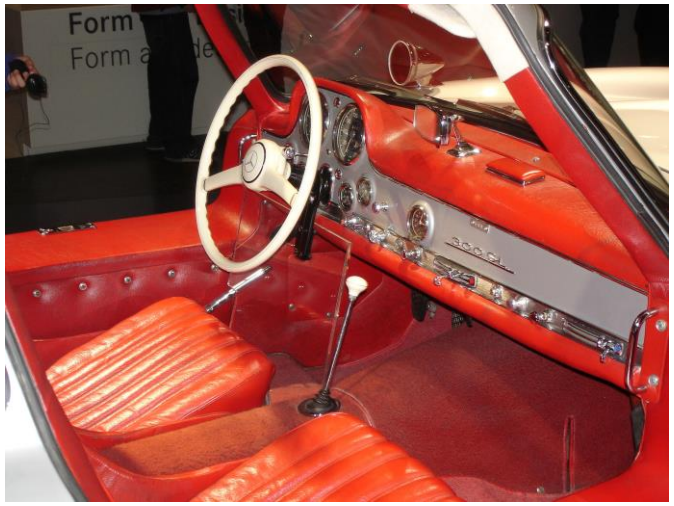
Car hacking

Communication network and security risks in a car system

Tommaso Peletta & Jonathan Lo

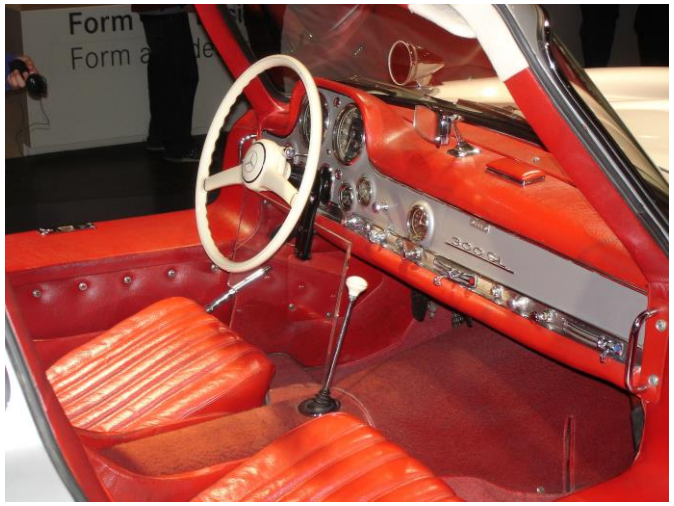
Software in modern cars

- Modern automobiles are no longer mere mechanical device
- Cars are more and more driven by software



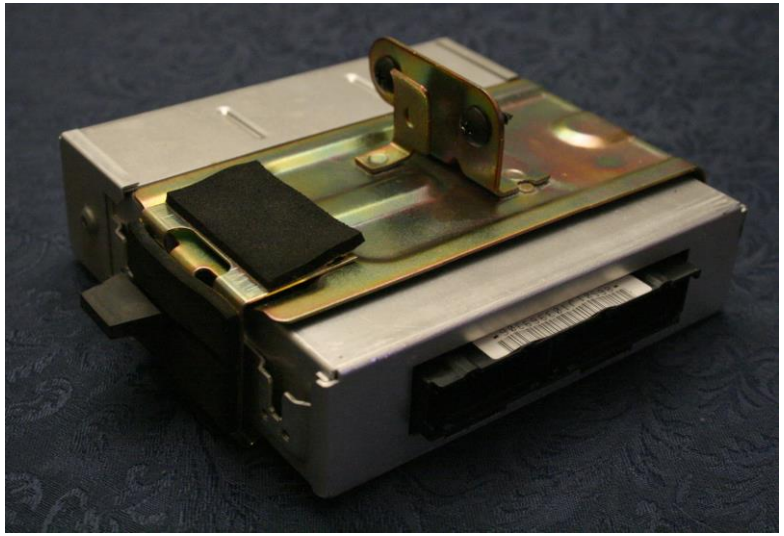
Software in modern cars

- Major advancements in efficiency and safety have introduced a range of new potential risks



Cars’ components : ECU

- ECU (Electronic Control Unit) : controls the electronical systems of a vehicle



Cars’ components : ECU (history)

- Motivation to use ECU : Improve efficiency

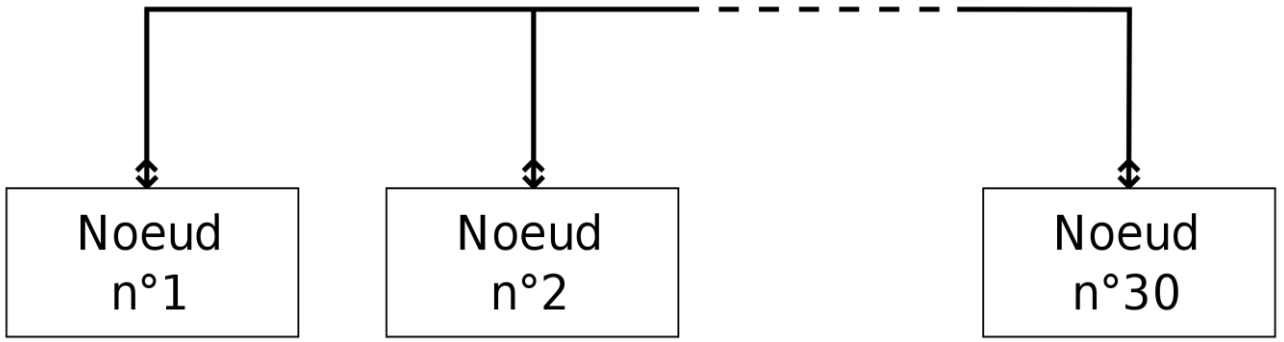
- To measure the oxygen present in exhaust fumes then adjust fuel/oxygen mixture

Cars’ components : ECU (coupling)

- Many features require complex interactions across ECUs
- Active Cruise Control (ACC) : systems scan the road and automatically adapt acceleration

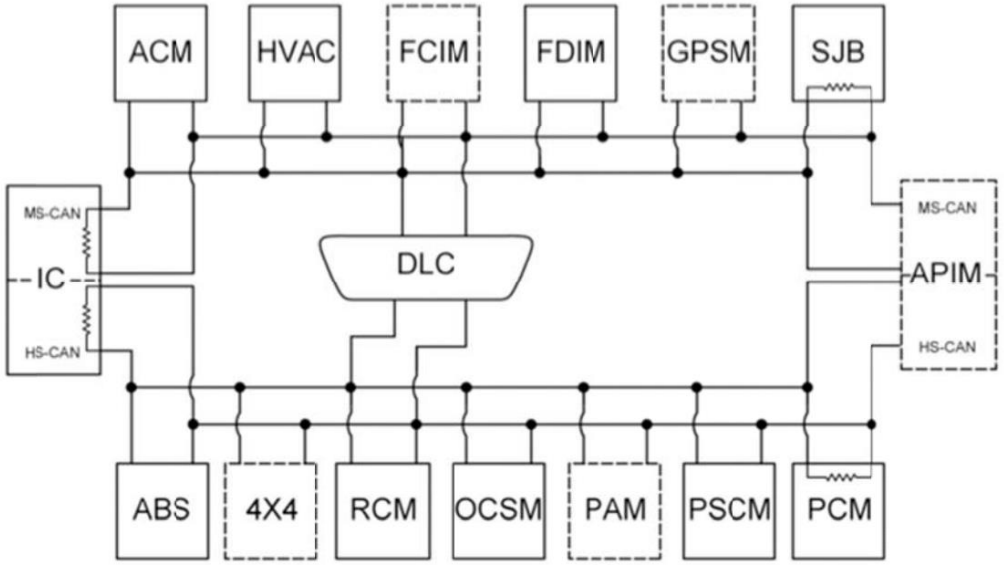
Cars’ components : CAN

- CAN bus (Controller Area Network) : allow devices to communicate with each other without host computer
- Broadcast



Cars’ components : CAN

- High Speed and Low Speed CAN bus connects the components
- «Bridged» : example of Central Locking systems (CLS)

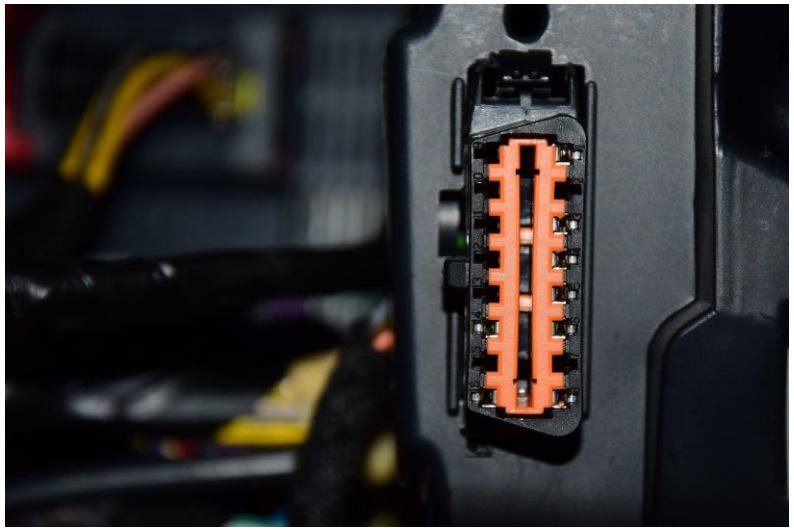


Cars' components : CAN

Component	Functionality	Low-Speed Comm. Bus	High-Speed Comm. Bus
ECM	*Engine Control Module* Controls the engine using information from sensors to determine the amount of fuel, ignition timing, and other engine parameters.		✓
EBCM	*Electronic Brake Control Module* Controls the Antilock Brake System (ABS) pump motor and valves, preventing brakes from locking up and skidding by regulating hydraulic pressure.		✓
TCM	*Transmission Control Module* Controls electronic transmission using data from sensors and from the ECM to determine when and how to change gears.		✓
BCM	*Body Control Module* Controls various vehicle functions, provides information to occupants, and acts as a firewall between the two subnets.	✓	✓
Telematics	*Telematics Module* Enables remote data communication with the vehicle via cellular link.	✓	✓
RCDLR	*Remote Control Door Lock Receiver* Receives the signal from the car's key fob to lock/unlock the doors and the trunk. It also receives data wirelessly from the Tire Pressure Monitoring System sensors.	✓	
HVAC	*Heating, Ventilation, Air Conditioning* Controls cabin environment.	✓	
SDM	*Inflatable Restraint Sensing and Diagnostic Module* Controls airbags and seat belt pretensioners.	✓	
IPC/DIC	*Instrument Panel Cluster/Driver Information Center* Displays information to the driver about speed, fuel level, and various alerts about the car's status.	✓	
Radio	*Radio* In addition to regular radio functions, funnels and generates most of the in-cabin sounds (beeps, buzzes, chimes).	✓	
TDM	*Theft Deterrent Module* Prevents vehicle from starting without a legitimate key.	✓	

Cars’ components : OBD-II

- On-Board Diagnostic (OBD-II) : port under the dash in almost every modern vehicles
- It provides direct and standard access to internal automotive networks



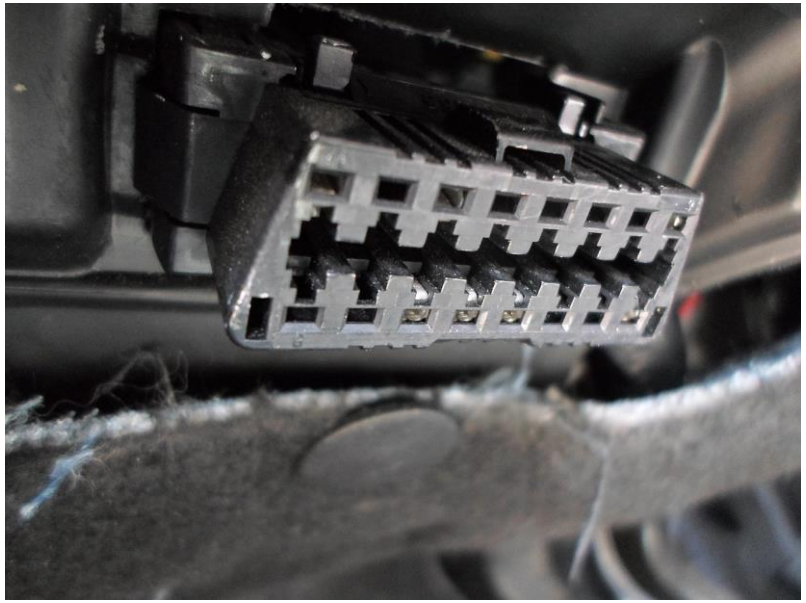
Transfer protocol : ISO-TP

- International standard for sending data packets over CAN bus
- Publish and subscribe model (broadcast)
- One or more metadata bytes to the beginning of each CAN packets (PCI, Protocol Control Information)
- The ID of the packet (first two bytes) represent also a measure of the priority (low ID = high priority)

ID: 0760, Len: 08, Data: 10 82 FF 00 00 00 00 00

External connection to the CAN bus

- Physical connection to the OBD-II port via a OBD-II adapter cable
- Wireless connection via Bluetooth, radio, …



Retrieve sensitive informations

- Easy to sniff CAN packets because of broadcast transfer
- Understand used protocol
- Identify the actions triggered by the packets

Attacks via CAN bus : speedometer hack

- Isolate the packets sent to the RPM display and replay it
- In the Ford Escape 2010, it is controlled by packets with ID 0201 on the high speed connector

ID: 0201, Len: 08, Data: AA BB 00 00 CC DD 00 00

- AA BB : RPM displayed
- CC DD : speed displayed

Attacks via CAN bus : DOS

- Flood the CAN network with packets containing ID 00 00 (highest possible priority)
- Every other packets will be ignored
- By attacking this way while the car is still shut down, the vehicle will never start

Attacks via CAN bus : Diagnostic packets

- Authentication needed to send diagnostic packets (challenge-response)
- The ECU and the sender share a cryptographic function and a key
- The sender request a cryptographic seed to the ECU
- The sender encrypt the obtained seed and send it back to the ECU to prove that it has the key

Attacks via CAN bus : Diagnostic packets

- Some cars always use the same seed, meaning that if we sniff one time the encrypted seed, we can always use it to authenticate

- Ford Escape 2010 uses different pseudo-random seed, so we need the key in order to authenticate

- It uses 407 keys that do not have a high entropy such as:

JAMES
MAZDA
MazdA
mAZDa
PANDA

Attacks via CAN bus : engage brakes

- Send *DiagnosticCommand B1003C*

- Second parameter of one byte gives how much the brakes should be applied

ID: 0760, Len: 08, Data: 04 B1 00 3C FF 00 00 00

How to prevent these attacks

- Observe the frequency of the packets sent in a normal routine
- Remote patch system in order to regularly patch vehicle

Thanks for your attention !

Questions ?