UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

Dipartimento di Ingegneria
"Enzo Ferrari"

Automotive Cyber Security

Lecture 1 – Introduction

Mirco Marchetti

University of Modena and Reggio Emilia

mirco.marchetti@unimore.it

Lecturer

- Mirco Marchetti
  - Associate professor at the Department of Engineering “Enzo Ferrari”, University of Modena and Reggio Emilia
  - Deputy director of the Interdepartmental Research Center on Safety and Security (CRIS)
  - Lecturer of “computer networks and protocols” and (ICT) “cyber security”
  - Experienced researcher in automotive cyber security
  - Often wears nerdy t-shirts
- Office hours
  - Always ask for an appointment by email mirco.marchetti@unimore.it
  - Include [ACS] in the subject of all emails related to this course. That will increase your chances of a timely answer…
  - … in case you do not receive a timely answer, resend after 48 hours ☺
  - Office: DIEF, building MO27, left side, second floor
  - Lab: CRIS, DIEF, building MO27, left side, second floor

Main topics of this course

- Introduction to automotive cyber security
- Architecture and vulnerabilities of in-vehicle cyber systems
- Discussion of known cyber attacks to modern vehicles
- Design and implementation of secure vehicles
- Current and future solutions for the detection of cyber attacks
- Security issues of V2X communications

Lectures

- Timetable
  - Tuesday 17:00-18:30, room P1.6
  - Wednesday 16:00-18:30, room P1.5

- Try to be interactive!
  - There are no silly questions
  - Do not be afraid of asking questions in English
  - You can also ask them in Italian

Final exam

- One final oral exam.

Exam schedules

- Exam days to be defined. Tentative exam schedule:
  - Mid January 2024
  - End January 2024
  - Mid February 2024
  - June 2024
  - July 2024
  - September 2024

- Dates will be posted on esse3 (UniMoRe and UniPr).

… what about AFTER the exam?

- I can supervise or co-supervise thesis related to automotive cyber security, both in the industry and in our research lab

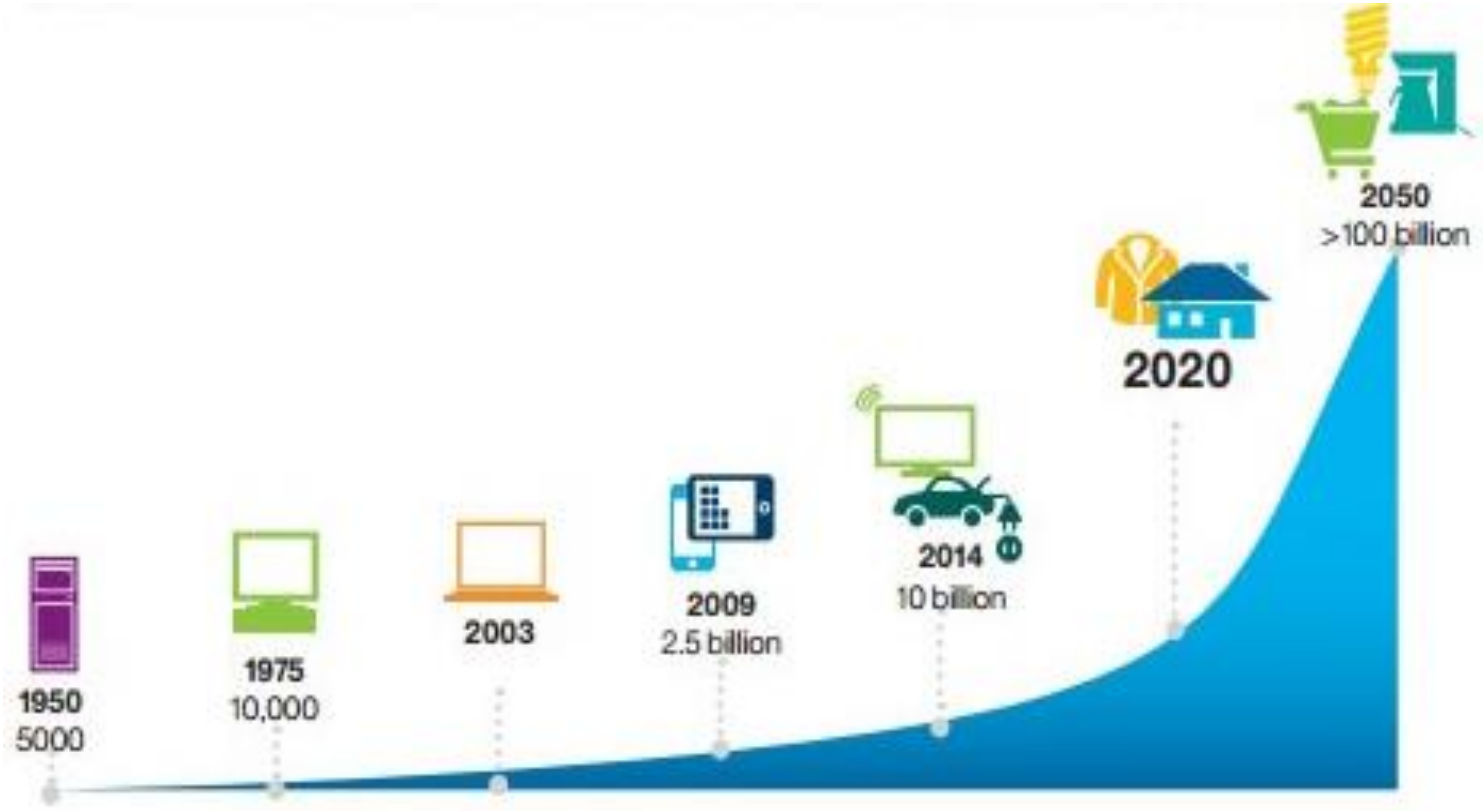
Communication channels

- Course Website (Moodle)
  - Slides
  - Announcements ← check them frequently!
  - Streaming and recordings

- Yes, lectures will be streamed and recorded through Microsoft Teams (linked from the course website). Keep in mind that streaming and recording will be “best effort”: they are meant to be a tool for helping you, not a drop-in replacement for attendance.

Let’s begin!

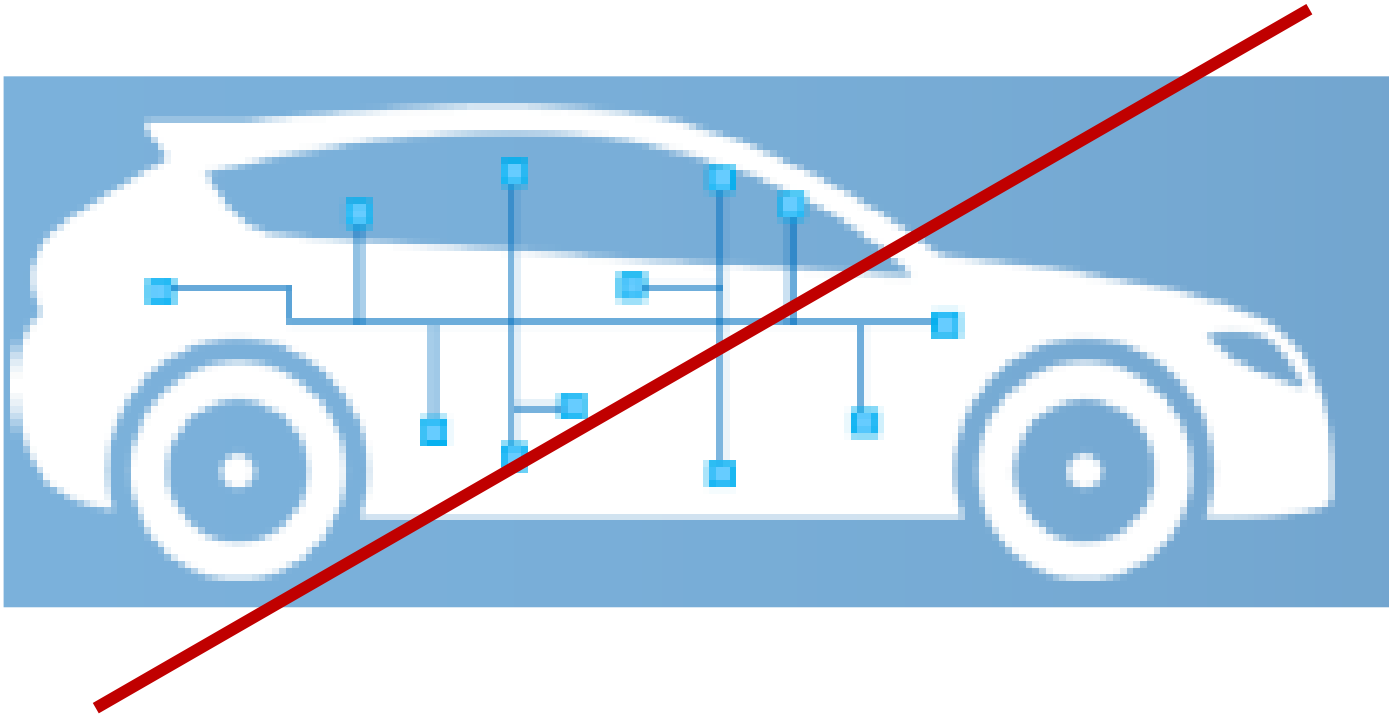
Interconnected/Autonomous vehicles in the context of cyber-physical systems



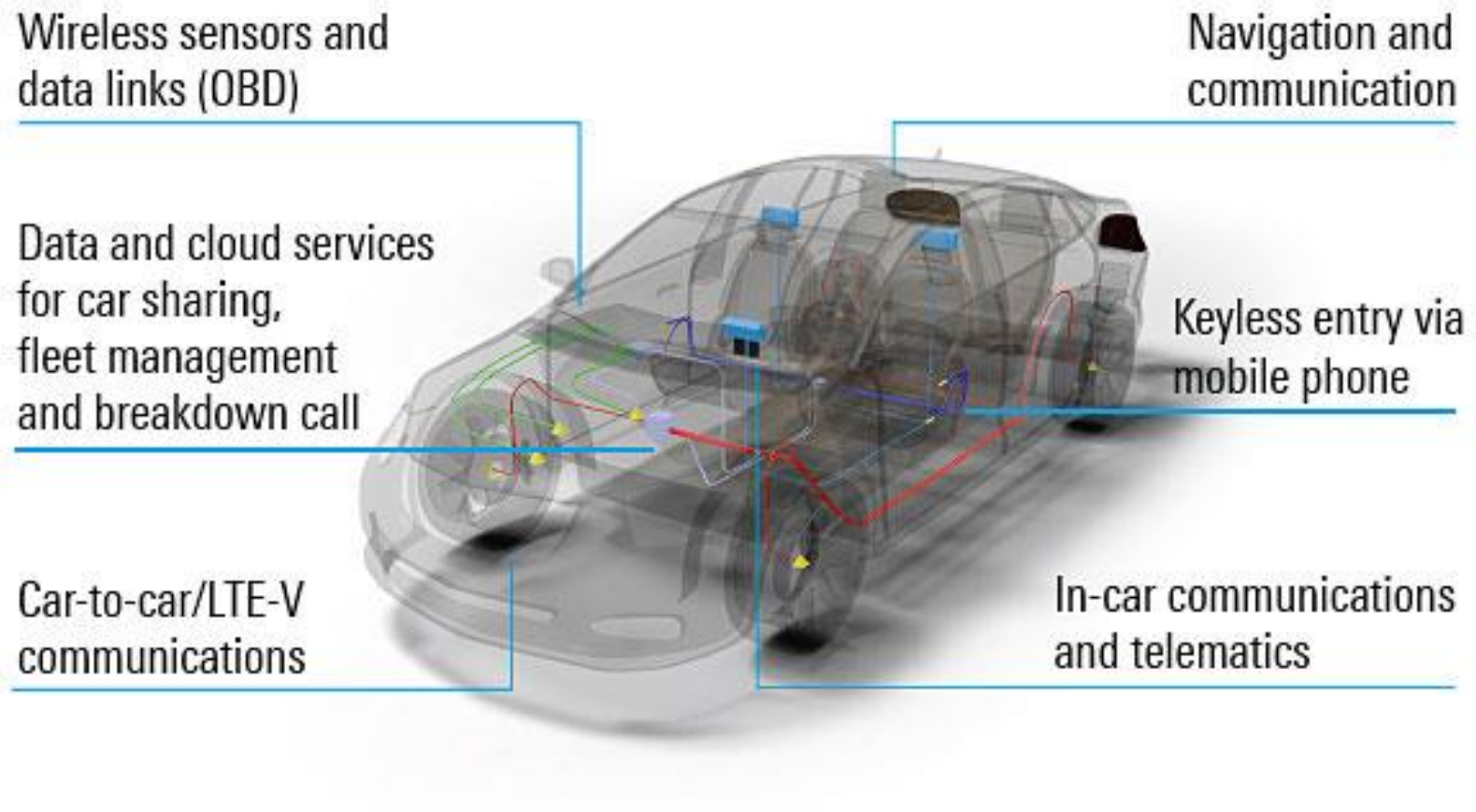
Cyber-physical system: definition

A **cyber-physical** (also styled **cyberphysical**) **system** (**CPS**) is a mechanism that is controlled or monitored by computer-based algorithms, tightly integrated with the Internet and its users. In cyber-physical systems, *physical and software components are deeply intertwined, each operating on different spatial and temporal scales, exhibiting multiple and distinct behavioral modalities, and interacting with each other in a lot of ways that change with context*. Examples of CPS include smart grid, autonomous automobile systems, medical monitoring, process control systems, robotics systems, and automatic pilot avionics.

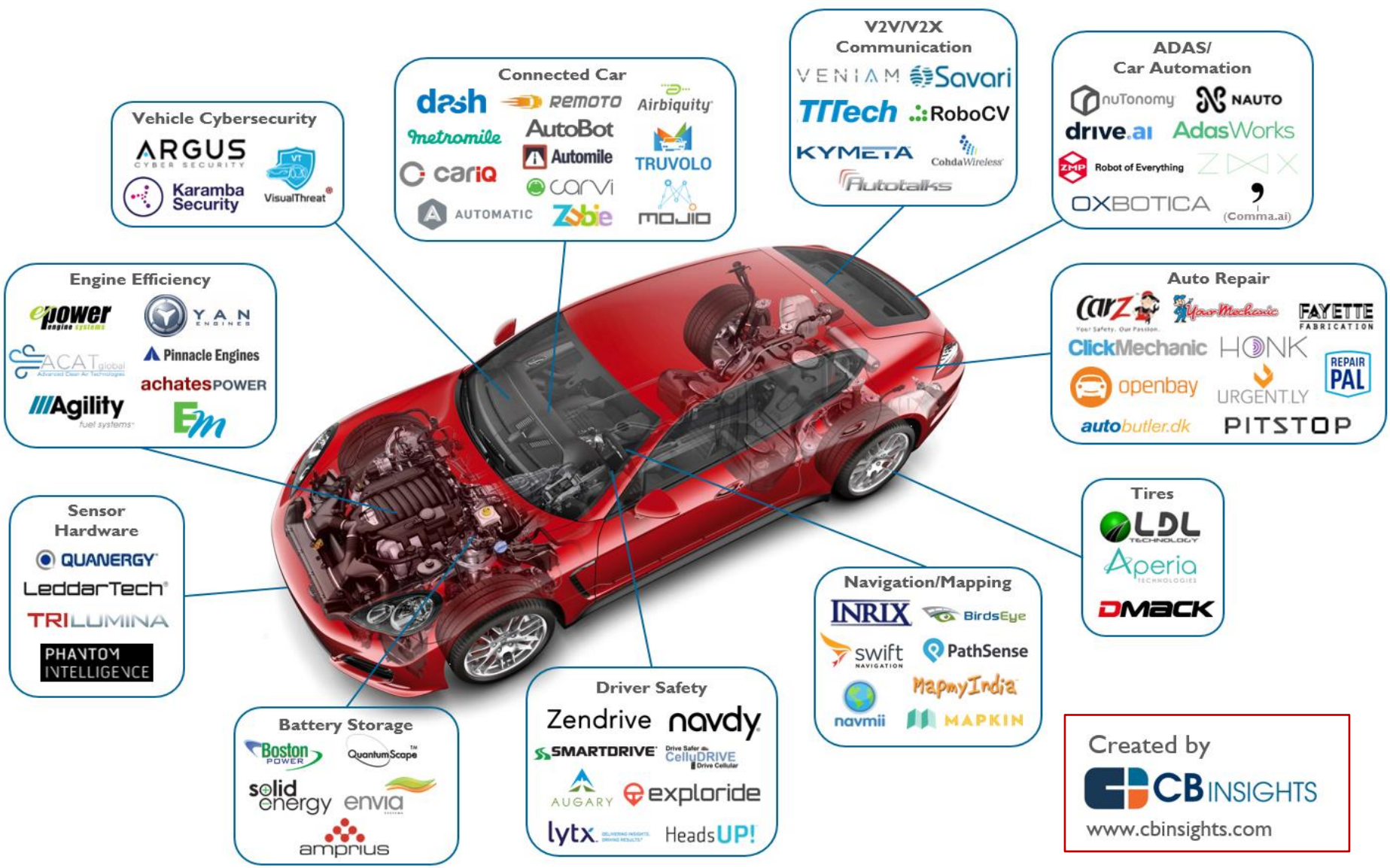
Typical model of a vehicle



Connected car



Modern vehicles are complex ecosystems



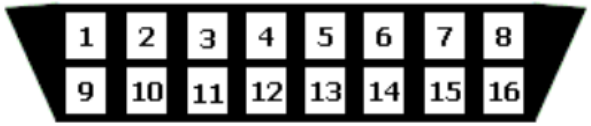
Created by CB INSIGHTS
www.cbinsights.com

Terms

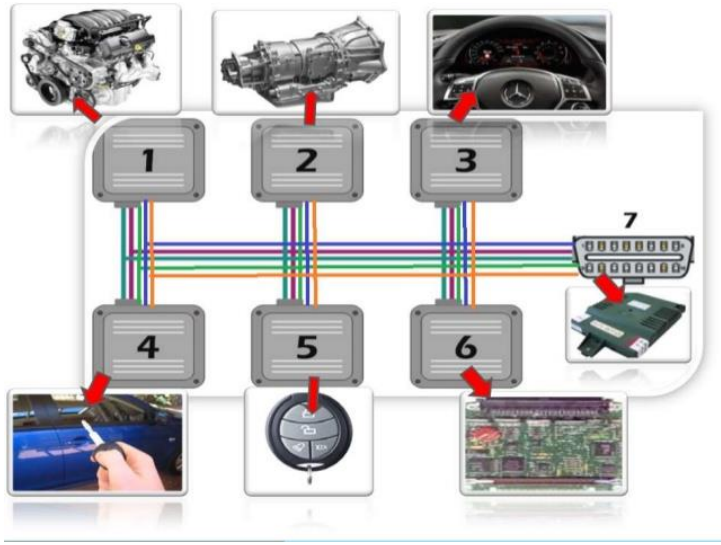
- **OEM** – Original Equipment Manufacturer (that is, car maker)
- **Tier One** – direct major suppliers of parts to OEMs
- **Tier Two** – key suppliers to Tier one suppliers, without supplying a product directly to OEM companies. (One company may be a Tier one supplier to one company and a Tier two supplier to another company, or may be a Tier one supplier for one product and a Tier two supplier for a different product line.)
- **Tier Three** – suppliers to Tier two firms
- **Tier Four** – providers of basic raw materials, such as steel and glass, to higher-tier suppliers

Inside car

- **OBD** - On-Board Diagnostics
  (new version OBD-II)



- **CAN** – Controller Area Network (ISO 11898). Others: LIN, FlexRay, MOST, Ethernet

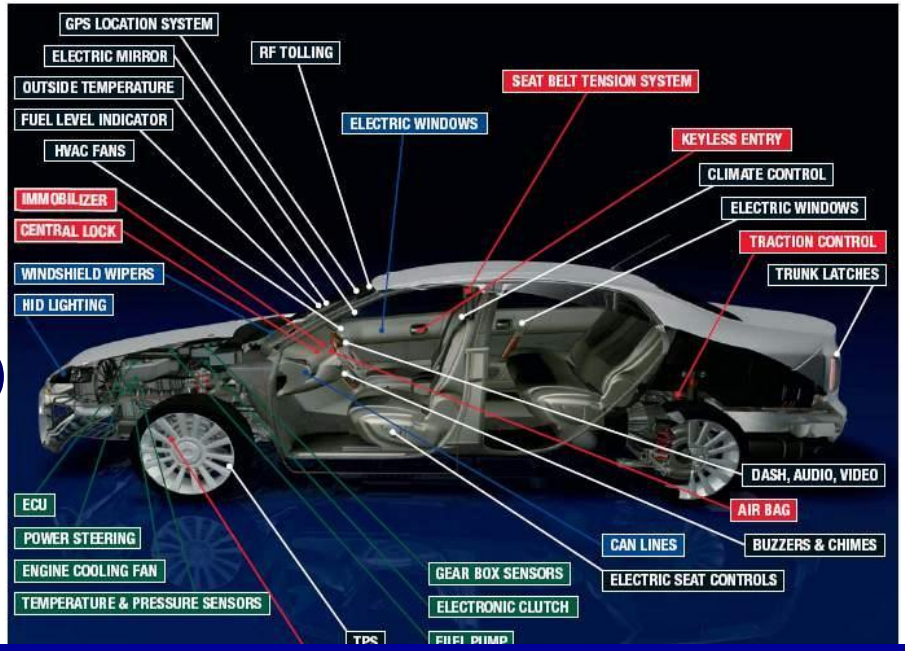


- **ECU** – Electronic Control Unit
  (not to confuse with Engine Control Unit)

Types of ECU

There is no single computer but multiple modules (50-150) connected through one or multiple CAN bus

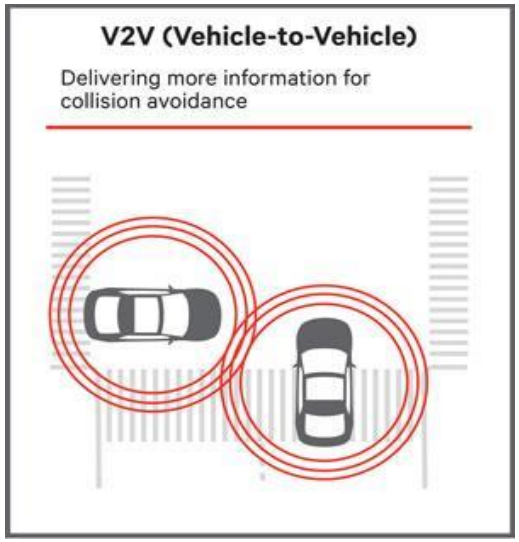
- Electronic/engine Control Module (ECM)
- Powertrain Control Module (PCM), often both engine and transmission
- Transmission Control Module (TCM)
- Brake Control Module (BCM)
- Central Control Module (CCM)
- Central Timing Module (CTM)
- General Electronic Module (GEM)
- Body Control Module (BCM)
- Suspension Control Module (SCM)
- …

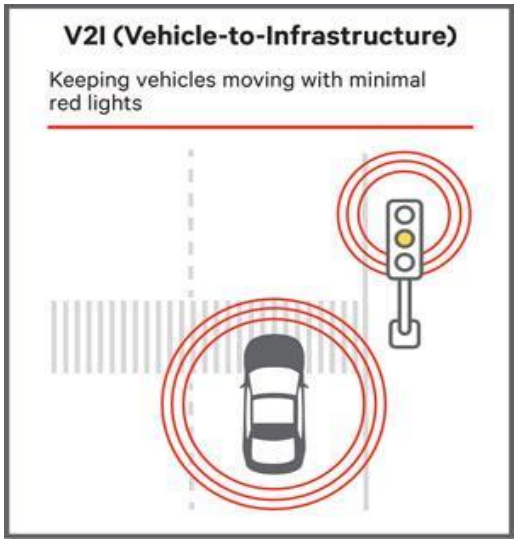


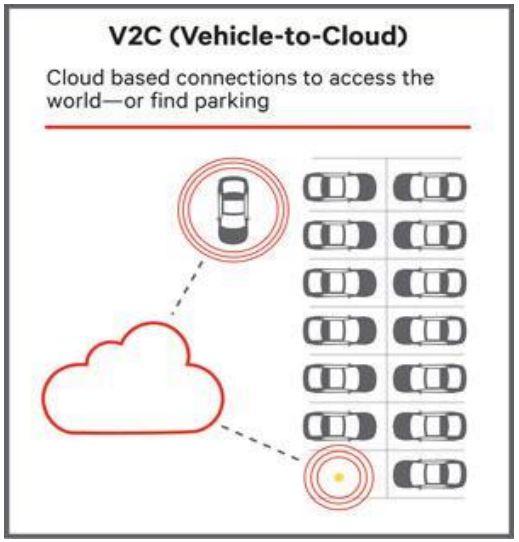
Outside car

- **OTA** – Over The Air
- **FOTA** – Firmware Over The Air

- **V2X**







Evolution of automotive technologies

1990	2015	2030
		
No information security issues	Remote cyberattacks documented by researchers	As vulnerable as a PC connected to the Internet
Very few electronic components	Hundreds of connected electronic components	Full-fledged computer network
No software-defined behaviors	Safety-relevant behaviors controlled by software	Everything is controlled by software
No external connectivity	External connectivity (Internet, OTA, …)	Integrated network connectivity

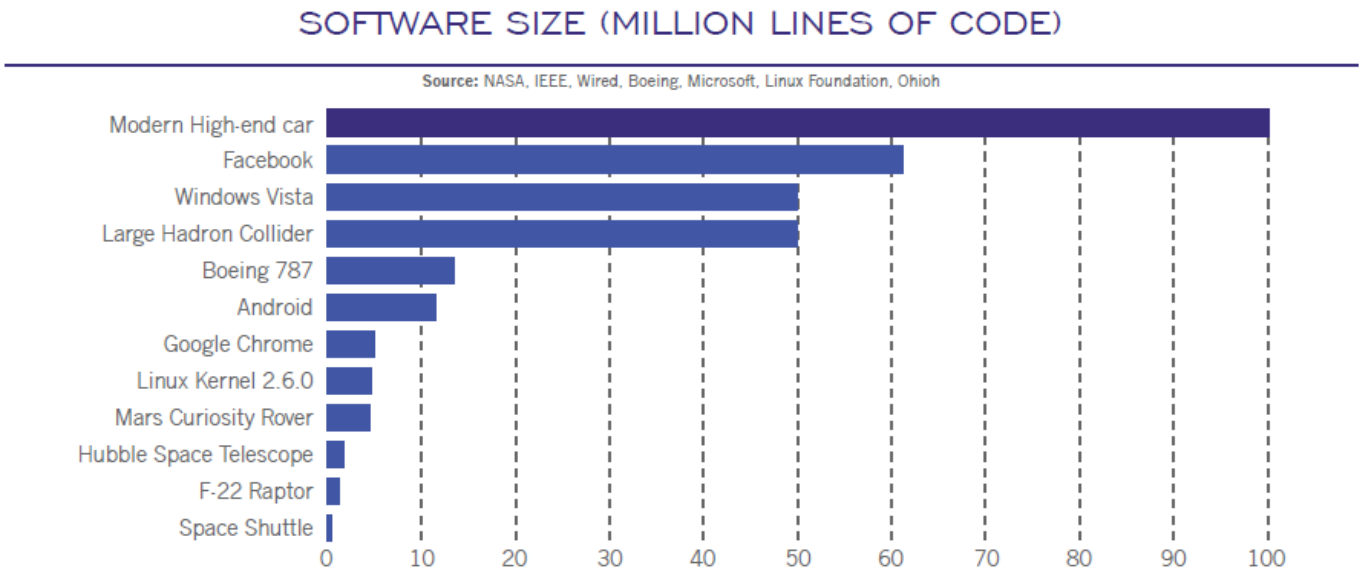
Evolution of automotive technologies

1990	2015	2030
		
No information security issues	Remote cyberattacks documented by researchers	As vulnerable as a PC connected to the Internet
Very few electronic components	Hundreds of connected electronic components	Full-fledged computer network
No software-defined behaviors	Safety-relevant behaviors controlled by software	Everything is controlled by software
No external connectivity	External connectivity (Internet, OTA, …)	Integrated network connectivity


SECURITY ISSUES

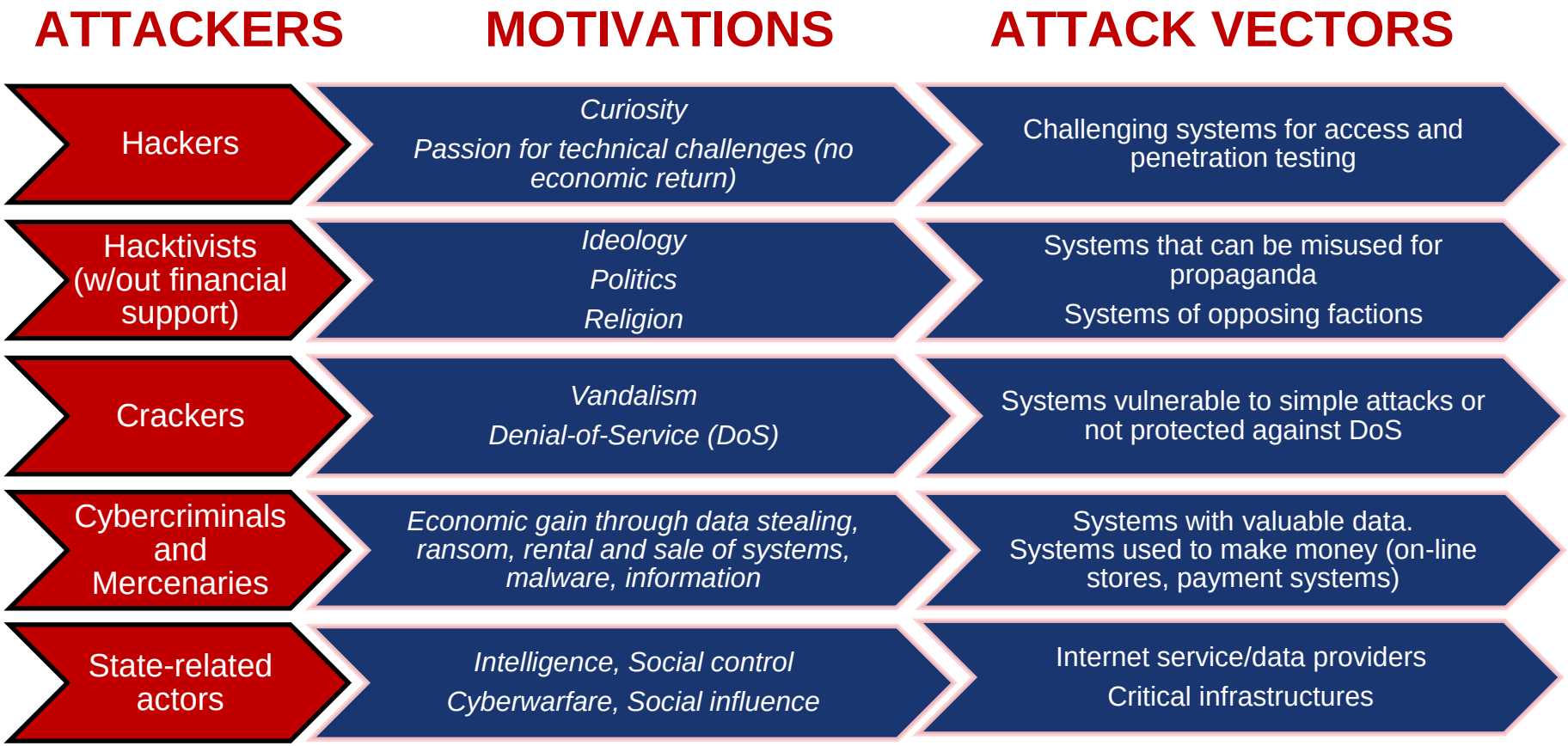
Vulnerabilities due to increasing complexity

1. **Car software**
   - **Today, especially for infotainment systems**
   - **Tomorrow, especially for autonomous driving**



2. **Number of ECUs: from 50 to 150**
3. **Traffic mostly in CAN buses**

We know everything about cyber attacks in IT



And even about cyber defenses: TECHNOLOGIES, GOVERNANCE, STANDARD, BEST PRACTICES, …

Three unpleasant truths

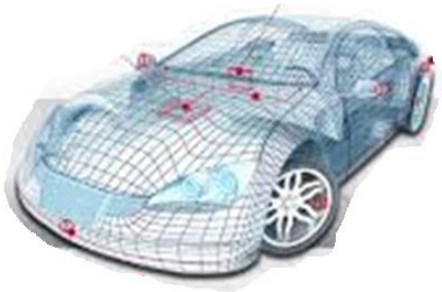
1. **No matter how well an organization defends itself, there will always be vulnerabilities to cyberattacks**
   - Advanced threats exploit human nature AND technology (100+ new malware are created every minute: *one for You*, *and You*, *and You*, …)

2. **Governments must defend primarily themselves and cannot protect your business everyday**
   - "There are two kinds of companies in the United States: those who have been hacked… and those who don't know yet" [James Comey, FBI Director, Oct. 2014]

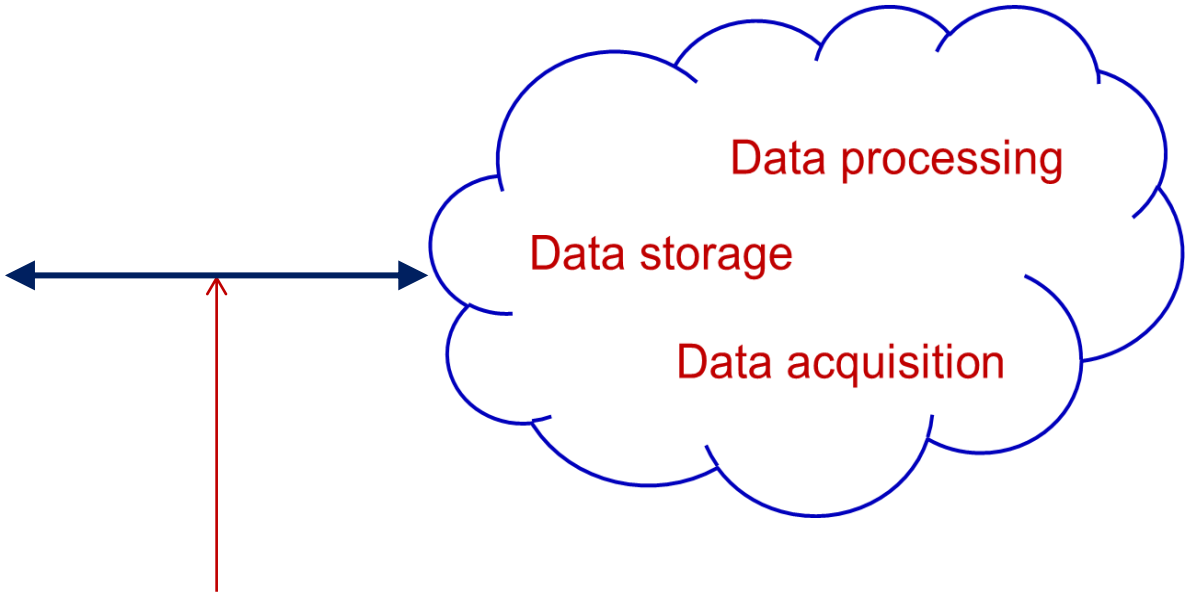
3. **Technological defensive tools are necessary but not sufficient, especially for the foreseeable future that will include "smart objects"**
   - Magic Shield and Silver Bullet against cyberattacks do not exist

Who are the attackers?

Attackers with access to the vehicle



Insiders



External attackers

(from the Internet, mobile broadband networks, or the external environment in general)

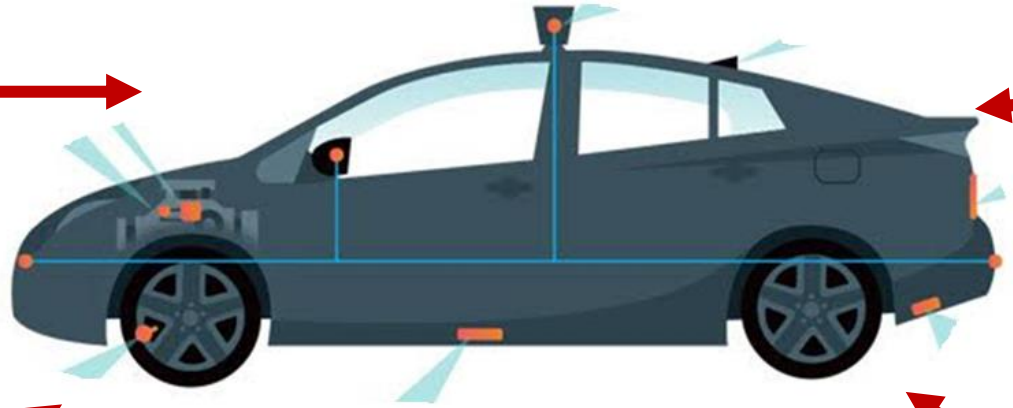
Competent attackers

There are competent and motivated individuals behind advanced attacks

1. They keep studying
2. They exchange information
3. They are eager to experiment novel forms of attacks against the most recent technologies
4. They continuously adapt their attack vectors (not only technological) to overcome defenses, e.g.,
   - **Technology**
   - **Intelligence** (open, grey, dark sources)
   - **Psychology** (leveraging trust, rule inobservance, habit, narcissism, self-confidence, dissatisfaction, ideology, etc.)

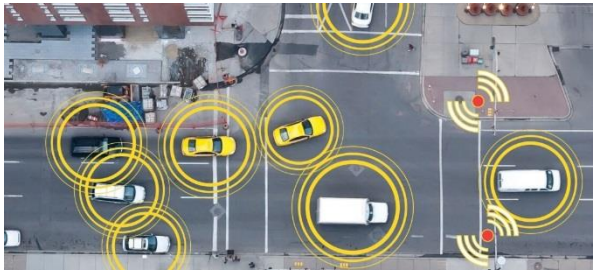
Attackers can leverage multiple penetration vectors

Smartphone



Infotainment

OTA-V2I



OTA-V2V

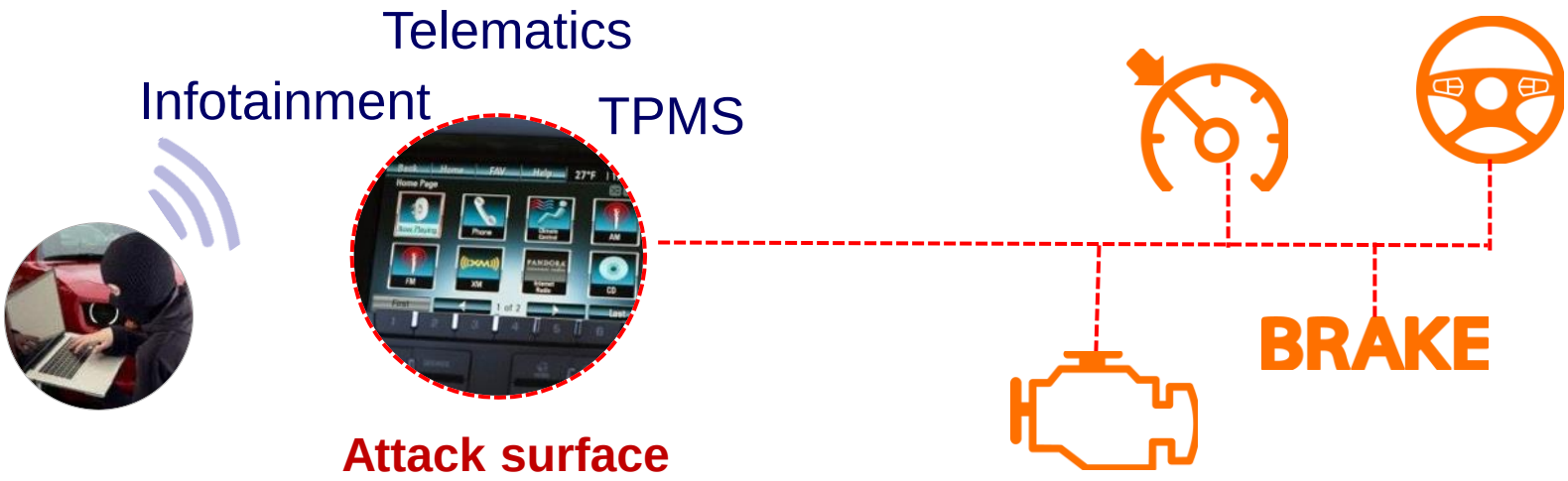
ODB-II

Bluetooth

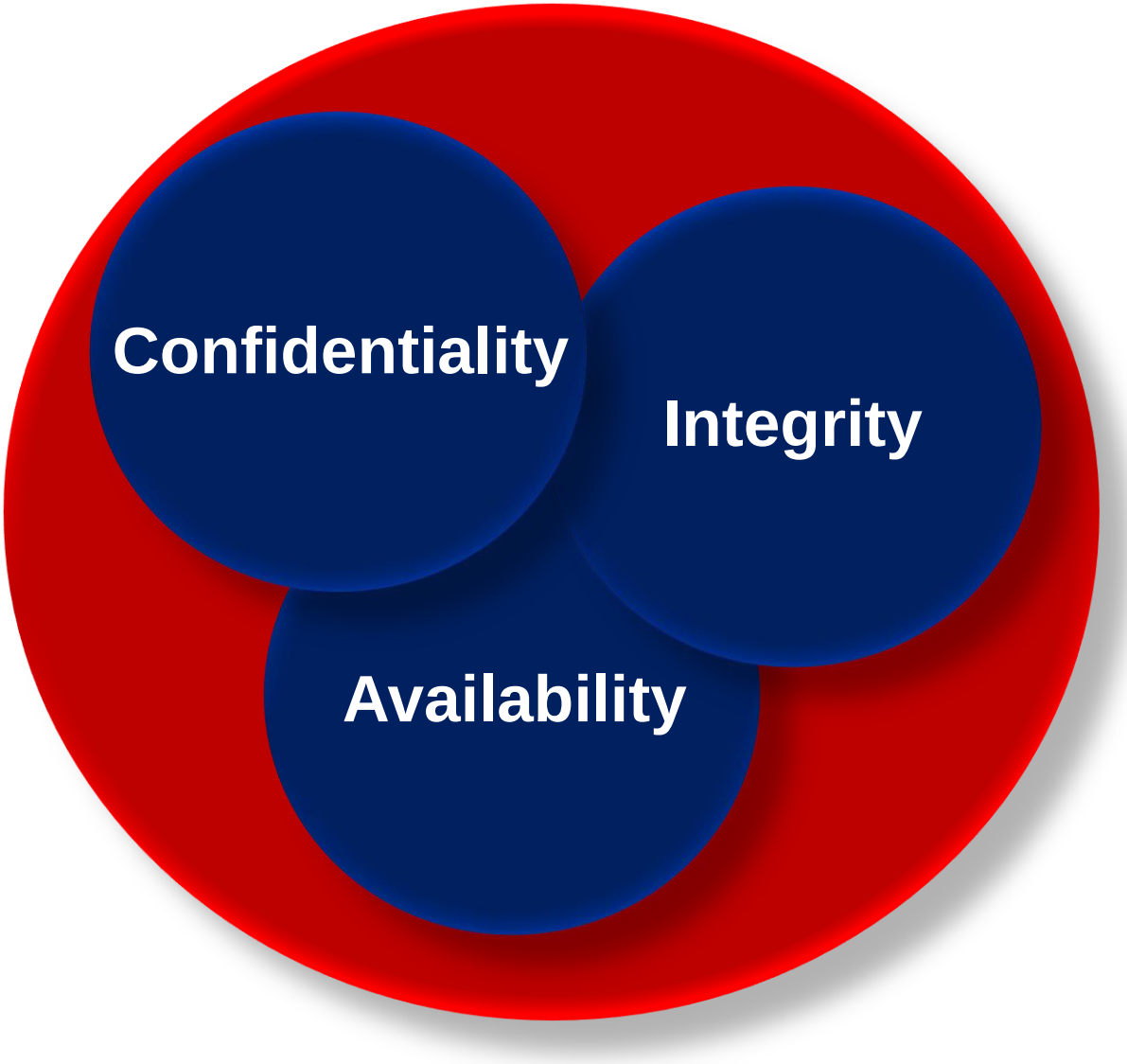
Attack vectors through Infotainment

- Bluetooth, WiFi, keyless entry
- Cellular gateways (e.g., modems, Femtocells)
- OnStar or OnStar-like digital radio
- Insecure OS configuration, update media, inter-process communications
- Android app on the driver’s phone synched to the car’s network
- Malicious audio file burned onto a CD in the car’s stereo
- Radio-readable information monitoring systems
- …

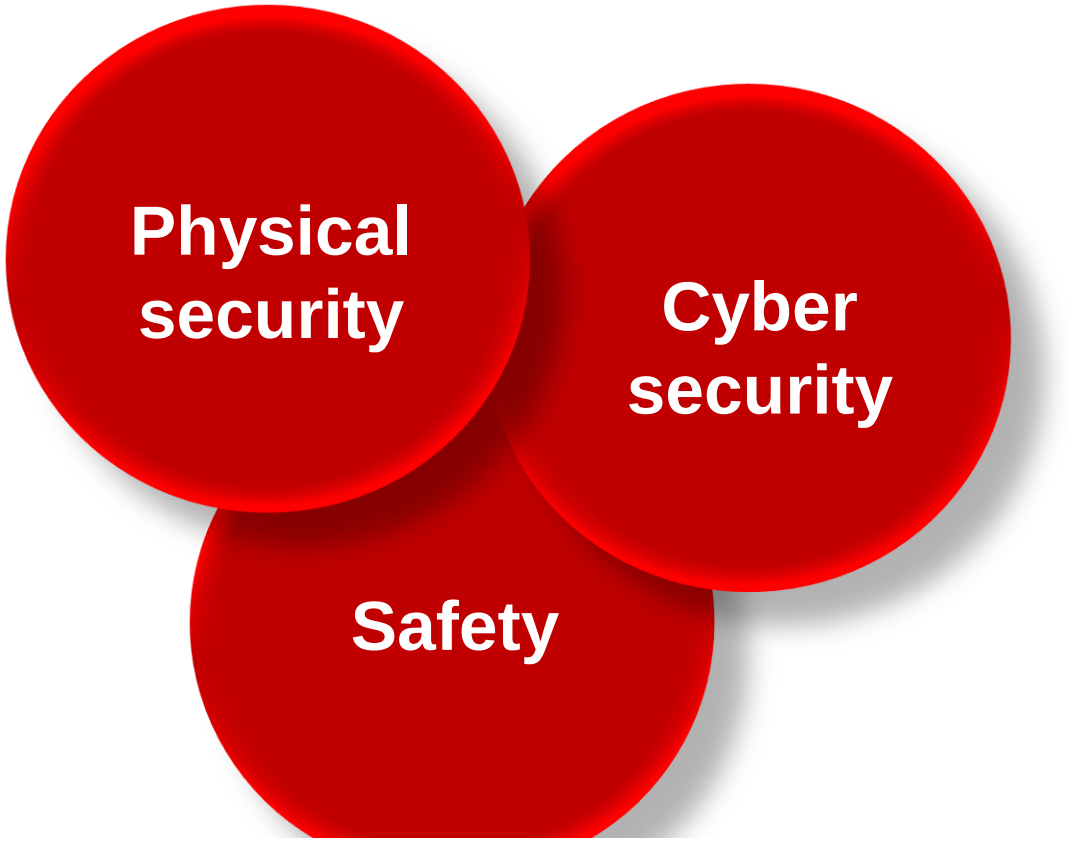
From external to internal CAN bus and then…



Cyber security



In automotive industry, all securities and safety merge



"Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment"

Security threats

- **Physical insecurity** (***light***): Annoyance attacks, such as blinking LEDs, raising sounds, adjusting the mirrors, false readings of speedometer and fuel gauge
- **Physical insecurity** (***serious***): Car theft by unlocking doors, bypassing immobilizer, etc.

- **Cyber insecurity - *Confidentiality***: eavesdropping data, car location
- **Cyber insecurity – *Integrity***: attack on GPS navigation system
- **Cyber insecurity – *Availability***: prevent ignition, ransomware

Safety threats:
incidents, assassination, terrorism

- Turn off the engine
- Force acceleration of the vehicle
- Disable breaks
- Tighten seat belts
- Inflate airbags
- Take control of the steering wheel

Main goals of cyberattacks

Espionage

Sabotage (*infrastructure*)

Sabotage (*people*)

Theft (*data and money*)

Theft (*property*)

Reputation damage

Anything different for vehicles?

Example: RollJam

- We will cover it in detail in later lectures
- RollJam ($32) hacks keyless entry systems, alarm systems and garage door openers
- Proven on Nissan, Cadillac, Ford, Toyota, Lotus, Volkswagen, and Chrysler vehicles; Cobra and Viper alarm systems; and Genie and Liftmaster garage door openers

- Reference: http://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/

Example: On-Star in GM

- We will cover it in detail in later lectures
- Any On-Star equipped GM car could be located, unlocked and started via the phone app
- **It uses SSL encryption, but it does not properly check the certificate**

- Reference: http://arstechnica.com/security/2015/07/ownstar-researcher-hijacks-remote-access-to-onstar/

Example: Dongle firmware

- The firmware running on the dongle is minimal and insecure
- It does no validation or signing of firmware updates, no secure boot, no cellular authentication, no secure communications or encryption, no data execution prevention or attack mitigation technologies…

- Reference: http://www.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure/

Example: TomTom

- TomTom OBD-II dongle used to reduce insurance rates for customers
- Hacked by UCSD by sending SMS messages to control the CAN bus to control brakes, steering, etc. Confirmed in Corvette, Prius, Escape

- Reference: http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/

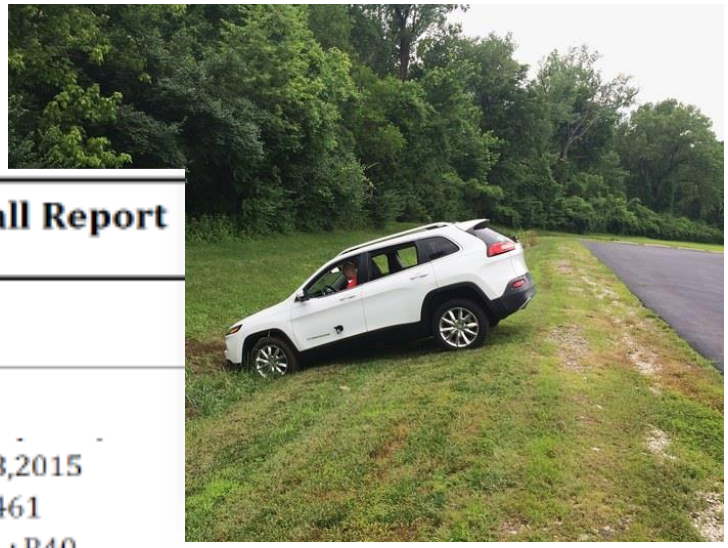
Example: Dealers and Mechanics

- Infections of equipment used by mechanics and dealerships to update car software and run vehicle diagnostics

- An infected vehicle can spread an infection to a dealership's testing equipment, which in turn would spread the malware to every vehicle the dealership services

Successful attack on Jeep Cherokee (*by Miller and Valasek*, Wired 2015)

1. Remote exploitation over the Internet
2. Jailbreak infotainment system
3. Reverse engineer radio's program code
4. Control over engine, steering, brakes, ...



Part 573 Safety Recall Report

Manufacturer Name :
Submission Date : JUL 23,2015
NHTSA Recall No. : 15V-461
Manufacturer Recall No. : R40

Nice videos

- https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#69f95a5b228c

- https://www.youtube.com/watch?v=MK0SrxBC1xs

- … after some background we will learn exactly what they did to achieve these results.

Jeep: A cascade of vulnerabilities

- You can directly contact a car from the Internet
- You can port scan the car
- The car listens for unauthenticated connections
- The head unit (radio/navigator) runs an OS that is not configured properly
- The head unit's application software is not secured properly
- The head unit is connected to both vehicle CAN networks: infotainment and powertrain
- Head unit navigator upgrade software delivery includes flashing tools and lots of commented script files
- The CAN interface firmware in the head unit is not protected

Fixing: even worse!

- Go to a dealer and he will take care of it

OR

- Plug in a USB flash drive you receive in the mail, then update the firmware in the head unit

- *No possibility of remote software updates*


FCA
FIAT CHRYSLER AUTOMOBILES
FCA
Safety Recall R40
Secure USB
For one time use only
IMPORTANT!
SAFETY RECALL NOTICE
IMPORTANT SAFETY RECALL INFORMATION
Issued in Accordance
With Federal Law
NHTSA
R40/ NHTSA 15V-461
RADIO SECURITY VULNERABILITY