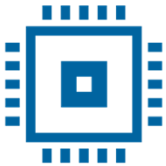
Industrial Control Systems Security (ICSS)

Session 5

17/04/2024 | Brasov | Alex Costache



Transilvania
University
of Brasov

FACULTY OF ELECTRICAL ENGINEERING
AND COMPUTER SCIENCE

Agenda

1. Course topics
2. Cyber security in automotive - introduction

3. Exercise

1.Course topics

Course topics

- Main topics covered in this lesson:
  - Introduction in automotive cybersecurity
  - Types of cyber attacks, examples
  - Exercise

Theoretical part: ~ 1h

Laboratory part: ~ 1,5h

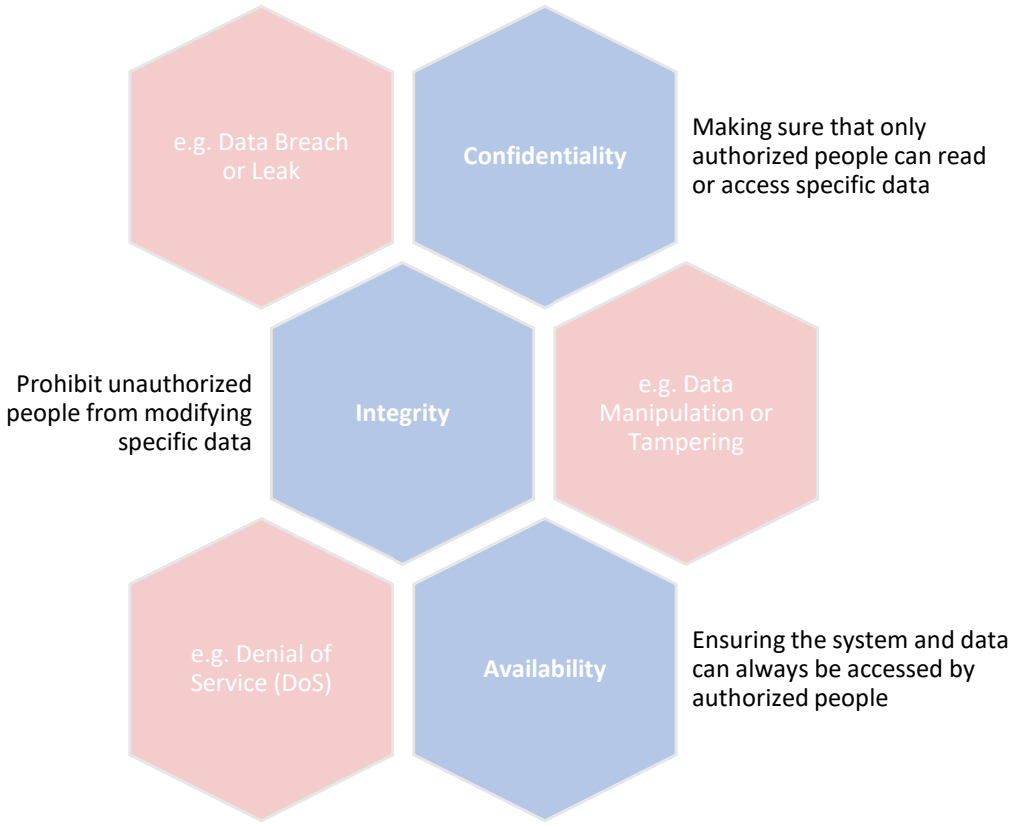
2. Cyber security in automotive

2. Cyber security in automotive

Cybersecurity: why do we need it?

- Same like physical security (locks, fences, or police officers) is used to minimize crime in the **real** world,

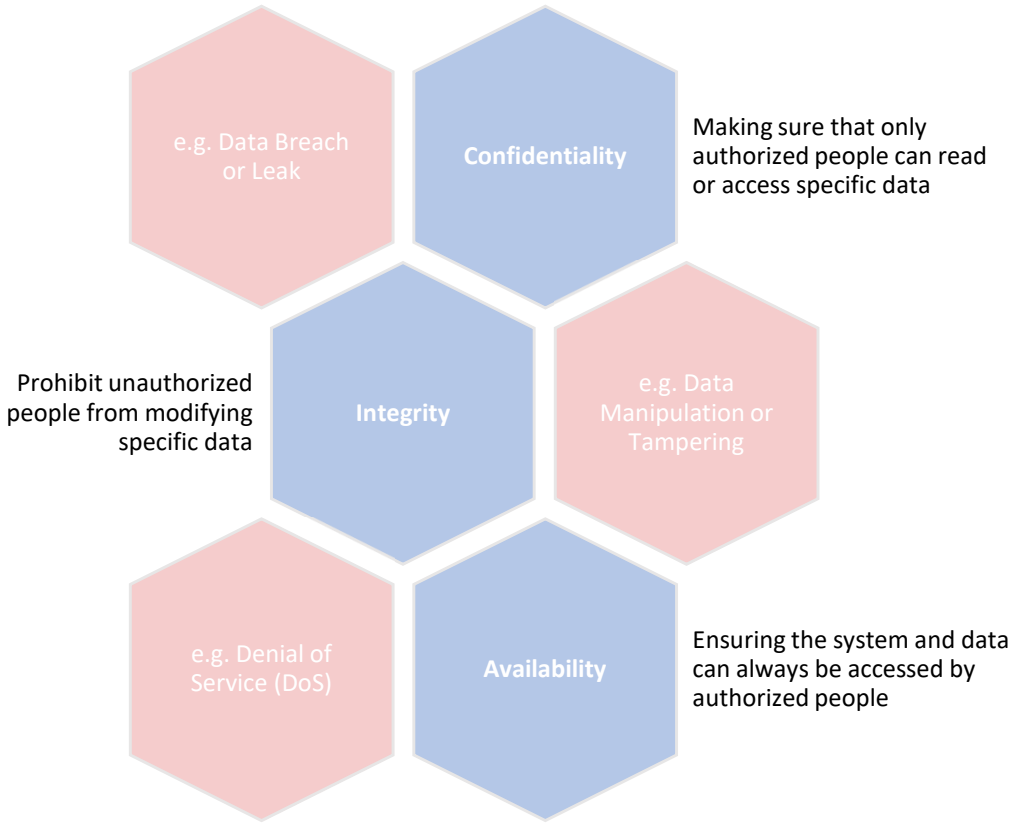
cybersecurity is used to minimize crime in the **virtual** world.



2. Cyber security in automotive

Cybersecurity: why do we need it?

- Cybersecurity -> set of techniques to protect the **secrecy** (**confidentiality**), **integrity**, and **availability** of computer systems and data against threats.



2. Cyber security in automotive

- Automotive Cybersecurity: why?

A car used to be a closed system <- this changed

A modern car:

- offers many interfaces
- contains large amount of software / computerization

2. Cyber security in automotive

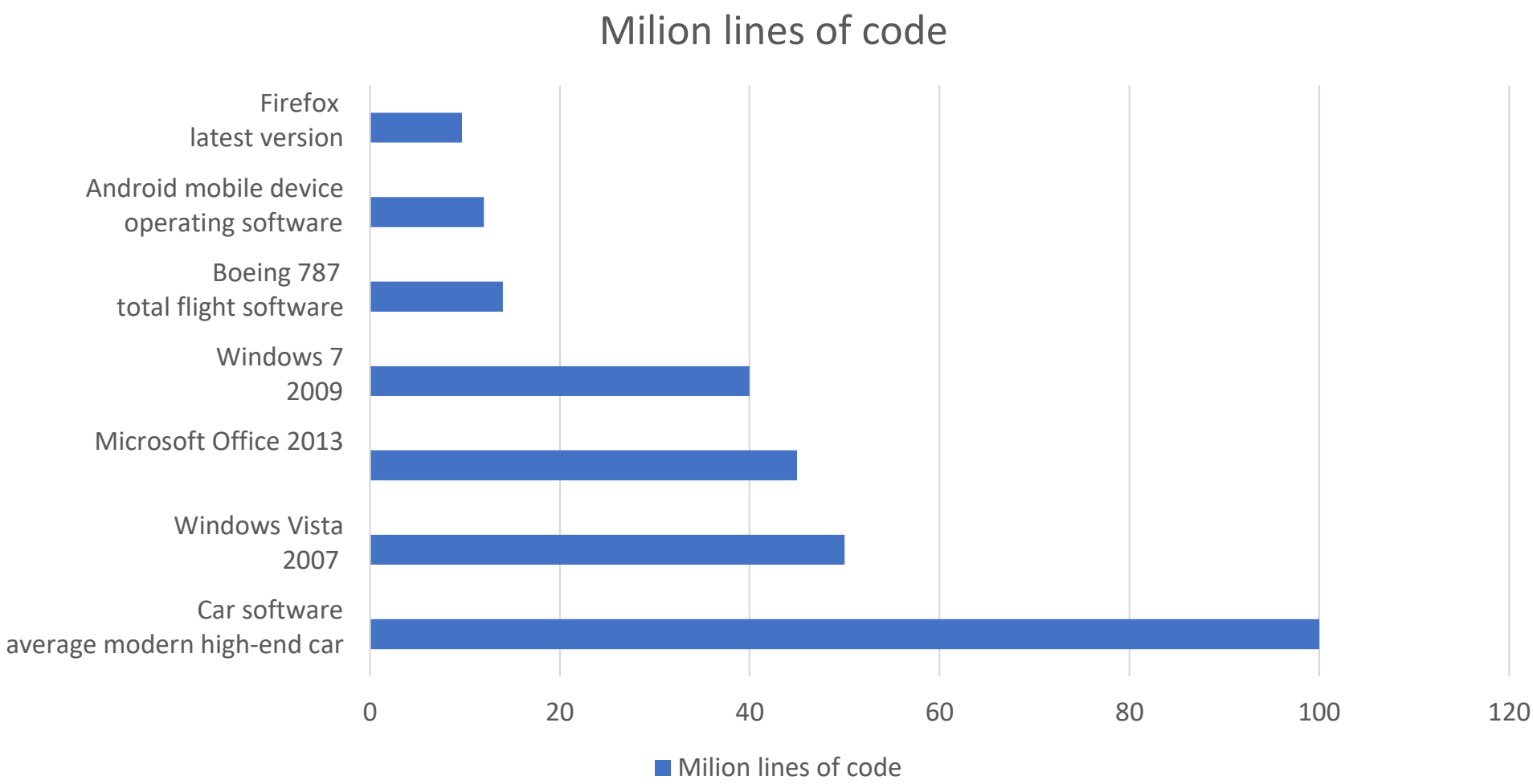
- Automotive Cybersecurity: types of attacks

  - **“White hat”:** Publicity, Research
  - **“Black hat”:** Stealing cars, unlock functionality for free, … ramsomware?

Hacking cars used to be driven mostly by academia, but in 2018 “black hat” attacks surpassed “white hat” attacks

2. Cyber security in automotive

- Complexity of car software



Source: https://informationisbeautiful.net/visualizations/million-lines-of-code/

2. Cyber security in automotive

Examples of automotive hacks (1/4)

- One of the first automotive hacks: compromise of TPMS (2010)
  - Published by researchers at University of South Carolina
  - Experimental analysis of two popular TPMSs used in a large fraction of vehicles in the United States
  - Eavesdropping of IDs to track vehicles
  - Spoofing of sensor messages due to missing authentication and input validation

TPMS - tire pressure monitoring system

2. Cyber security in automotive

Examples of automotive hacks (2/4)

- **Jeep Cherokee (2015)**
  - Security researchers Charlie Miller and Chris Valasek published at Black Hat USA 2015 the vulnerabilities of the Jeep Cherokee
  - Manipulating air conditioning, radio, windshield wipers completely remotely
  - Deactivate acceleration, deactivate brakes completely remotely
  - Resulted in callback of 1.4 million Jeeps

Article link: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/

2. Cyber security in automotive

Examples of automotive hacks (3/4)

- **GM Corvette (2015)**
  - Research Team from University of California at San Diego
  - Using an insurance dongle
  - Send text message to dongle plugged into OBD-II port
  - Remotely turn on windshield wipers
  - Remotely enable and disable brakes

Article link:
https://www.zdnet.com/article/how-to-hack-a-corvette-with-a-text-message/

2. Cyber security in automotive

Examples of automotive hacks (4/4)

- **Tesla Model-S (2016)**
  - Security researchers from Keen Security Lab
  - Remote takeover with malicious hotspot
  - Access fake website through malicious Wi-Fi hotspot
  - Control the car‘s features like braking system, changing display content, opening doors, sun roof or trunk

Article link:
https://www.theverge.com/2016/9/19/12985120/tesla-model-s-hack-vulnerability-keen-labs

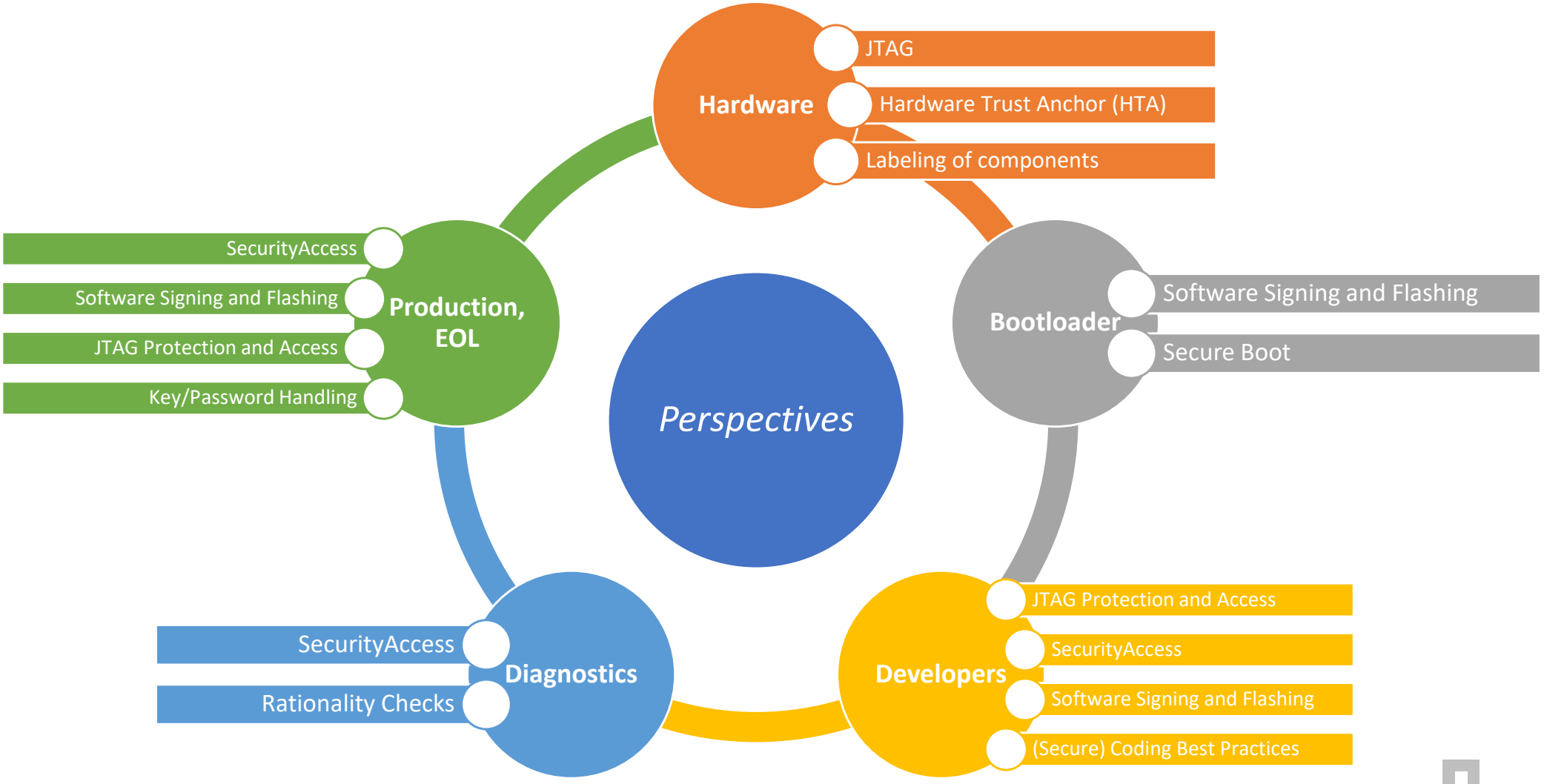
2. Cyber security in automotive

Applied protection mechanisms

1. **Secure Diagnostics**
   Protecting diagnostic functionality with challenge-response mechanism and rationality checks
2. **Secure Programming** and **Secure Boot**
   Protecting authenticity and integrity of flashed firmware with a signature
3. **Debug Interfaces**
   Disabling JTAG for unauthorized users with a password
4. **Secure On-Board Communication**
   Signing messages and verifying signatures of critical messages received via CAN

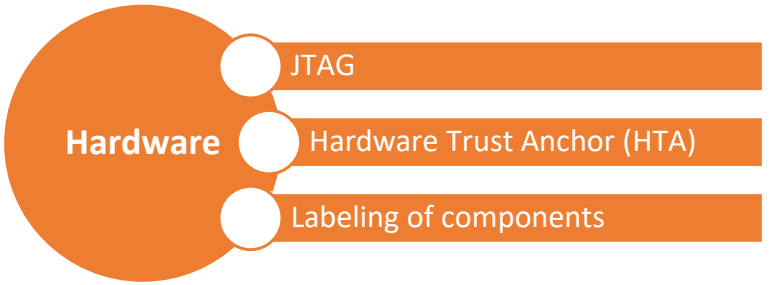
2. Cyber security in automotive

- Security perspectives in the system



2. Cyber security in automotive

- Hardware perspective:



JTAG interface:

Protect JTAG interface:

- remove JTAG connector (do not populate JTAG connector)
- JTAG pads not labeled on PCB

Labelling of components:

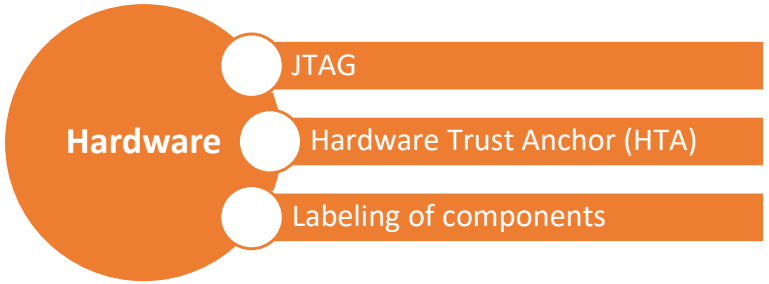
- remove the labels from the components to increase the difficulty to identify them

Hardware Trust Anchor (HTA):

- protect sensitive data in ways that software can not manipulate
- provide crypto functions

2. Cyber security in automotive

- Hardware perspective:



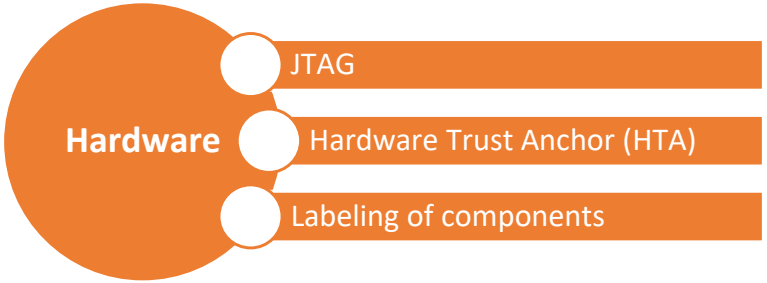
Hardware Trust Anchor (HTA):

Different standardized feature sets for HTAs:

- Secure Hardware Extension (SHE)
- EVITA concept (Secure Onboard Architecture)
- Trusted Platform Module (TPM)

2. Cyber security in automotive

- Hardware perspective:



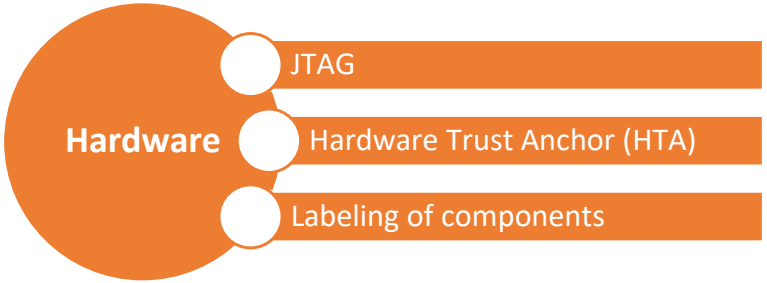
Hardware Trust Anchor (HTA):

Secure Hardware Extension (SHE)

The SHE specification defines a set of functions and a programmer's model (API) that allows a secure zone to coexist within any electronic control unit installed in the vehicle.

2. Cyber security in automotive

- Hardware perspective:



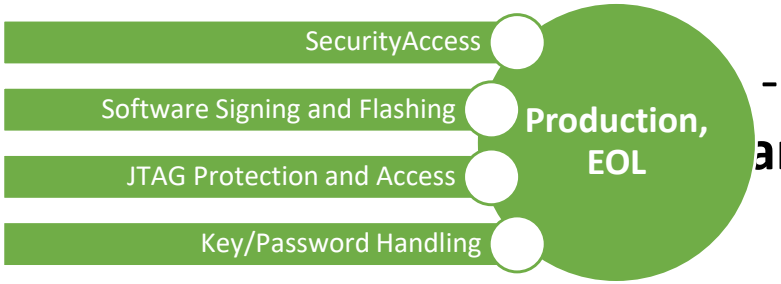
Hardware Trust Anchor (HTA):

Secure Hardware Extension (SHE)

The secure zone's most significant features are the storage and management of security keys, plus encapsulating authentication, encryption and decryption algorithms that application code
can access through the API.

2. Cyber security in automotive

- Production/EOL perspective:



- Implement **software signing and flashing** on production lines

- Secure **JTAG access** in EOL (End of Line) step

- Generate/get **keys/passwords** and perform the setup of these components in each part produced

- Perform part configuration in EOL process, activating all **security access** mechanisms according to customer requirements

2. Cyber security in automotive

- Bootloader perspective:

Secure Boot:

Secure boot is a process where your OS boot images and code are authenticated against the hardware before they are allowed to be used in the boot process.

2. Cyber security in automotive

- Bootloader perspective:

Software signing and flashing:

Bootloader will have to integrate cyber security functionalities in order to validate the software.

Bootloader will validate the authenticity of the software before validating it and starting the application software.

2. Cyber security in automotive

- Bootloader perspective:

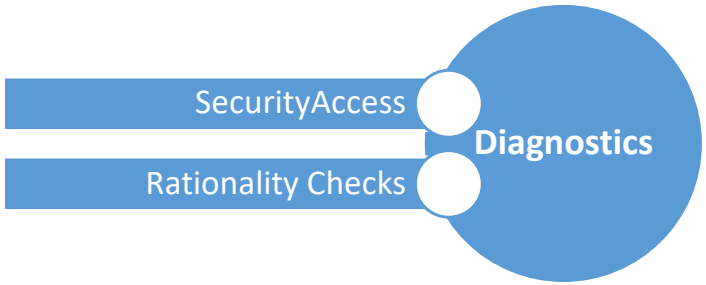
Software signing and flashing:

Bootloader specific cyber security actions:

- Hash calculations and validations
- Software signature calculation and validation
- Decrypt / decompress software containers

2. Cyber security in automotive

- Diagnostics perspective:



Security access:

- Implement cyber security related mechanisms to protect the communication

- Implement / integrate **rationality checks** (plausibility faults) – faults that are having as a fault source the component itself, or which may be caused by shunts, for example short to ground or open load connection with the component

2. Cyber security in automotive

- Developers perspective:

- Implement / integrate **JTAG Protection and Access** mechanisms in the software (for example protect JTAG with password for locking / unlocking the debug interface)

- Implement / integrate **Security Access** mechanisms

- Implement / integrate software **containers signing and flashing algorithms**. Implement binary post processing steps that will add the security mechanisms to the binary files.

Possible threats to ECU's

We need to protect the ECU's in order to prevent the following types of attacks:

Pivoting

The act of first using a compromised ECU to allow access and compromise other (otherwise inaccessible) ECU's

for example: **Jeep Cherokee (2015)**

Possible threats to ECU's

We need to protect the ECU's in order to prevent the following types of attacks:

Safety

The act of attempt to the safety of the driver:

- Direct impact, as in ASIL-related systems
- Indirect impact, for example by distracting the driver (blower, temperature, display)

Possible threats to ECU's

We need to protect the ECU's in order to prevent the following types of attacks:

Availability

Preventing Denial of Service attacks – non availability of different services offered by the system

Possible threats to ECU's

We need to protect the ECU's in order to prevent the following types of attacks:

Confidentiality

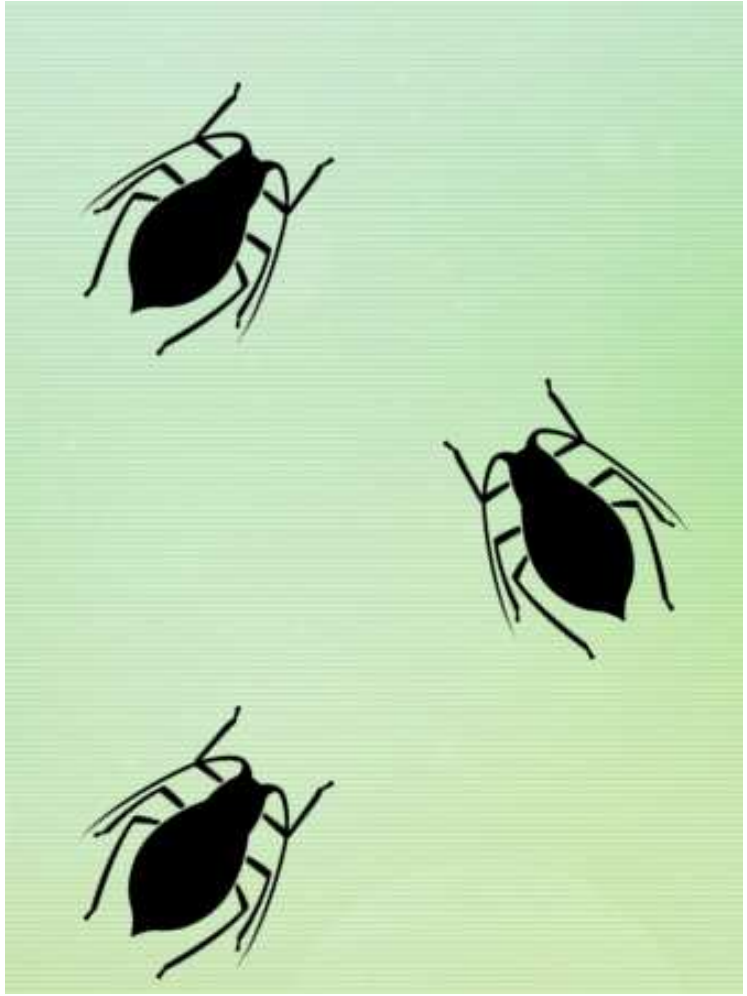
Protect PII (personally identifiable information) and IP (intellectual property) – leakage of sensitive information which the system holds about the users

2. Cyber security in automotive

Bug bounty programs

There are different programs which the car manufacturers are running in order to detect / improve the prevention mechanisms available in the ECU's that are integrated into the modern cars.

Following slides give a few examples of such programs:



2. Cyber security in automotive

- **Bug bounty programs**

Tesla:

- Launched in June 2015
- Originally only applied to bugs in web application and paid $25-$1000 per vulnerability
- Now pays anywhere from $100-$10,000 depending on the bug
- So far **over 300 vulnerabilities** have been found

2. Cyber security in automotive

- **Bug bounty programs**

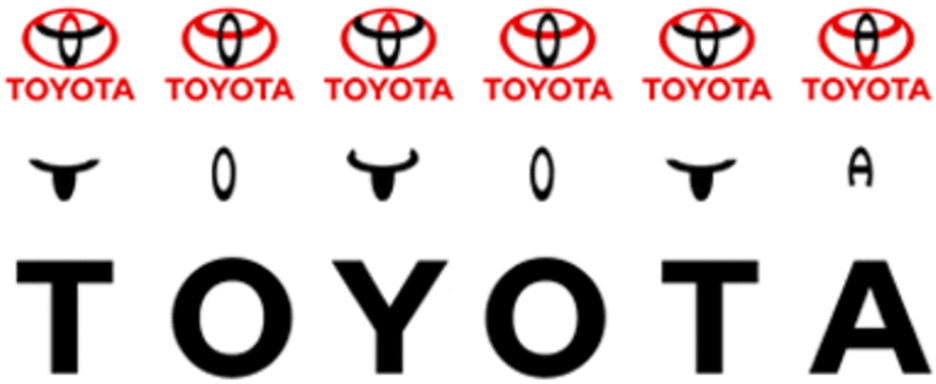
Fiat Chrysler (FSA):

- Started in July 2016
- First “major” car manufacturer to offer bounty program
- Run by Bugcrowd
- Pays between $150-$1500 depending on the severity

Bug bounty programs

Toyota:

- Opened an account with HackerOne in February 2018
- Vulnerability disclosure program, no cash bounty offered
- At least 120 vulnerabilities fixed so far



2. Cyber security in automotive

- **Bug bounty programs**

Ford:

- Has a vulnerability disclosure program through Bugcrowd
- Awards “points” to hackers but no cash rewards
- So far 1515 vulnerabilities have been rewarded

3. Exercise:

- Study the uC datasheet
- Create memory layout
- Set compiler/linker options
- Set OS and test basic functionality