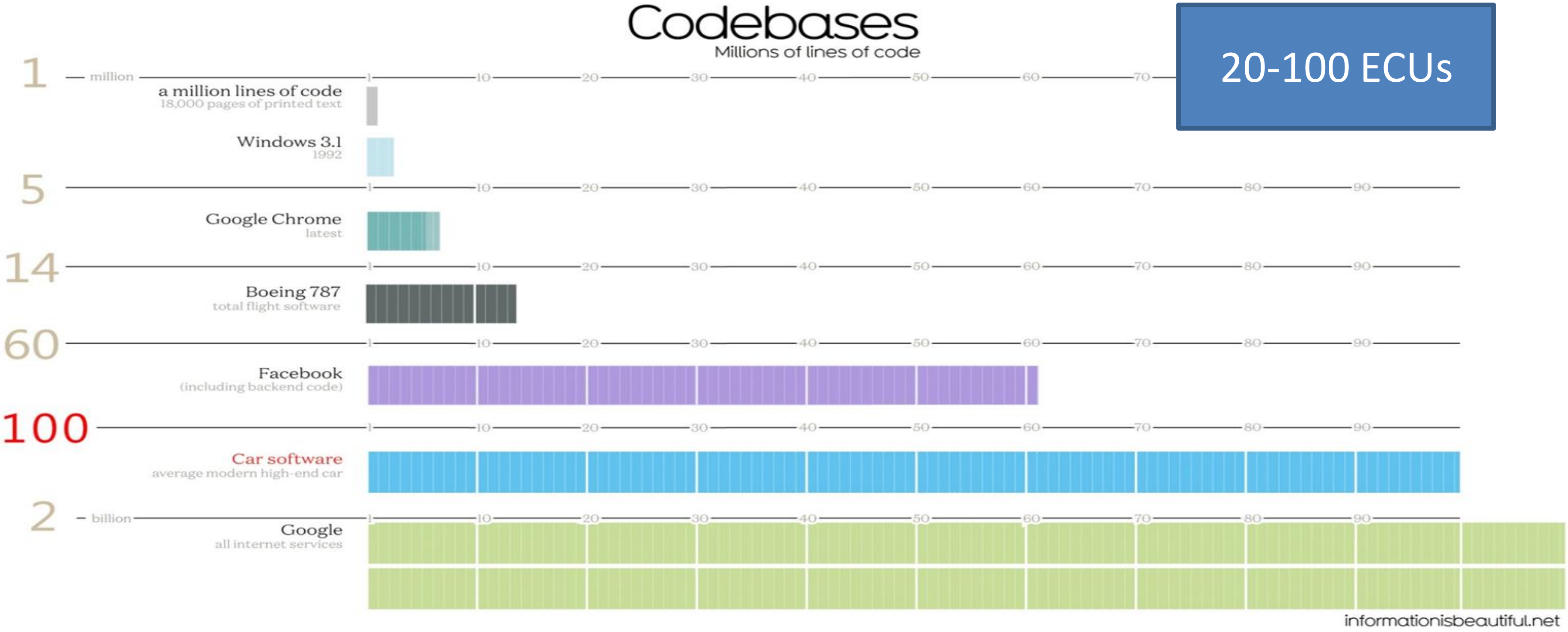
Connected and Super Intelligent

Unhackable Cars



Really?

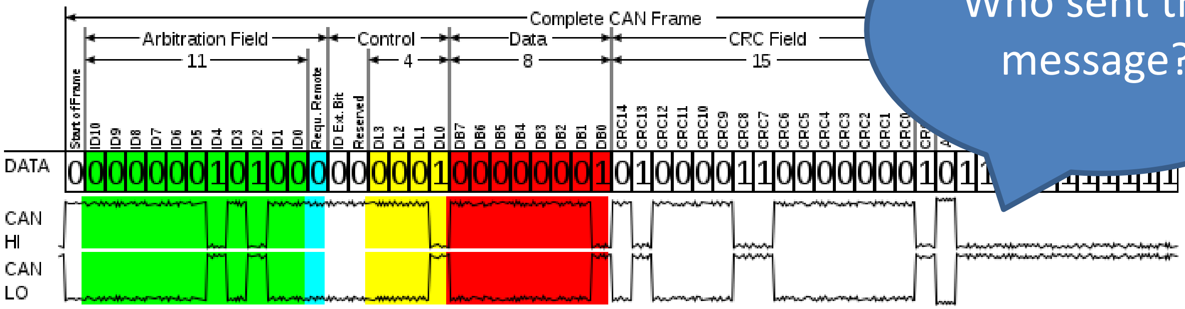
Dumb is the New Smart



20-100 ECUs

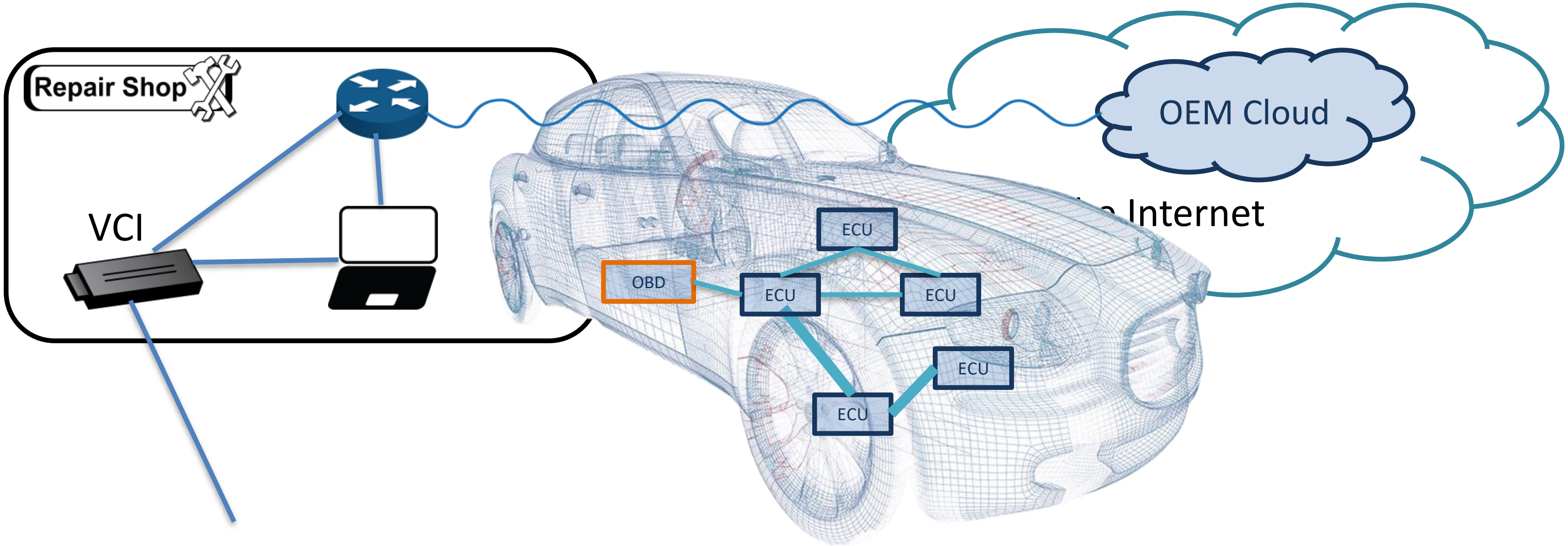
CAN Bus – Automotive Networks Queen

- Selected Security challenges
  - Lack of device authentication
  - Lack of content authentication



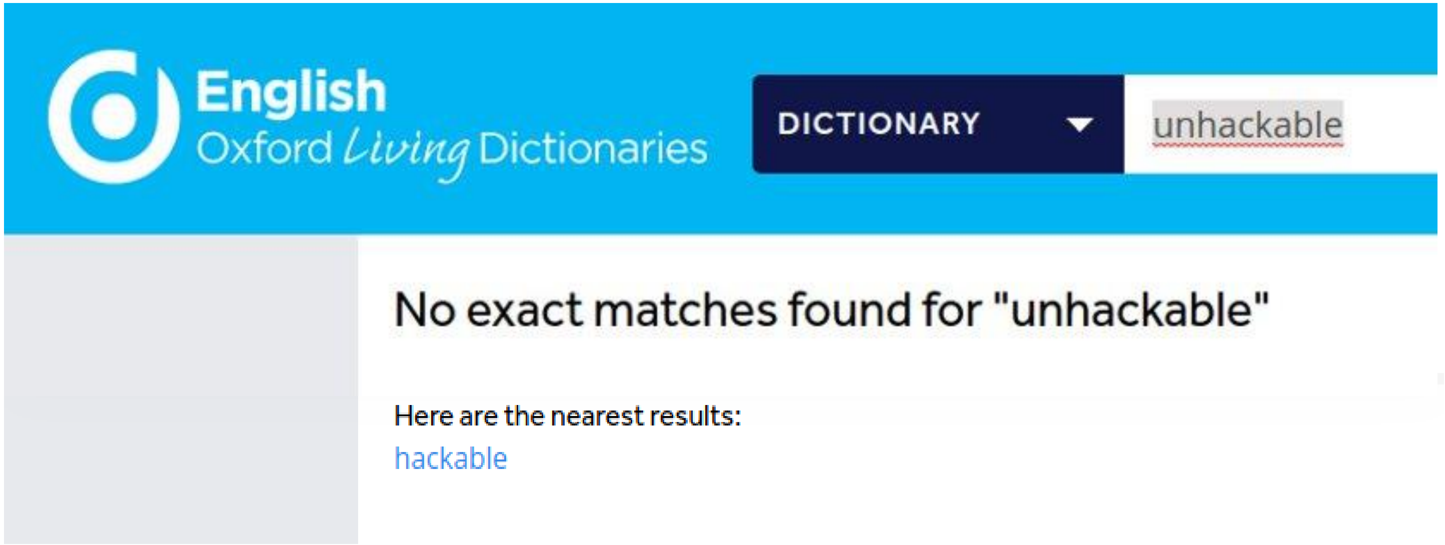
Who sent this message?

The Architecture



Vector Attacks Analysis - Yannay

Unhackable



No exact matches found for "unhackable"

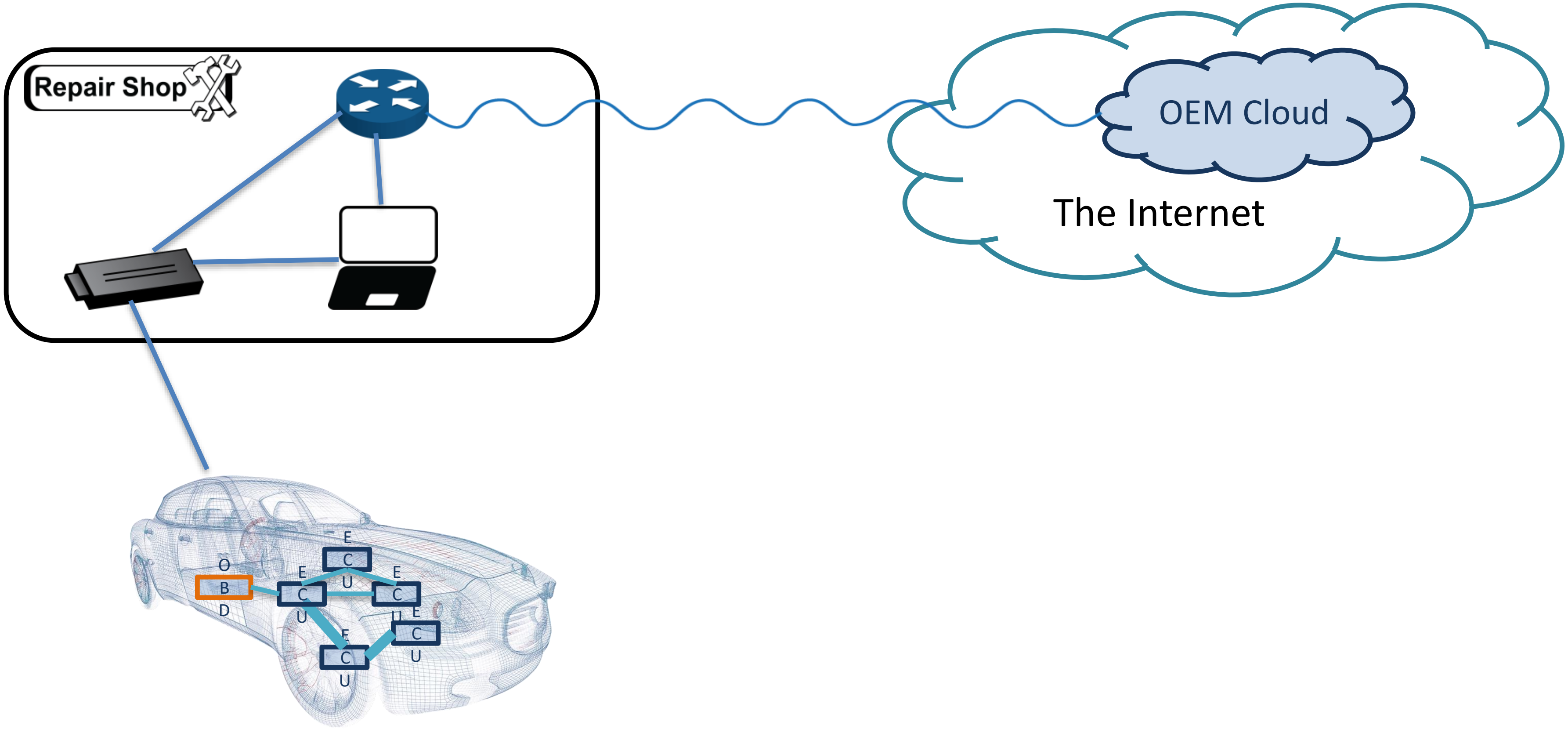
Here are the nearest results:

hackable

Car Hacking Objectives

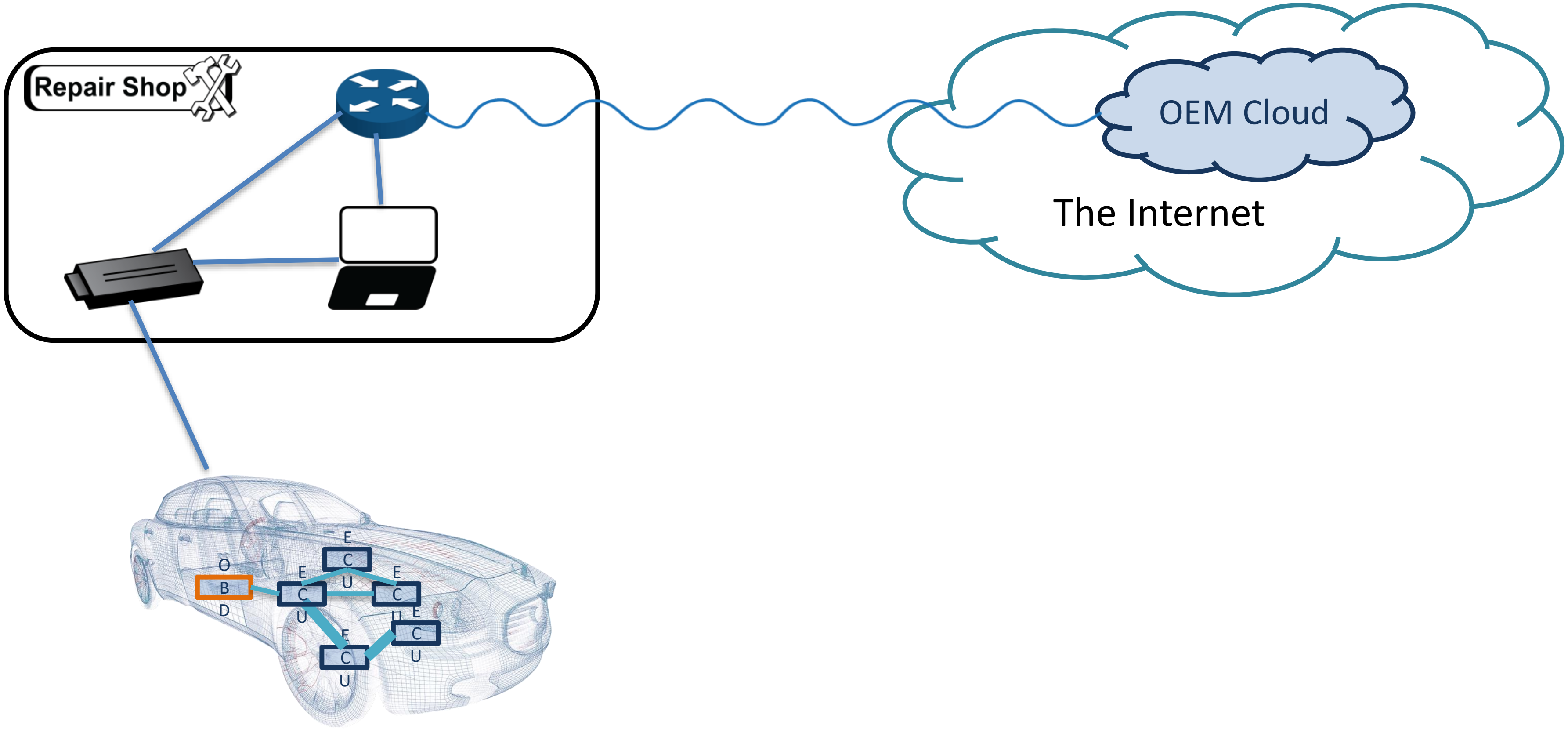
- Control critical functions
- Sabotage
- Private information theft
- OEM deception

The Architecture



ENIGMATOS
Automotive Cyber Security

The Architecture



ENIGMATOS
Automotive Cyber Security

Trust Model

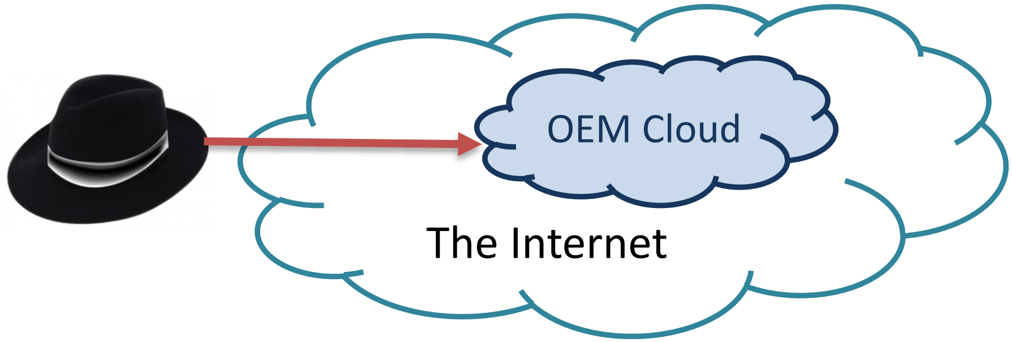
Potential Attack Surfaces

- Internet
- Rogue Cars

The Internets

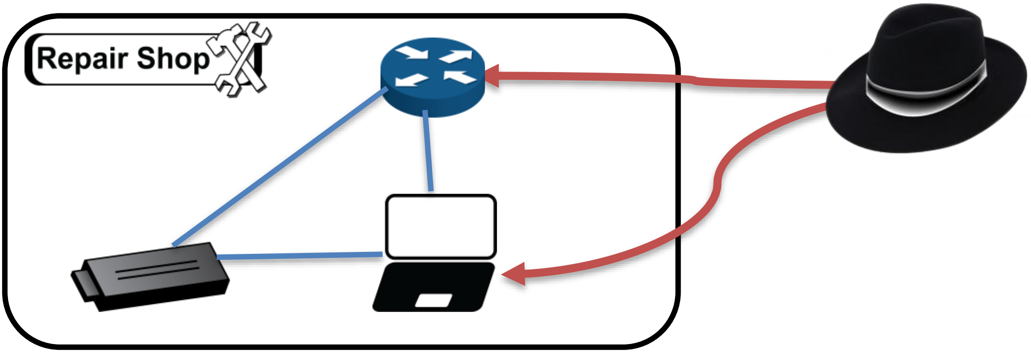
Internet to Cloud

- Looks Promising
- Most objectives achieved
- Full scale



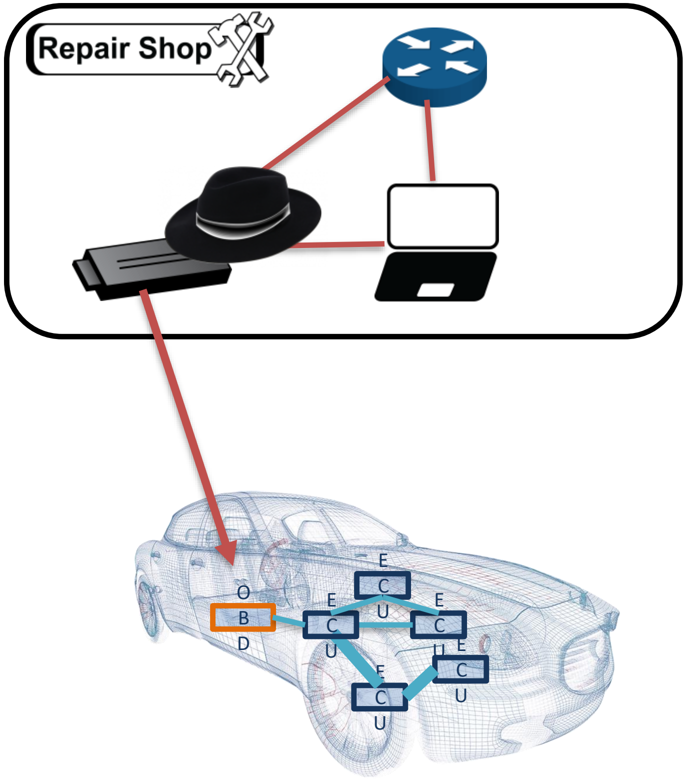
Internet to Repair Shop

- Feasible
  - IoT
  - Old Machines
- Distributed
- Objectives: 1 hop away

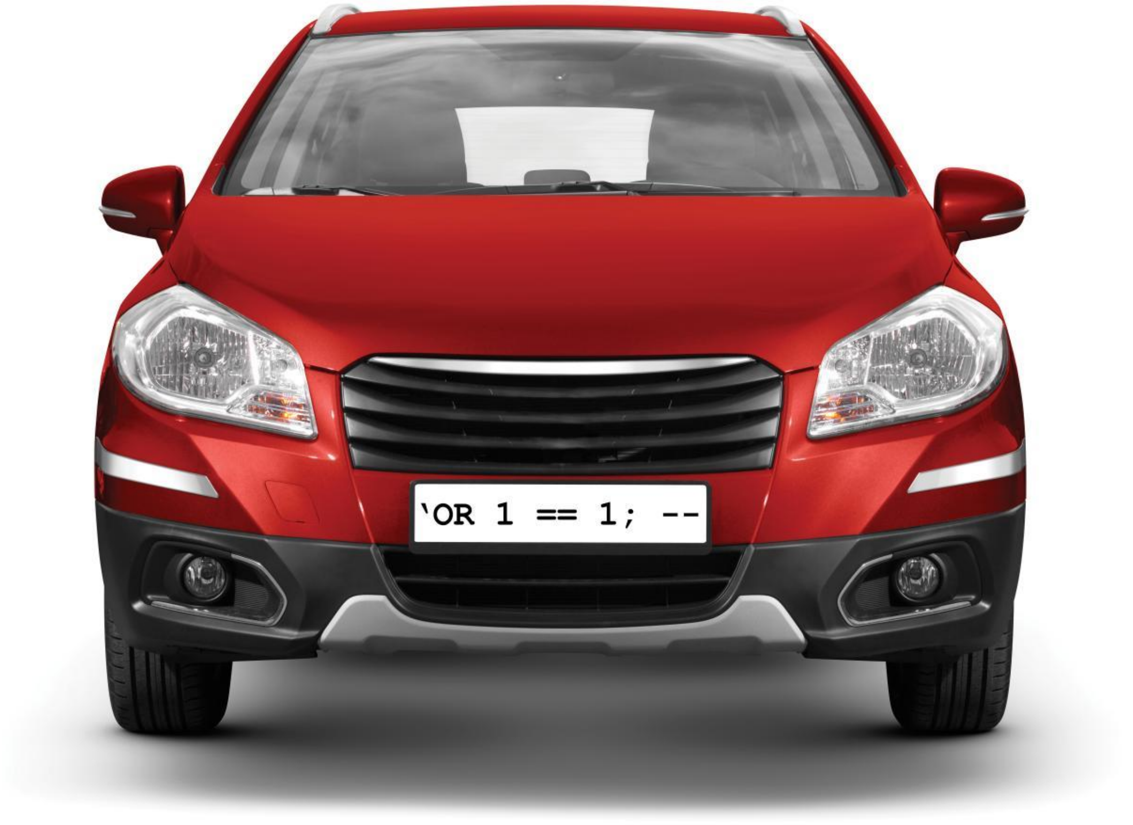


Repair Shop to VCI

- Easy
  - – By design
  - – Badly Secured
- All objectives achieved

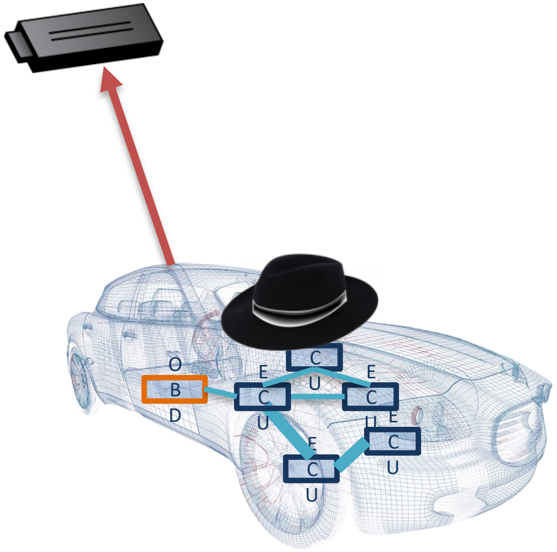


Rogue Car



Car to VCI

- Easy, Easy, Easy
- All objectives achieved
- Can it scale?



ENIGMATOS Automotive Cyber Security

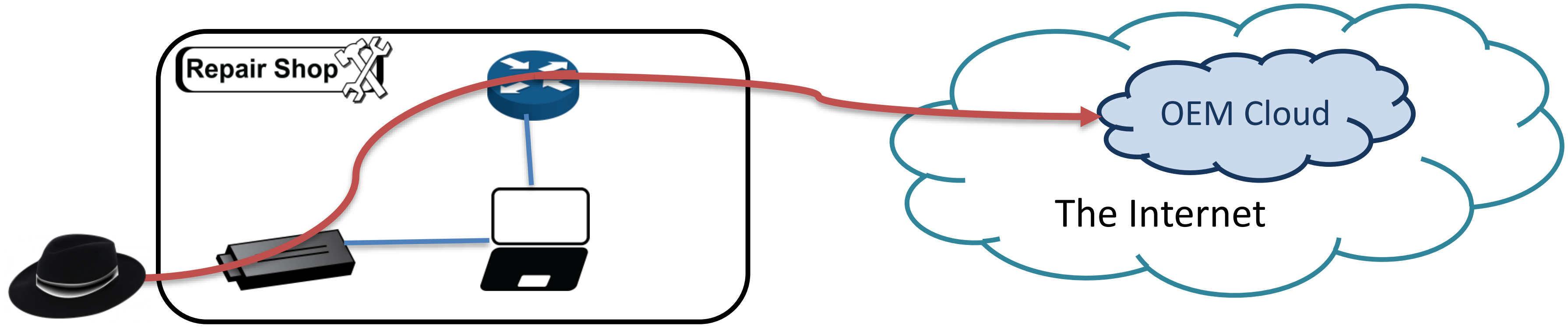
Plan for Scale

- Rogue car attacks VCI
- VCI attacks car
- Car attacks another VCI
- ???
- Profit

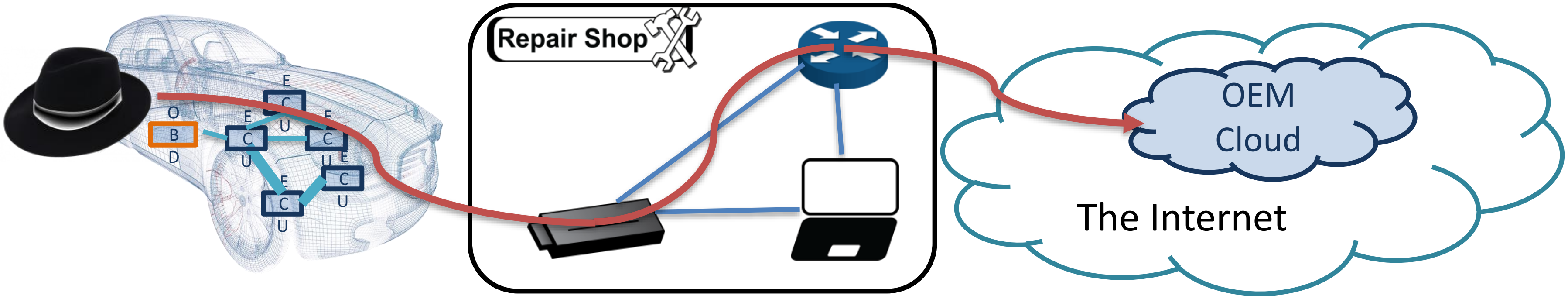
Weird Bonus Vectors

VCI to Cloud

- Trusted Input
- Direct Access



Car to Cloud

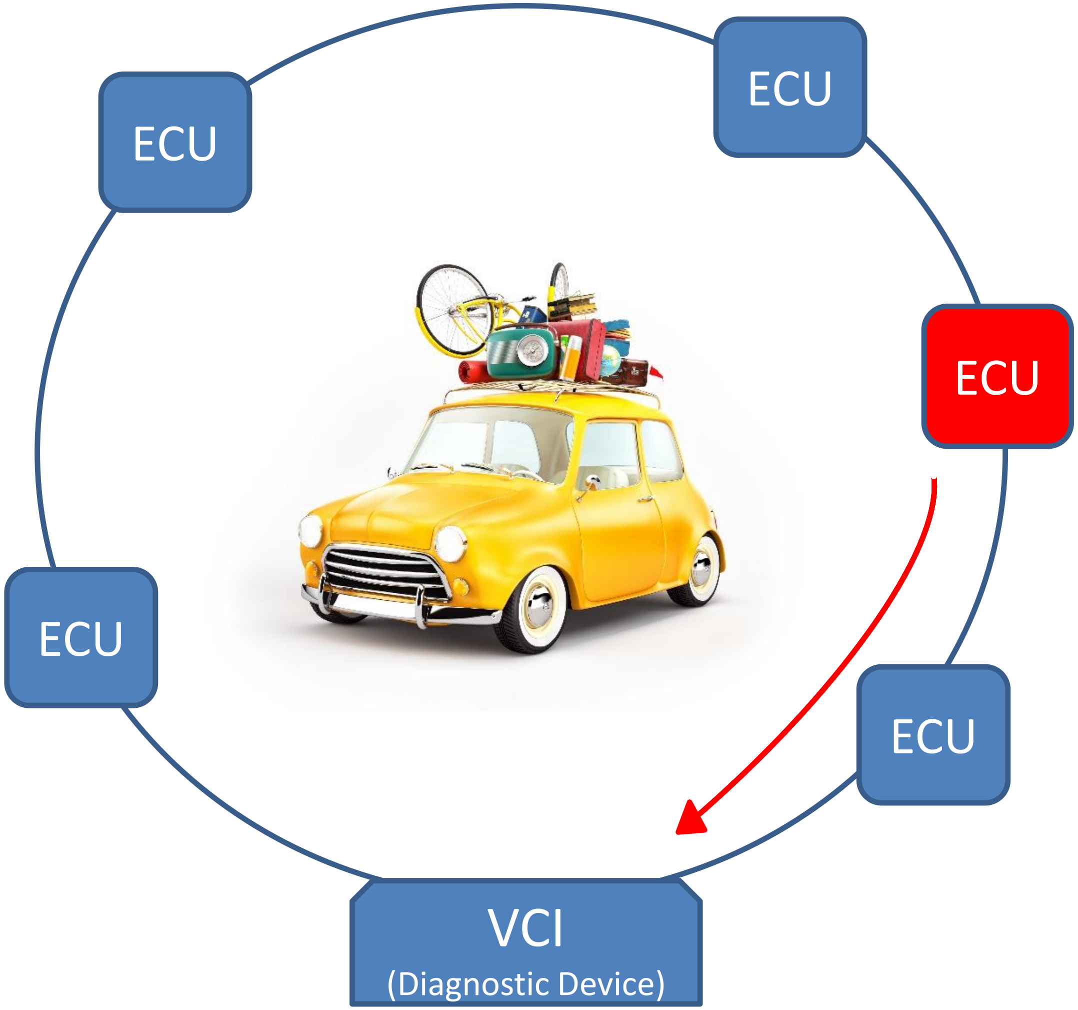


Ecosystem Research 101

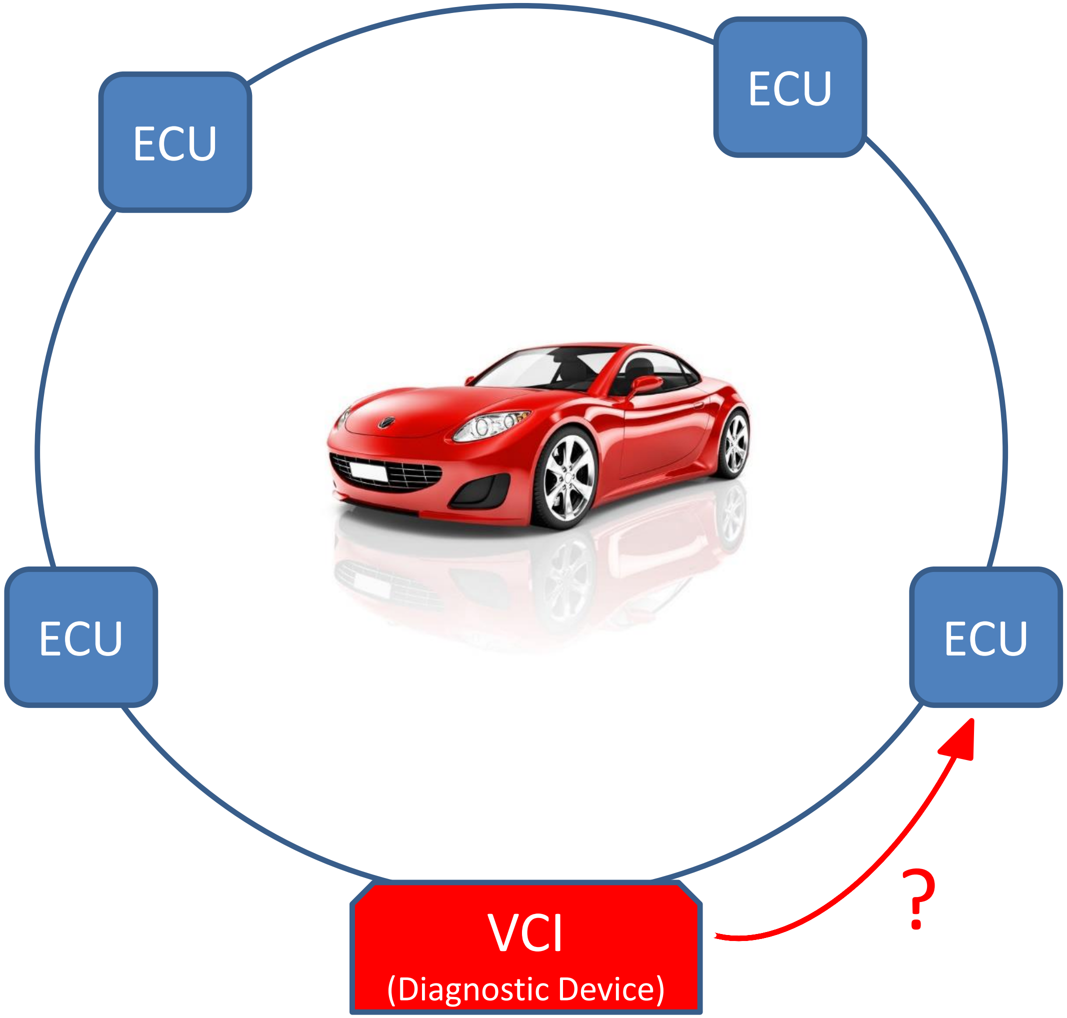
- OEM Cloud – web research
- VCI – embedded research
- Car – CAN and ECU and stuff

Applied Hacking - Liran

Quick review



Quick review



CAN BUS

(OR: I have access to the car. Now what?)

CAN? What is CAN?

Developed by Bosch in 1983

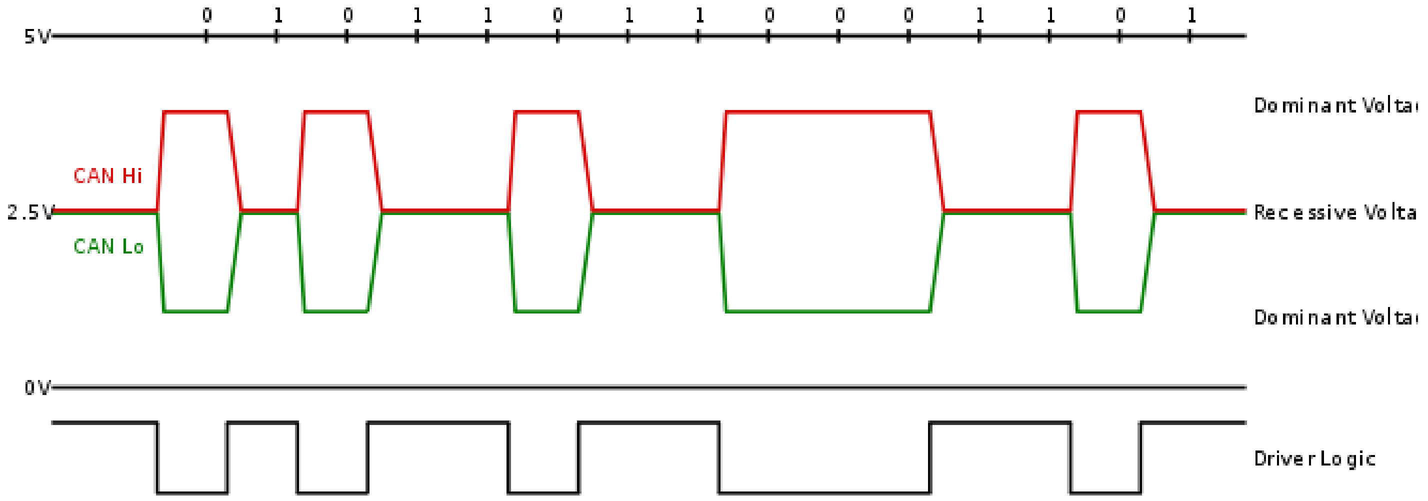
Standardized in 1993 by The ISO (International Organization for Standardization)

- Fast (Up to 1Mbps)
- Cheap
- Reliable

ENIGMATOS
Automotive Cyber Security

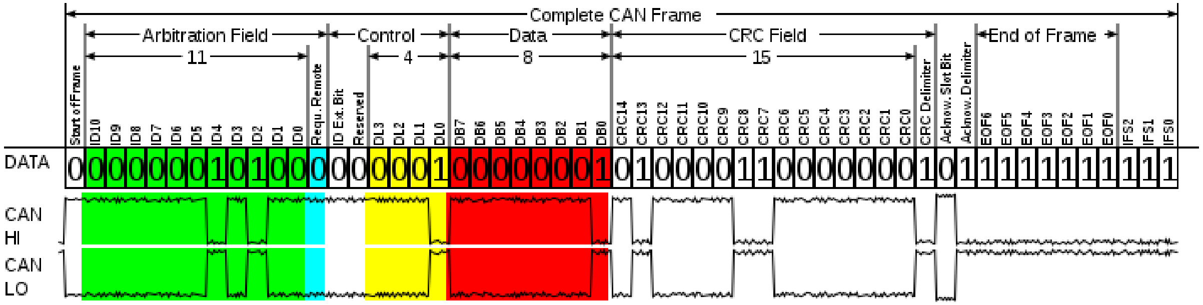
CAN? What is CAN?

CAN? What is CAN?



ENIGMATOS
Automotive Cyber Security

CAN Message

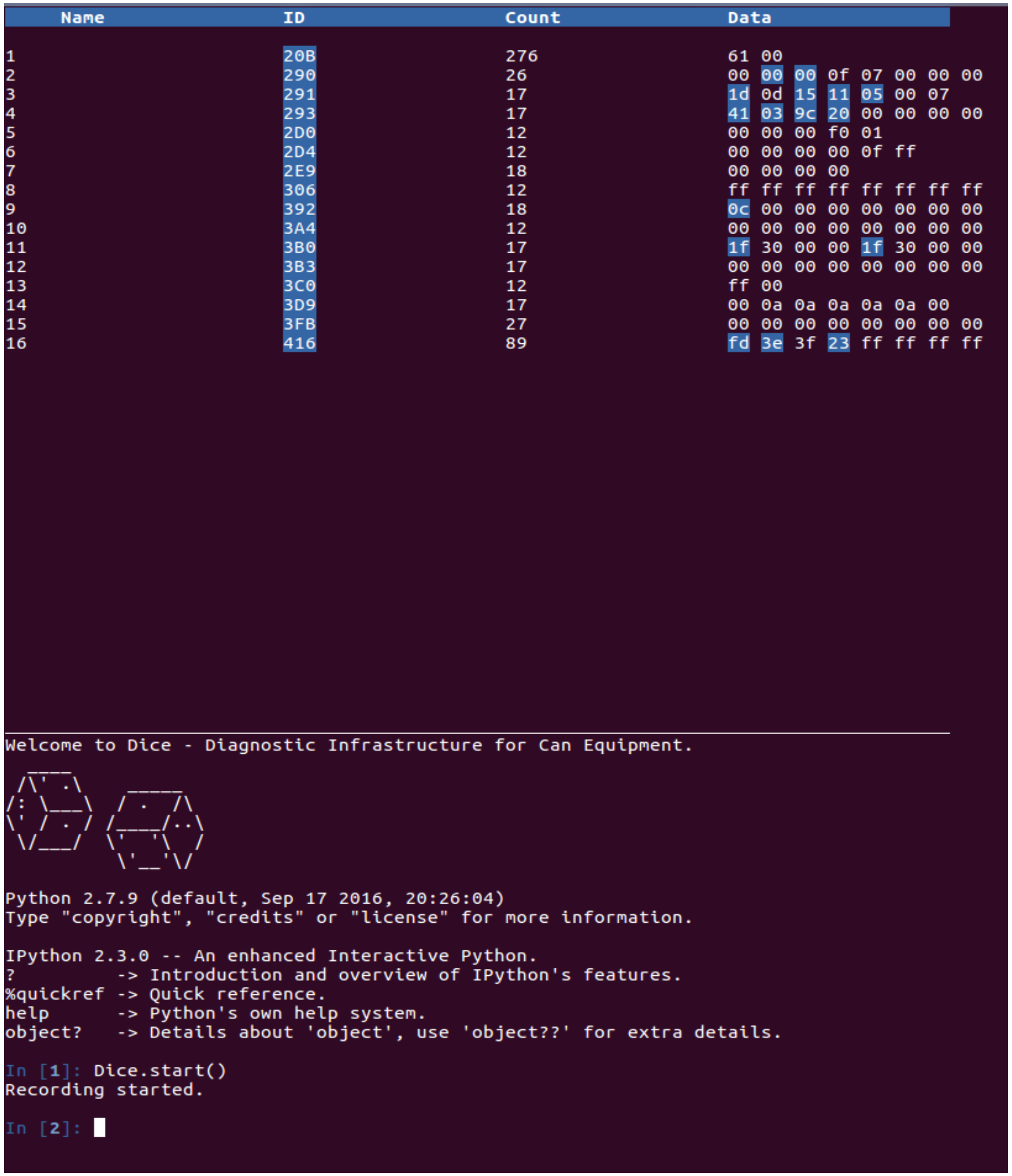


Field name	Length (bits)	Purpose
Start-of-frame	1	Denotes the start of frame transmission
Identifier (green)	11	A (unique) identifier which also represents the message priority
Remote transmission request (RTR) (blue)	1	Must be dominant (0) for data frames and recessive (1) for remote request frames (see Remote Frame, below)
Identifier extension bit (IDE)	1	Must be dominant (0) for base frame format with 11-bit identifiers
Reserved bit (r0)	1	Reserved bit. Must be dominant (0), but accepted as either dominant or recessive.
Data length code (DLC) (yellow)	4	Number of bytes of data (0–8 bytes)[a]
Data field (red)	0–64 (0-8 bytes)	Data to be transmitted (length in bytes dictated by DLC field)
CRC	15	Cyclic redundancy check
CRC delimiter	1	Must be recessive (1)
ACK slot	1	Transmitter sends recessive (1) and any receiver can assert a dominant (0)
ACK delimiter	1	Must be recessive (1)
End-of-frame (EOF)	7	Must be recessive (1)

CAN Message

123 # 11 22 33 44 55 66 77 88

416 # fd 3e 3f 23 ff ff ff ff



```
     Name                 ID                   Count                Data

1                         20B                  276                  61 00
2                         290                  26                   00 00 00 0f 07 00 00 00
3                         291                  17                   1d 0d 15 11 05 00 07
4                         293                  17                   41 03 9c 20 00 00 00 00
5                         2D0                  12                   00 00 00 f0 01
6                         2D4                  12                   00 00 00 00 0f ff
7                         2E9                  18                   00 00 00 00
8                         306                  12                   ff ff ff ff ff ff ff ff
9                         392                  18                   0c 00 00 00 00 00 00 00
10                        3A4                  12                   00 00 00 00 00 00 00 00
11                        3B0                  17                   1f 30 00 00 1f 30 00 00
12                        3B3                  17                   00 00 00 00 00 00 00 00
13                        3C0                  12                   ff 00
14                        3D9                  17                   00 0a 0a 0a 0a 0a 00
15                        3FB                  27                   00 00 00 00 00 00 00 00
16                        416                  89                   fd 3e 3f 23 ff ff ff ff
```

```
Welcome to Dice - Diagnostic Infrastructure for Can Equipment.

  ____
 /\' .\    _____
/: \___\  / .  /\
\' / . / /____/..\
 \/___/  \'  '\  /
          \'__'\/

Python 2.7.9 (default, Sep 17 2016, 20:26:04)
Type "copyright", "credits" or "license" for more information.

IPython 2.3.0 -- An enhanced Interactive Python.
?         -> Introduction and overview of IPython's features.
%quickref -> Quick reference.
help      -> Python's own help system.
object?   -> Details about 'object', use 'object??' for extra details.

In [1]: Dice.start()
Recording started.

In [2]: 
```

Dice – Enigmatos Research Software

CAN Message Types

Sensor Messages

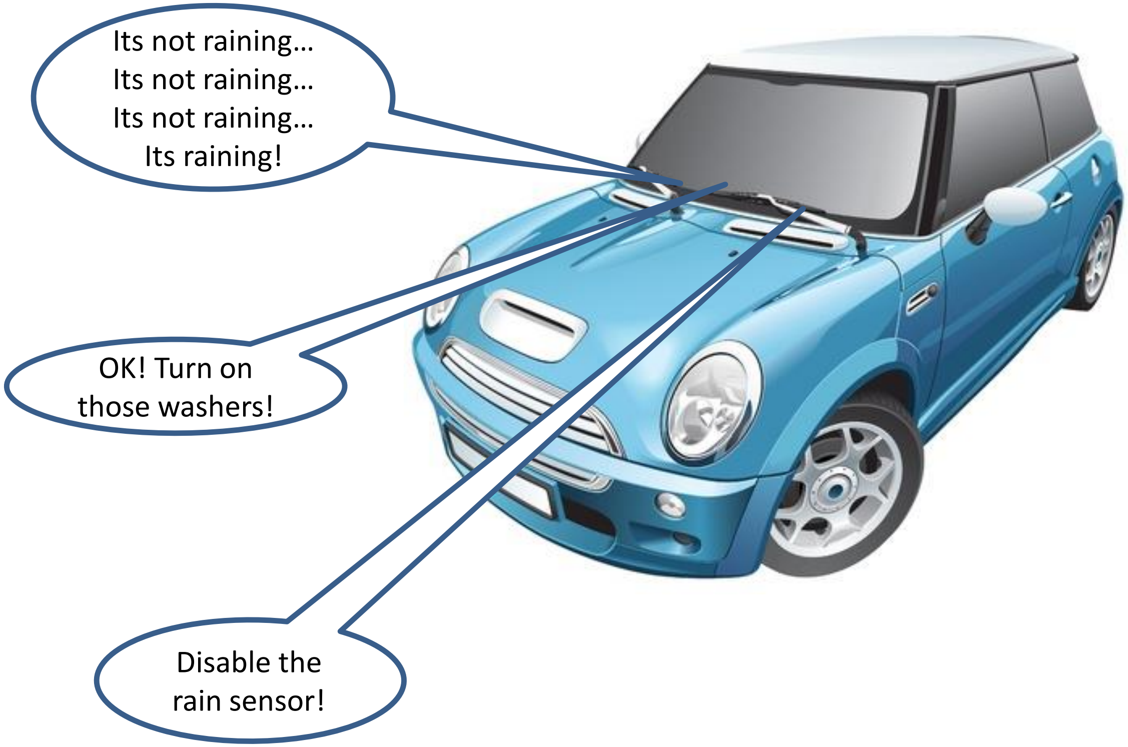
- Rain Sensor
- Gear Mode
- Speed
- Seatbelt Sensor

Actuators

- Turn on Washers
- Move Side Mirrors

Configurations

- Lock doors in high speeds



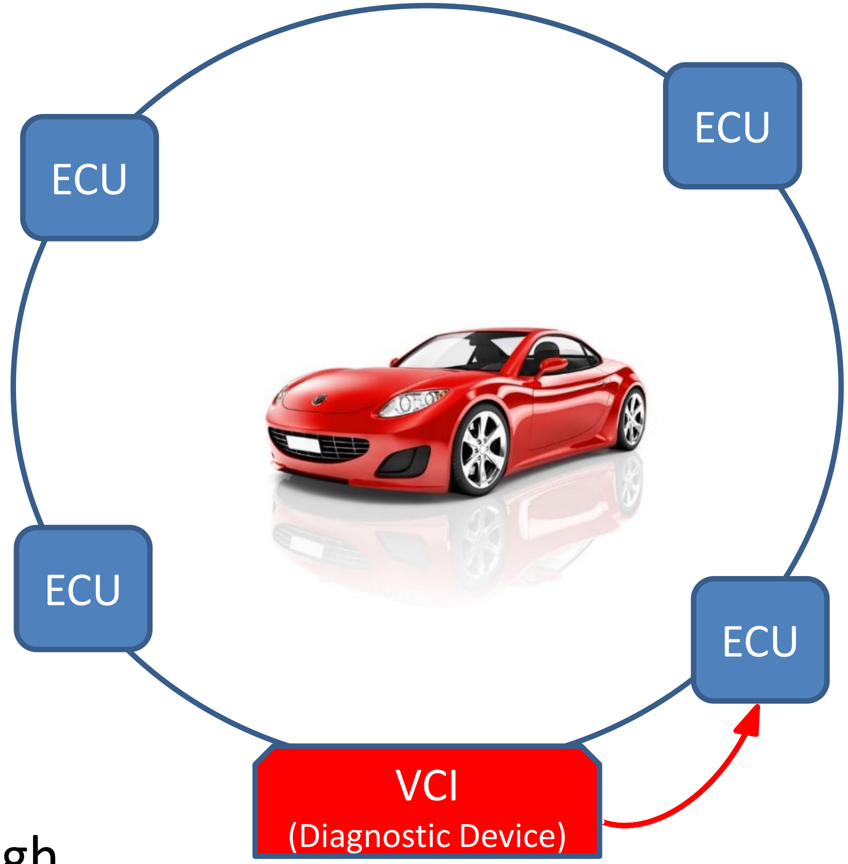
© All Rights Reserved Enigmatos

ENIGMATOS
Automotive Cyber Security

Possible Attacks

Actuators

- Starting the Engine
- Pressing the Breaks
- Turning on Indicators
- Pressing the Gas
- Folding Side Mirrors
- Starting Washers
- Wasting all Washer Fluid (muhaha!)
- etc



Configurations

- Disable Parking Sensor
- Disable Reverse Camera
- Disabling Car Alerts (oil, water, etc)
- Automatic Door Locking at High Speeds
- Automatic Breaks (according to motion sensor)
- Infotainment Voltage Time After Switch-off
- Automatic Washers
- Enable Video in Motion
- etc

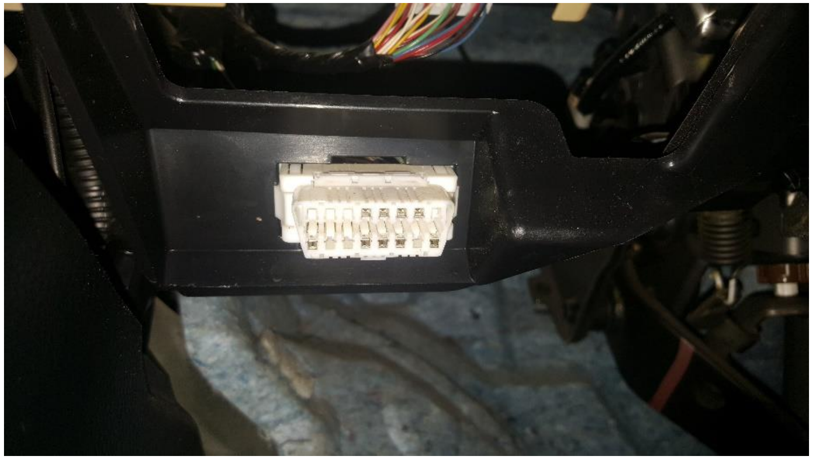
Not good enough…

Connecting To The CAN Bus - OBD

On-board diagnostics (OBD) is an automotive term referring to a vehicle's self-diagnostic and reporting capability.

OBD Messages:

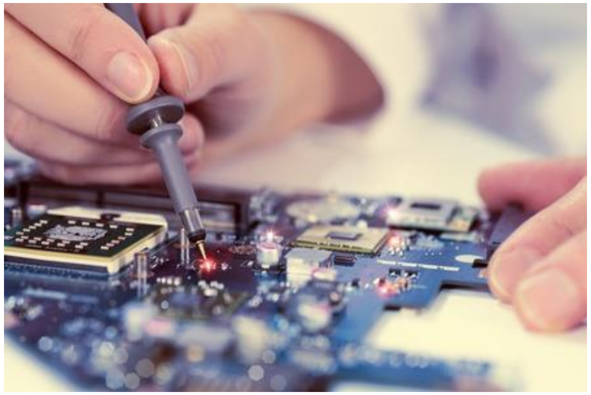
- Engine RPM (0xC)
- Vehicle speed (0xD)
- Throttle position (0x11)
- Engine run time (0x7F)



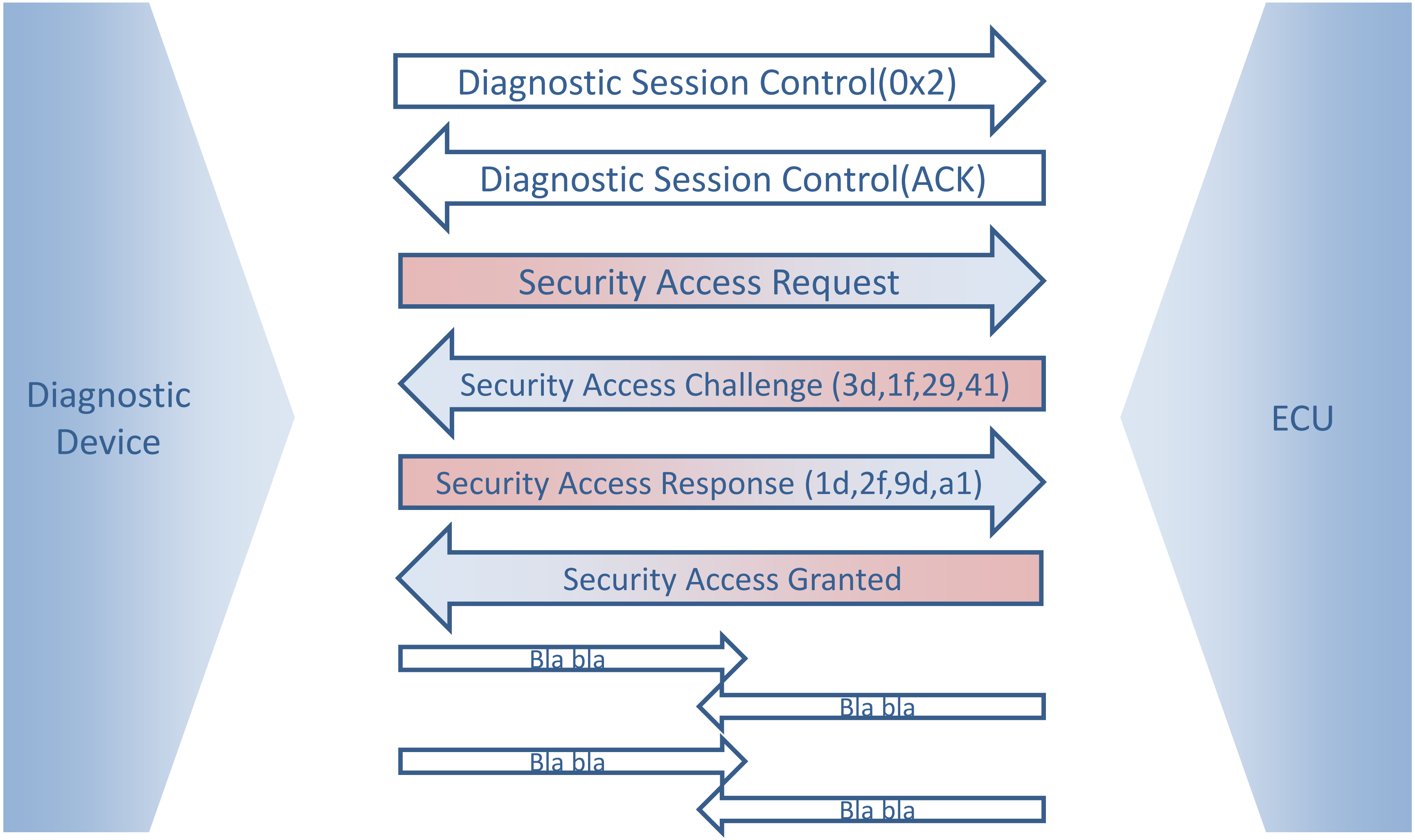
UDS Protocol

Unified Diagnostic Services (UDS) is a diagnostic communication protocol in the electronic control unit (ECU)
ECU specific communication

- ECU Reset
- Read DTC Information
- Clear Diagnostic Information
- **Firmware Upgrade**

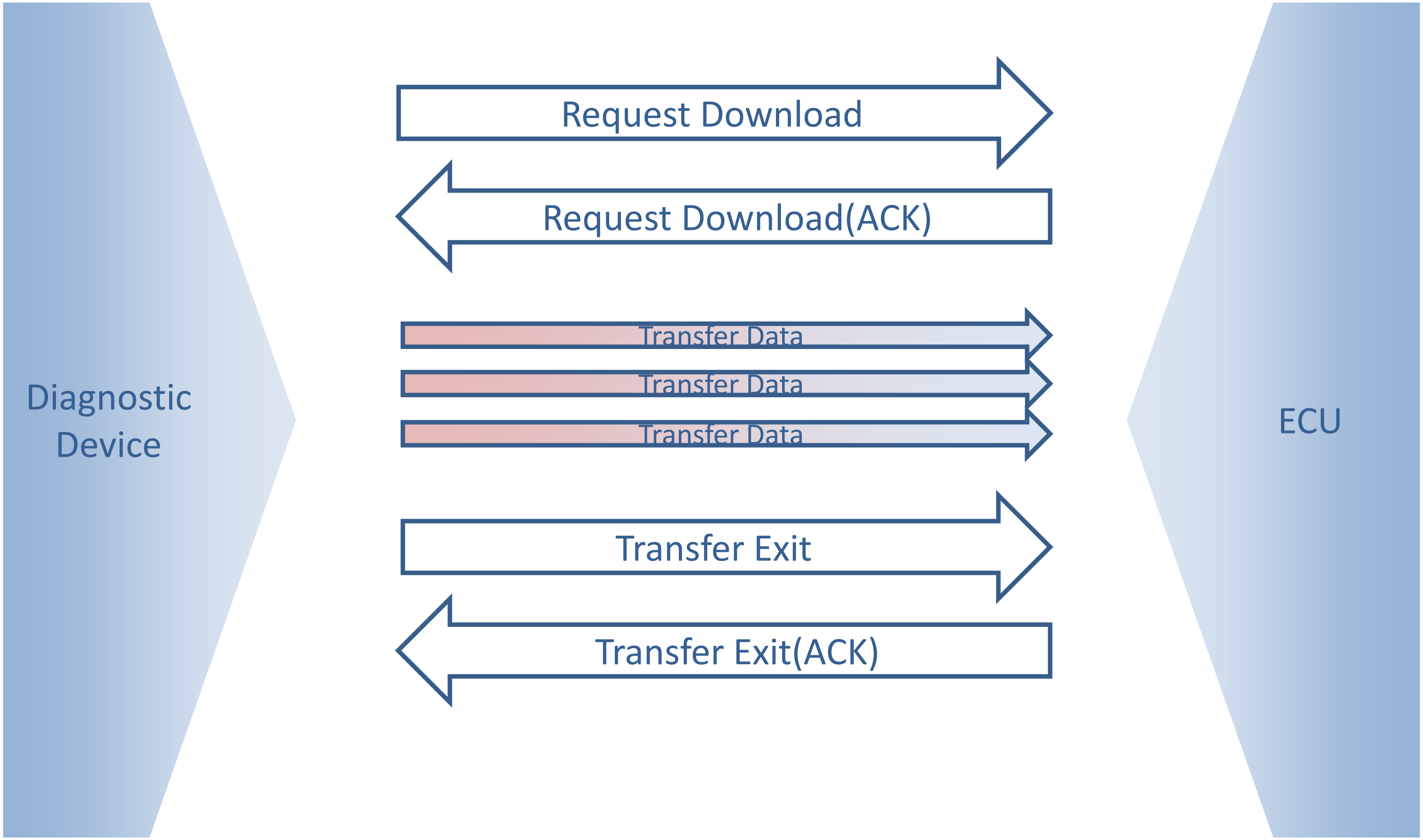


UDS – Firmware Upgrade


Diagnostic Device
ECU
Diagnostic Session Control(0x2)
Diagnostic Session Control(ACK)
Security Access Request
Security Access Challenge (3d,1f,29,41)
Security Access Response (1d,2f,9d,a1)
Security Access Granted
Bla bla
Bla bla
Bla bla
Bla bla

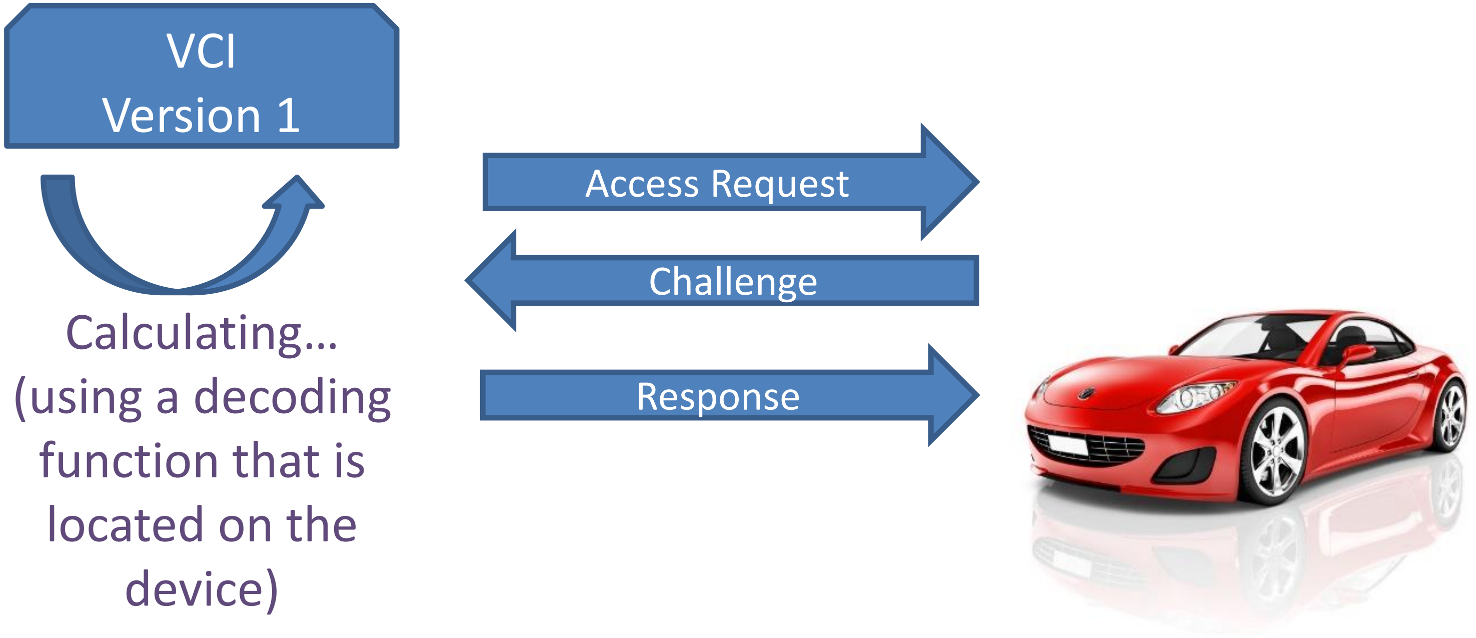
ENIGMATOS
Automotive Cyber Security

UDS – Firmware Upgrade



ENIGMATOS Automotive Cyber Security

VCI Version 1



VCI
Version 1

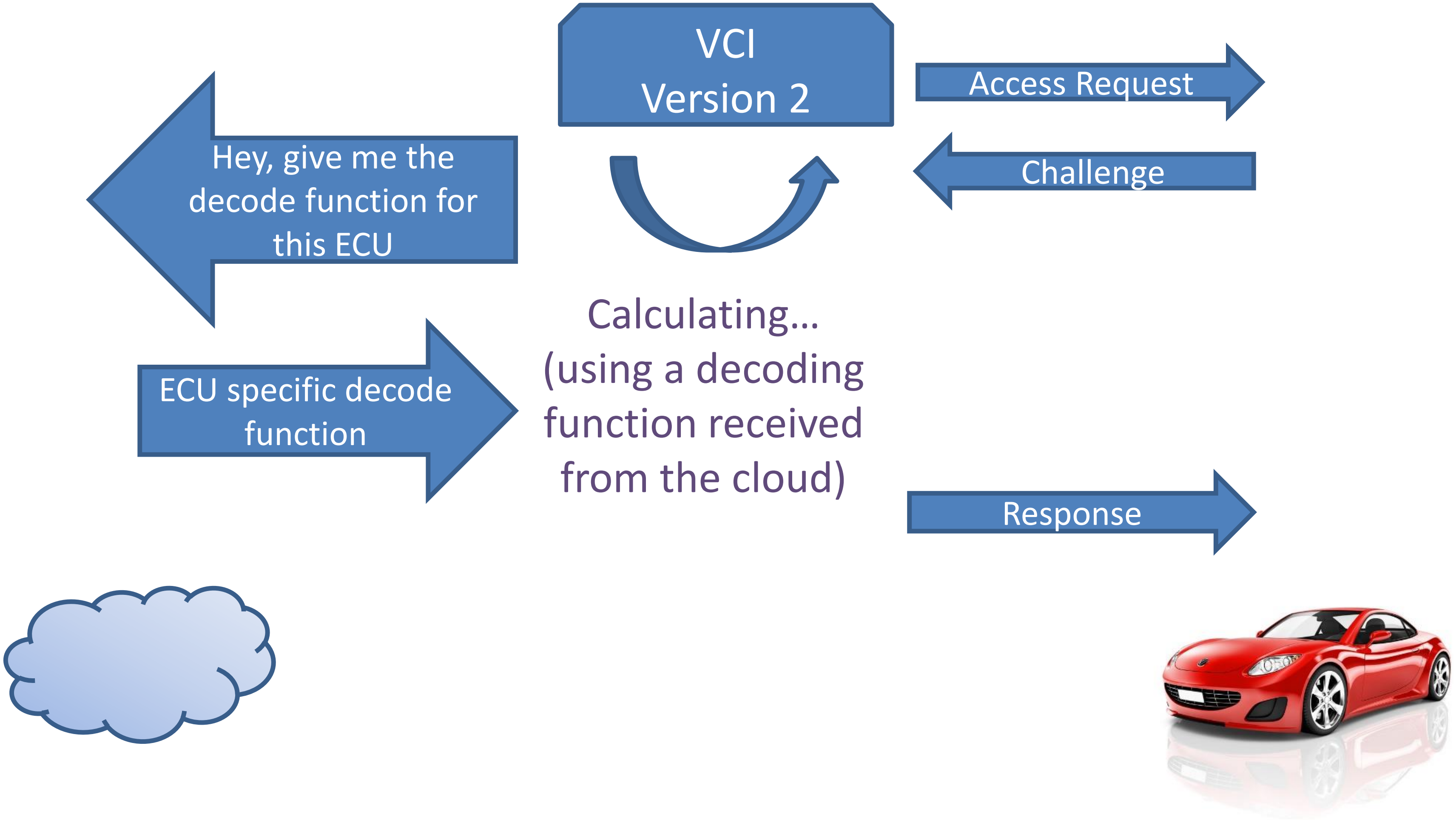
Access Request

Challenge

Response

Calculating…
(using a decoding function that is located on the device)

VCI Version 2



VCI
Version 2

Access Request

Challenge

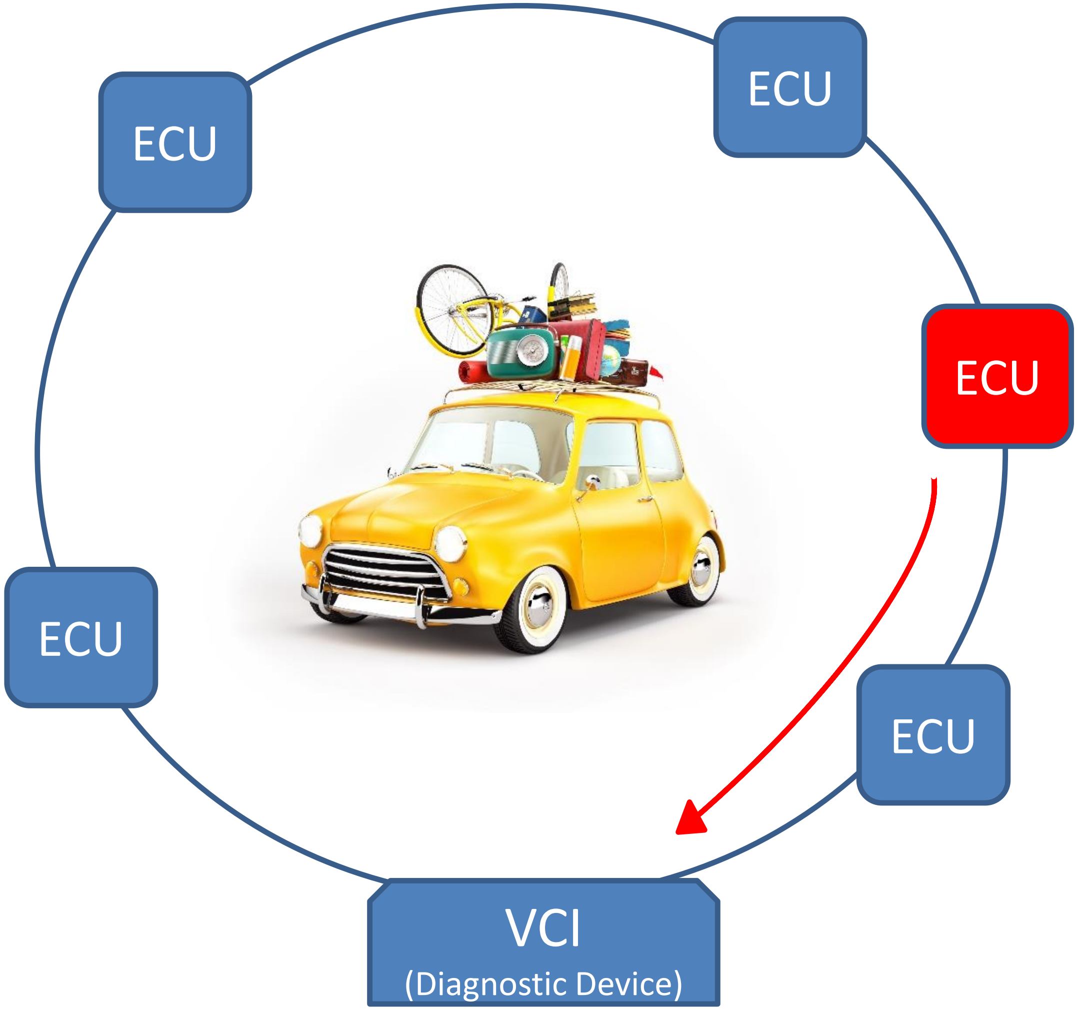
Hey, give me the decode function for this ECU

ECU specific decode function

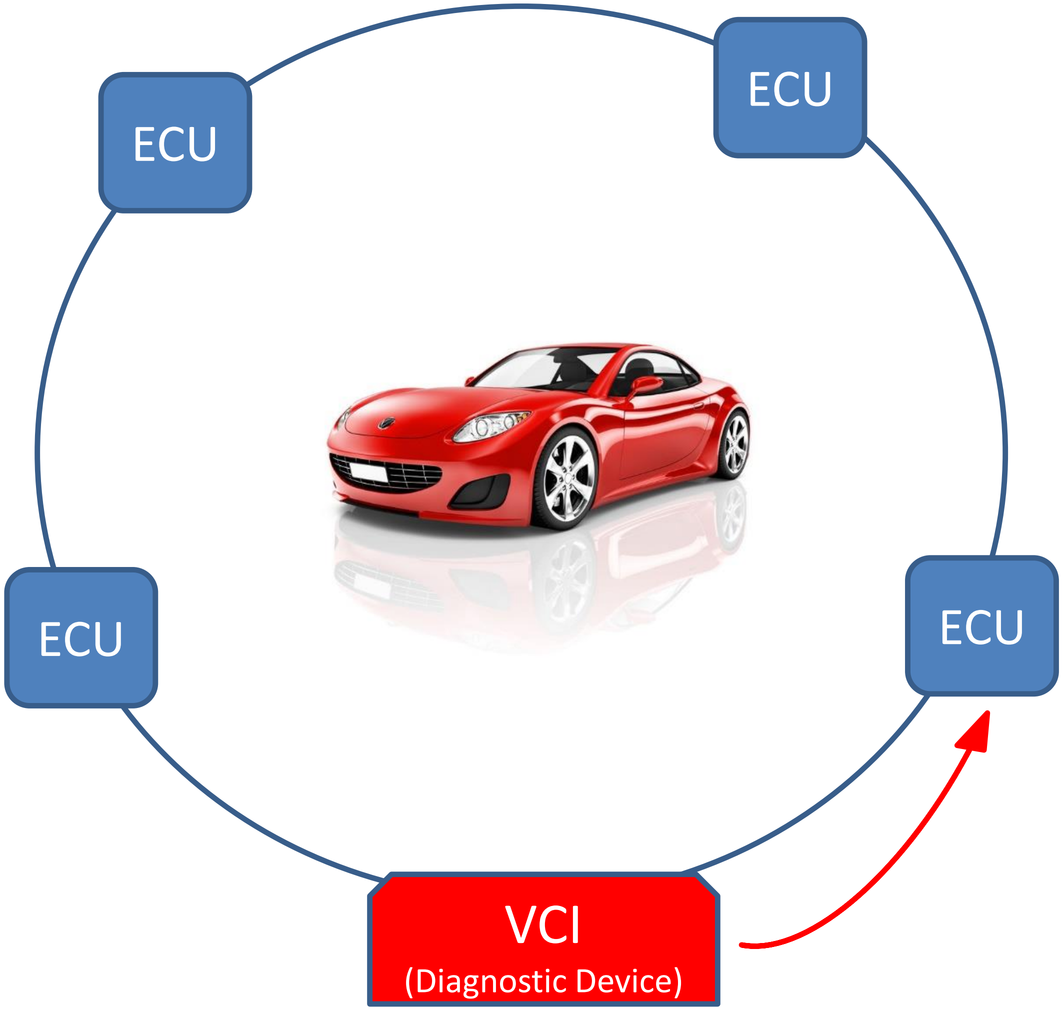
Calculating…
(using a decoding function received from the cloud)

Response

Summary



Summary



ECU

ECU

ECU

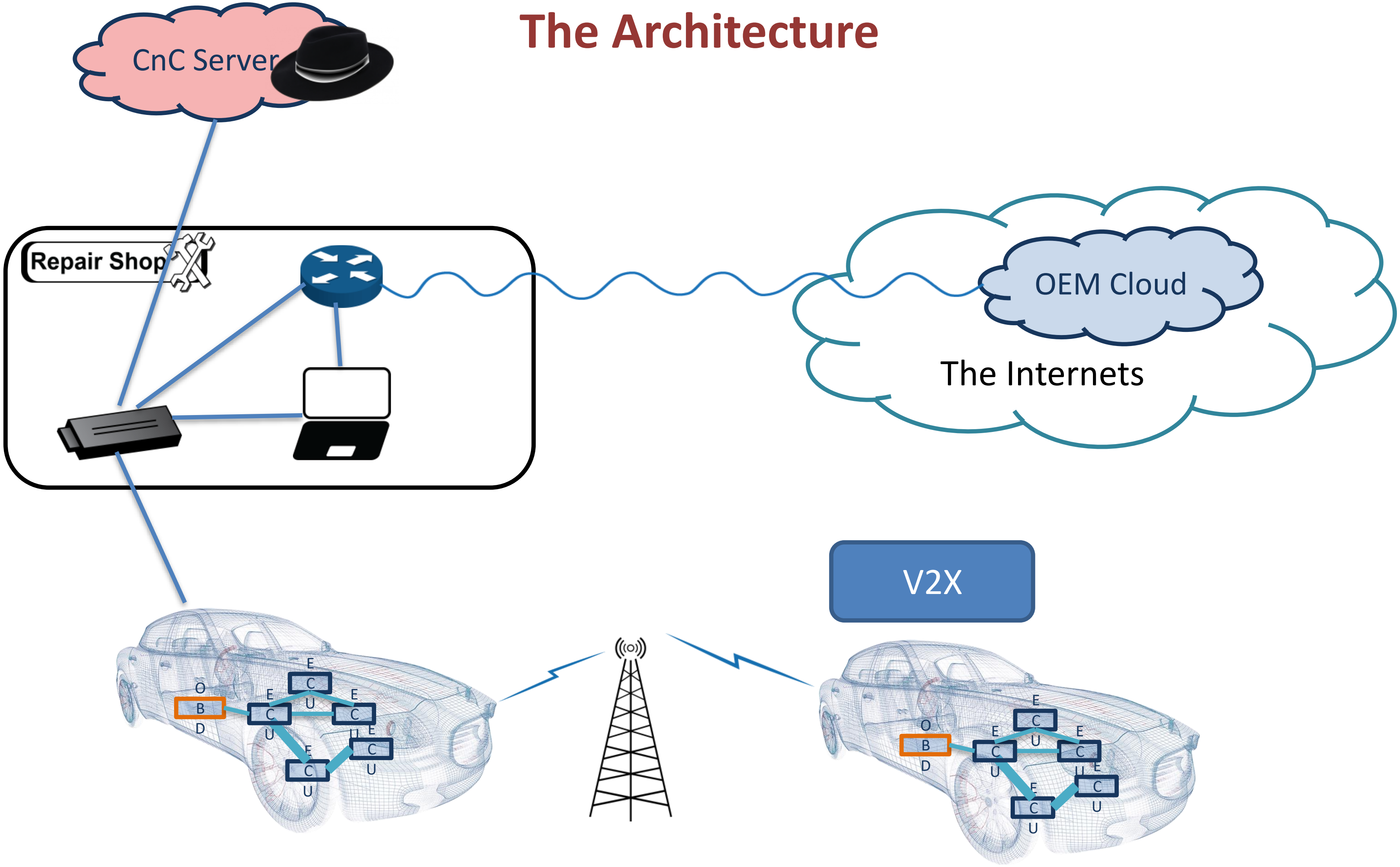
ECU

VCI

(Diagnostic Device)

Summary - Alex

The Architecture



ENIGMATOS
Automotive Cyber Security

What Next?

- Further Vendors Research
- Solutions
  - Short term – bandage (Security Review, hardening)
  - Long term – implement vehicle security solutions
- Cooperation, cooperation, cooperation

Questions

alex@enigmatos.com

yannayl@enigmatos.com @yannayli

liran@enigmatos.com

Thank You