

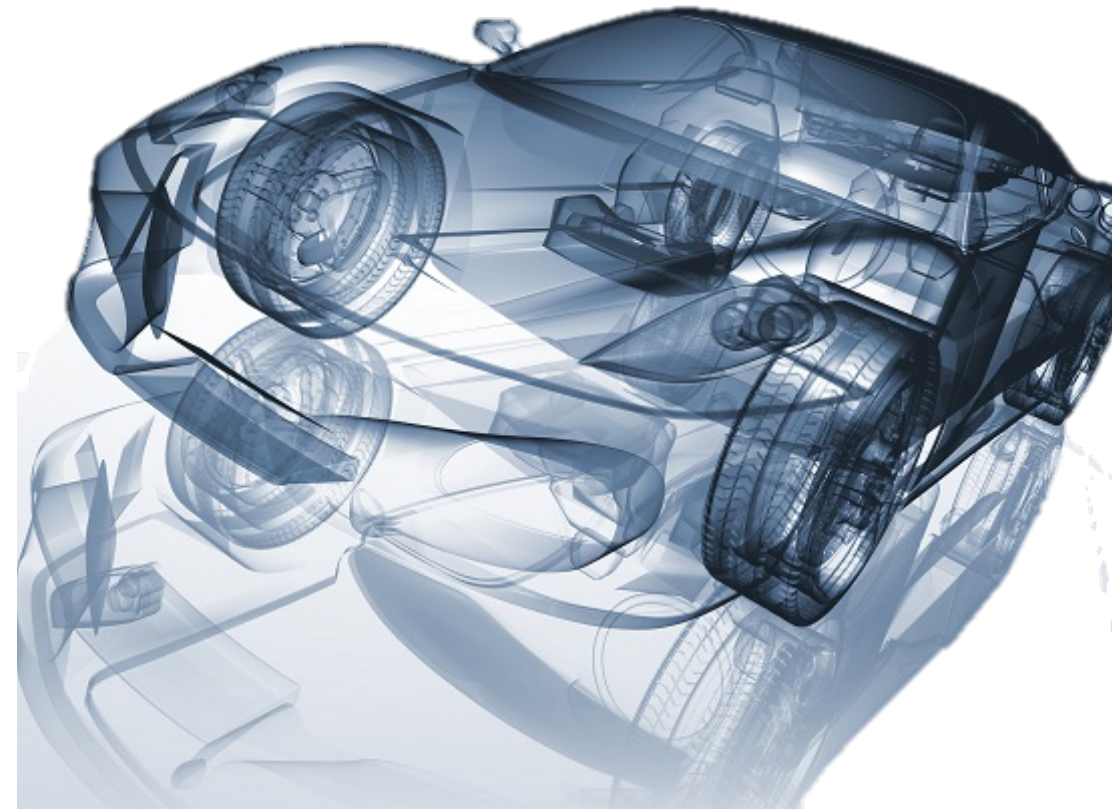


# SUR LA SÉCURITÉ DES VOITURES

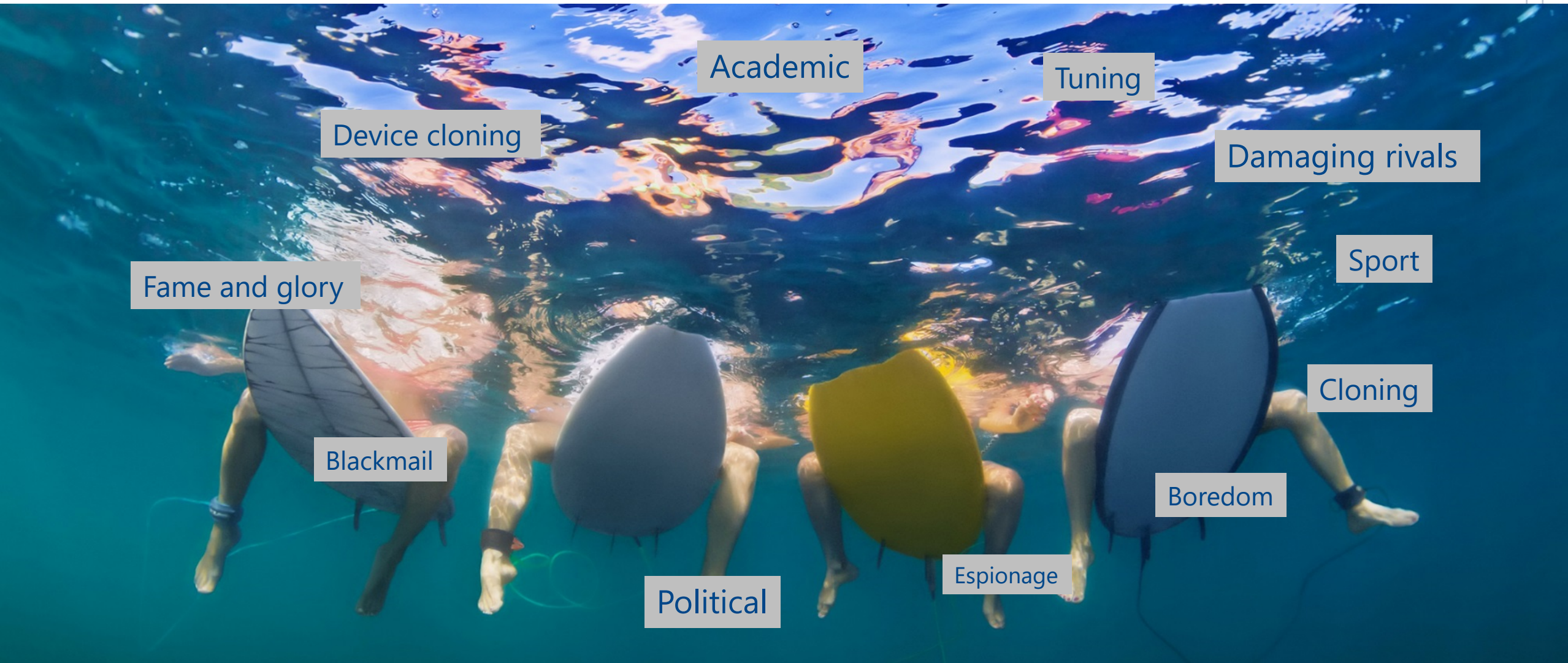
LOUBNA GHAMMAM

# AGENDA

- Motivation
- Security objectives / security goals
- Security counter-measures
- Key management



# CHANGING THE PERSPECTIVE: MOTIVATION OF THE ATTACKER



# ATTACKERS' GOALS

## EXAMPLES

- Personal damages
- Damage to the vehicles
- Privacy violation
- Disclosure of Intellectual Properties for companies
- Unlimited tuning

# RELEVANT ATTACKERS

## Global Attackers

**Attack from anywhere**  
(e.g. from the couch at home)

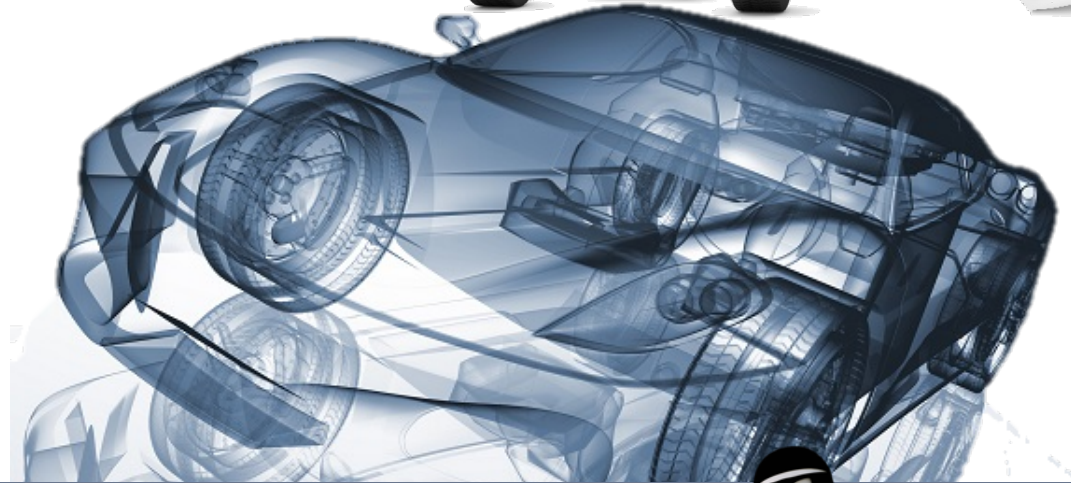
### Especially dangerous!

- Attack can be performed simultaneously on a whole fleet
- Attacker does not need access to the vehicle



## Neighborhood attackers

**Manipulation near the vehicle**  
(e.g. Bluetooth or WiFi hacks)



## Physical attackers

**Attacker gains physical access to the vehicle**  
(e.g. access to the vehicle bus, can replace ECUs)



# LATEST ATTACKS

## How Jeep Hackers Took Over Steering And Forced Emergency Stop At High Speed

 **Thomas Brewster** Forbes Staff  
Security  
I cover crime, privacy and security in digital and physical forms.



The Jeep emblem on a Grand Cherokee SUV. The 2014 Jeep has vulnerabilities that allow hackers hooked up to the system to take control of the car. (AP Photo/Gregory Bull)

## Hack the diagnostics connector, steal yourself a BMW in 3 minutes

By Bill Howard on July 10, 2012 at 8:57 am | 17 Comments

      209 SHARES

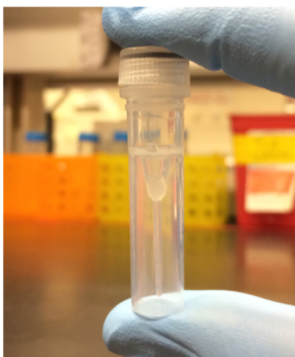


Your BMW comes with a \$160 key with a computer chip and security code inside to make the car hard to steal. The common thief can't steal your Bimmer, but in Europe, at least, hacker-thieves apparently have been

## CYBERCRIMINALS ARE FINDING NEW ATTACK METHODS FOR MEDICAL DEVICES

[nagictv](#) | October 8, 2018 | [Science](#) | 0 Comments

Cybercriminals use error messages from the connected medical devices, including radiological and x-ray machines and other imaging systems in order to obtain valuable information. The obtained data are used for attacks, increasing the likelihood of successful hacking, said the experts from the company Zingbox.

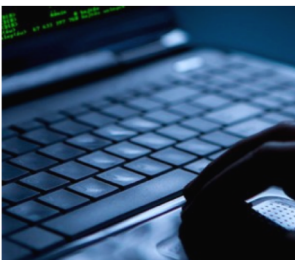


## Scientists Hack a Computer Using DNA

Malware can be encoded into a gene and used to take over a computer program.

by Antonio Regalado August 10, 2017

A researcher holds up a vial containing a malicious computer program stored as DNA.



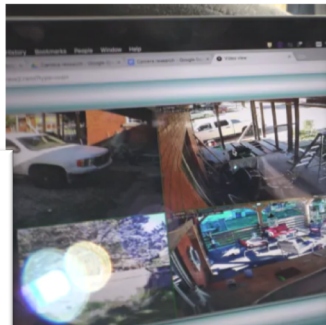
Experts are finding new attack methods to connect medical devices. We need to be one step ahead before they can cause real harm," the experts noted.

## We hired ethical hackers to hack a family's smart home – here's how it turned out

Vulnerabilities revealed in smart home devices prompt 1 manufacturer to immediately beef up protections

Luke Denne, Greg Sadler, Makda Ghebreslassie - CBC News - Posted: Sep 28, 2018 4:00 AM ET | Last Updated: September 30



Marketplace investigation found footage from hundreds of people's homes and businesses are being live streamed online. (Greg Sadler)

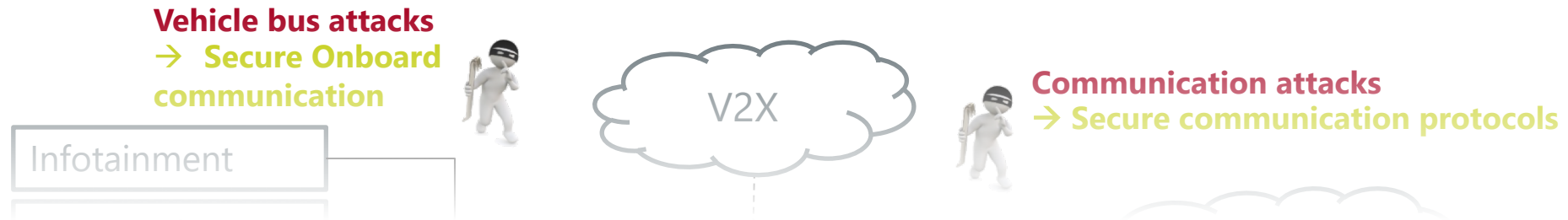
## Team of hackers take remote control of Tesla Model S from 12 miles away

Chinese researchers were able to interfere with the car's brakes, door locks and other electronic features, demonstrating an attack that could cause havoc

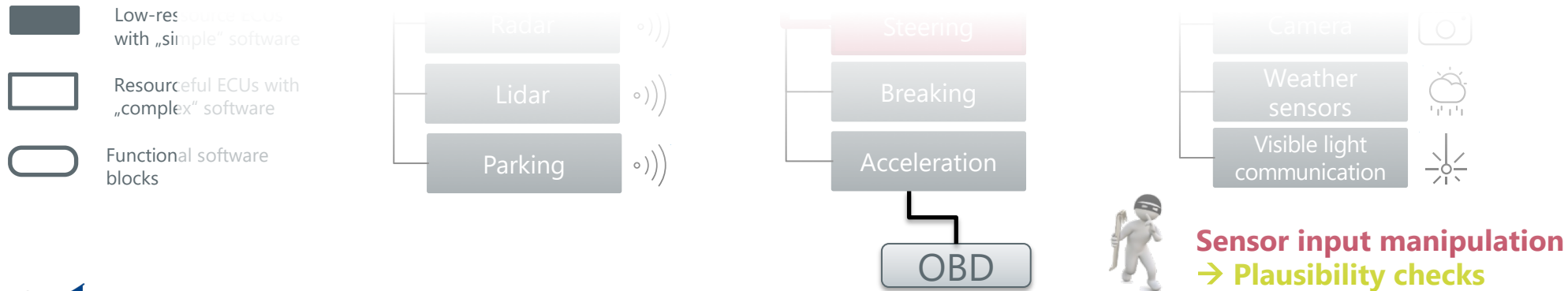


▲ Now that cars such as Tesla's are increasingly high-tech and connected to the internet, cybersecurity has become as important as traditional safety features. Photo: iStockphoto.com

# OVERVIEW: ADAS ATTACK LANDSCAPE



**„If it has software, substitute the word exposed“**  
Joshua Corman



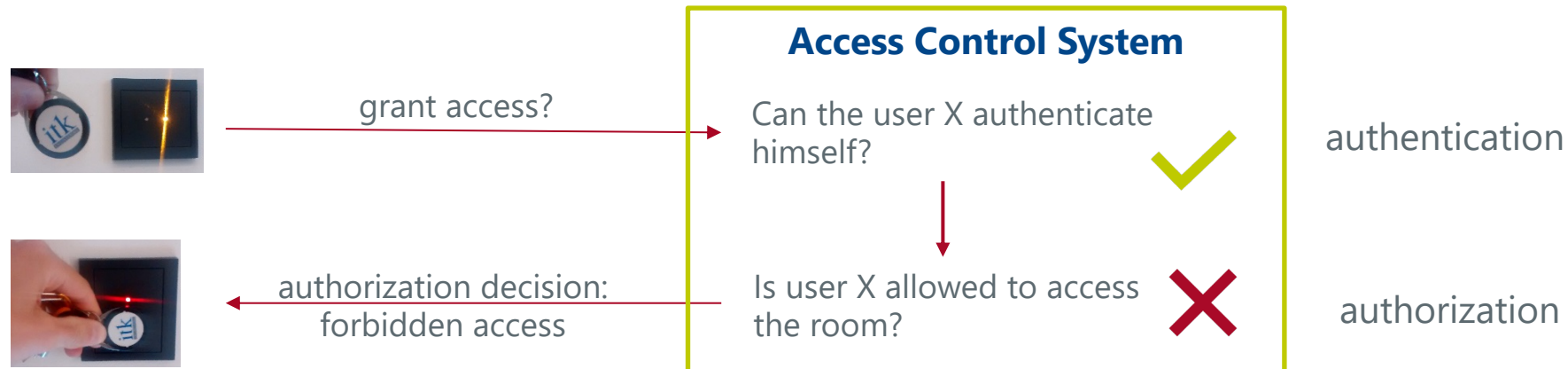


# SECURITY OBJECTIVES

# DEFINITIONS

## AUTHENTICATION VS. AUTHORIZATION

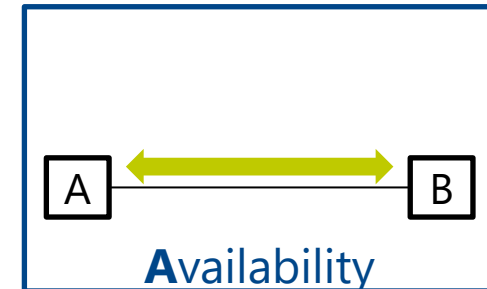
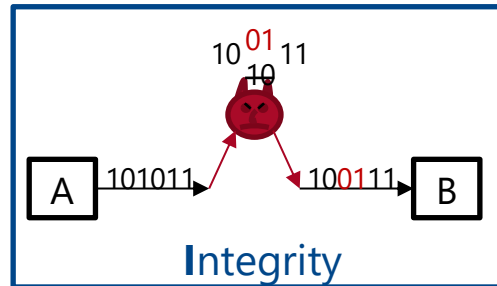
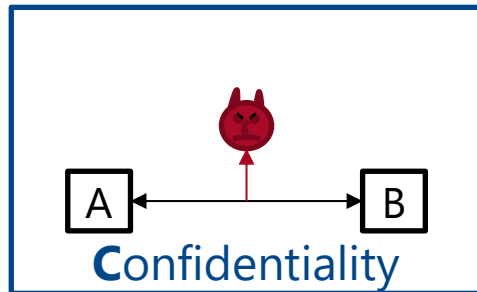
- Authentication:
  - proof that the identity has been verified
- Authorization:
  - not all authenticated users are authorized to perform specific tasks



# CIA-TRIAD

## STANDARD PROTECTION GOALS OF IT-SECURITY

- Confidentiality: data can only be read from authorized entities
- Integrity: ensures that the data has not been tampered with
- Availability: ensures that the data can be accessed at any time

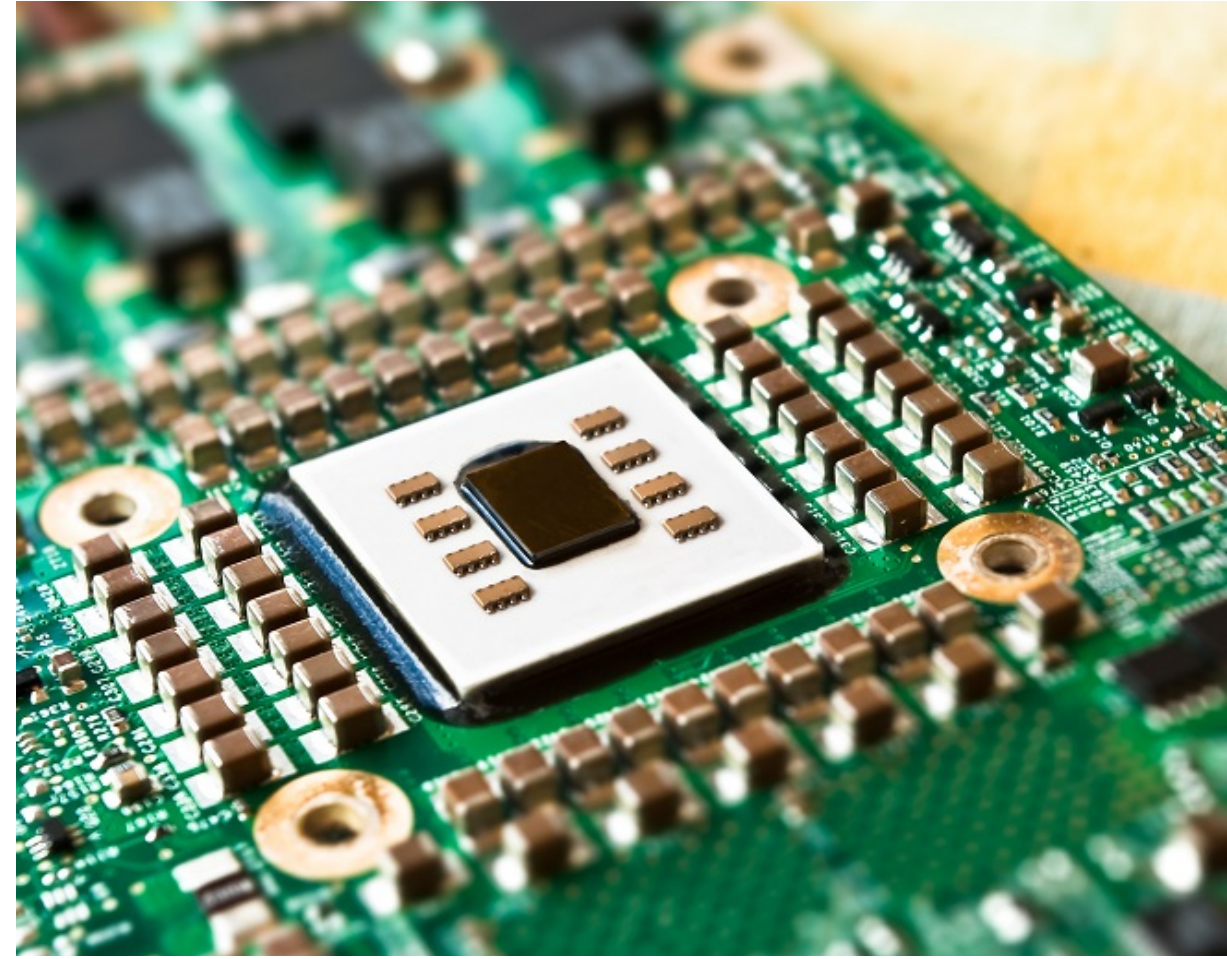




# COUNTER-MEASURES

# COUNTER-MEASURES

- Secure Diagnostics/Secure Access
- Secure Flashing
- Secure Boot
- Secure In-Vehicle Communication
- Secure Wireless Communication
- Secure Coding
- Secure Hardware Interfaces
- Secure Logging
- Secure Storage
- Secure Lifecycle
- .....





# SECURE ACCESS/ DIAGNOSTICS

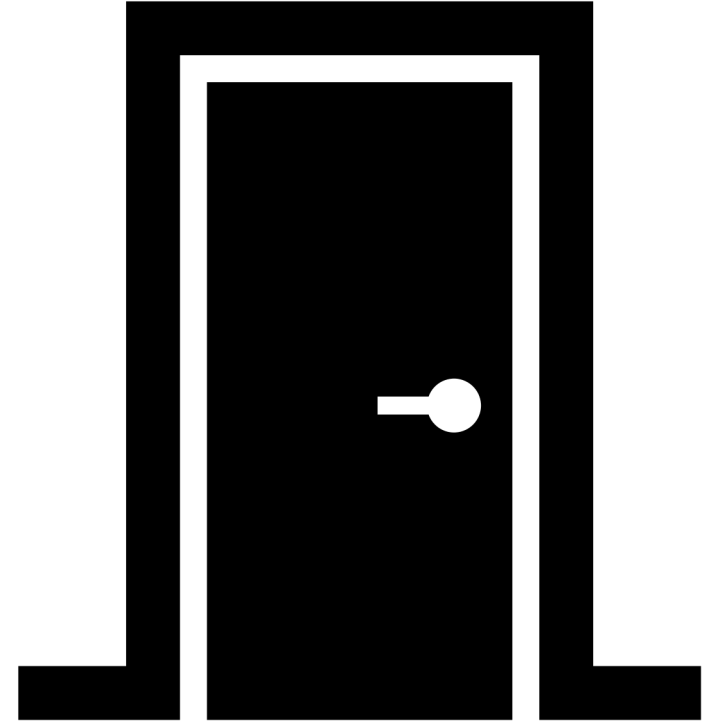
# DIAGNOSTICS

- How to open the door?
- Who is able to open it?
  - Only authorized persons with the key

Same goal for car diagnostics



Secure Diagnostics for each ECU of the car is needed



# SECURE DIAGNOSTICS

## RELEVANT ATTACKERS

### Network based attacker:

- Physical access Debug / Container Unit
- Physical access to the CAN bus
- Compromising another ECU



# SECURE DIAGNOSTICS

## GOALS



- Authentication of Diagnostic User
  - It has to be ensured that the entity sending diagnostic commands can be trusted
- Authentication of Diagnostic Session
  - Integrity and freshness of the diagnostic messages is protected
- Authorization of Diagnostic User
  - In addition, one can make sure that the authenticated user can only use certain commands
- Confidentiality of Diagnostic Session
  - Attackers cannot eavesdrop on the diagnostic session



# SECURE DIAGNOSTICS COUNTER-MEASURES

## CHALLENGE RESPONSE

- Key to open a diagnostic session is computed from a random number and a secret master key
- The cryptographic algorithm is considered to be public
- More access mechanisms are listed in ISO 14229 (UDS) (e.g., \$27 and \$29)

 <ul style="list-style-type: none"><li>▪ easy to implement</li></ul>	 <ul style="list-style-type: none"><li>▪ challenging to protect the secret key in the tester</li></ul>
---	---





# SECURE FLASHING

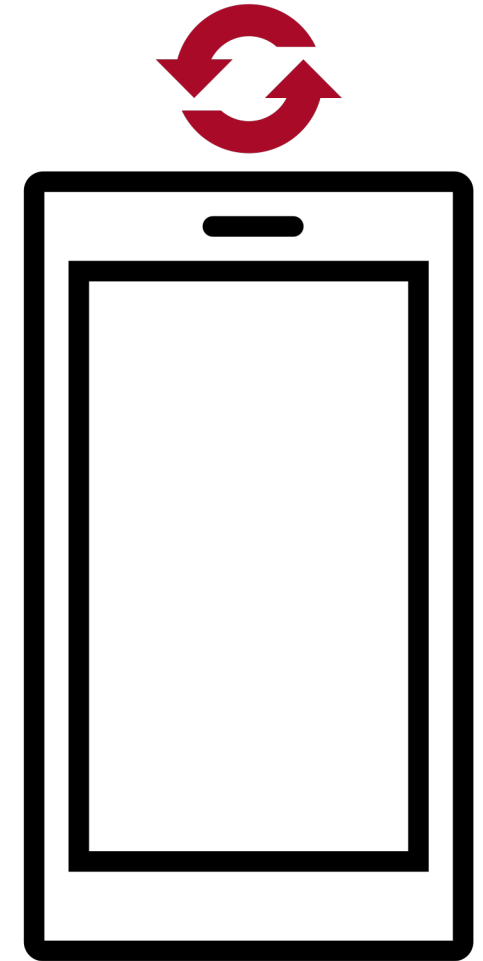
# FLASHING: NEW UPDATES

- Updates are important and are needed to:
  - Improve the performance of the smartphone
  - Add new functionalities

Same goals for car updates



Secure Flashing for each ECU of the car is needed



# SECURE FLASHING

## RELEVANT ATTACKERS

- Network based attacker:
  - Physical access Debug / Container Unit
  - Physical access to the CAN bus
  - Compromising another ECU
- Remote attackers



# SECURE FLASHING

## GOALS

- Authenticity and integrity of the update package
  - It has to be ensured that the update package has not been tampered with
- Freshness of update package
  - Downgrade attacks that would reopen patched vulnerabilities are prevented
- Confidentiality of the update package
  - By encrypting the package, the attacker does not have direct access the content by eavesdropping



# SECURE FLASHING

## COUNTER-MEASURES

### AUTHENTICITY AND INTEGRITY CHECK: NORMAL UPDATES

- Update package is digitally signed by a private key and distributed to the ECU. Bio-Hybrid validates the data with the public key
- Public key needs to be securely stored in the HSM. Otherwise, the attacker would be able to replace the key and sign malicious packages without being detected



- ensures the authenticity and integrity of the update package



- update time is increased due to the verification
- requires more RAM or storage to hold the update
- a PKI may be needed

# SECURE FLASHING COUNTER-MEASURES

## AUTHENTICITY, INTEGRITY, AND CONFIDENTIALITY: OVER THE AIR UPDATES

- Addition to the previous option: the update package is encrypted
- If the system stores the unencrypted update package before or after flashing, this option will not be sufficient to protect the confidentiality of the firmware



- Protects the authenticity, integrity and confidentiality of the update package



- Requires either distributed keys or a key negotiation
- Update time is increased due to the verification
- Requires more RAM or storage to hold the update before it is flashed. Must be secure if confidentiality is to be protected.
- Requires more secure storage to hold the key used in the encryption scheme



# CRYPTOGRAPHY

# HOW TO IMPLEMENT THESE COUNTERMEASURES? THANKS TO CRYPTOGRAPHY

- Symmetric Cryptography
- Asymmetric Cryptography
- Hash functions

"Security is based on the secrecy of the cryptographic material  
and not the cryptographic algorithm"

→ Cryptographic keys (not the algorithms) need to be protected

# KEY HANDLING WITH HSMS

## HSM: TRUST ANCHOR: CRYPTOGRAPHIC MATERIAL

- Attacker can extract / modify / delete existing keys
  - Cryptographic material shall be securely stored
- Attacker can manipulate the software that has access to the keys and cryptographic algorithms
  - Software having interfaces to the key storage or crypto-algorithms have to be separated from other components

### Solution: Use HSM ("*Hardware Secure Module*")

- Protect keys with an HSM
- crypto keys **do not leave** the HSM
- private keys are ideally generated within the HSM, or are provisioned securely during production
- cryptographic primitives are **executed solely** on the HSM



## Take Home Messages:

- Cars have many computers
- Protection of these computers is mandatory
- Cryptography is needed to achieve this protection and to ensure security in cars

**THANK YOU.**



**DR. LOUBNA GHAMMAM**

**Loubna.Ghammam@itk-engineering.de**



# SECURE DIAGNOSTICS COUNTER-MEASURES

## END-TO-END ENCRYPTION

- Diagnostic session becomes bounded to the tester / user
- Integrity and Freshness of diagnostic messages is ensured
- Confidentiality can be additionally protected



- Authenticity of diagnostic messages



- Challenging to protect the secret key in the tester
- Diagnostic messages become complex





# TRUSTED BOOT

# TRUSTED BOOT

## GOAL

- Integrity of non-volatile memory content at rest
  - In particular it prevents an attacker from tampering with the software stored on the non-volatile memory without detection

## ADDITIONAL GOAL

- Integrity of non-volatile memory during run-time
  - Experienced attackers can exploit software vulnerabilities in order to tamper or gain control of the ECU. A cyclic verification of the memory may detect such intrusions.



# TRUSTED BOOT



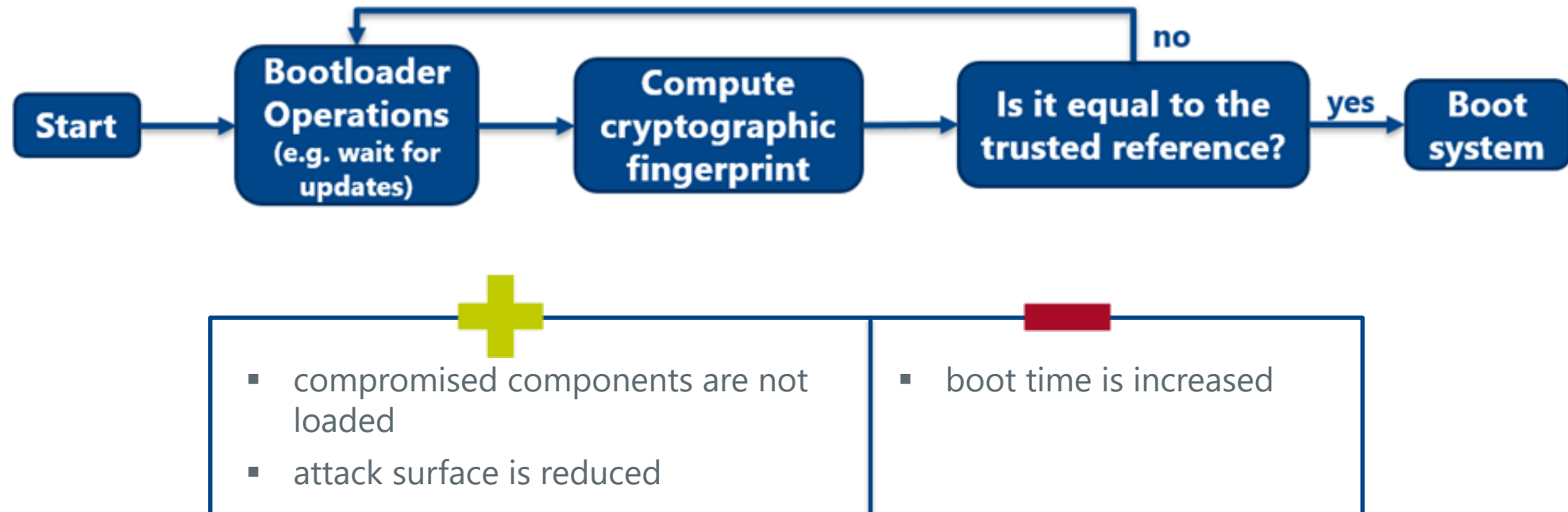
## RELEVANT ATTACKERS

- Software-based attacker
  - Malicious CAN messages can trigger certain exploits in the ECU (e.g. buffer overflow attack) and overwrite certain areas of the memory
- Diagnostic attacker
  - Maliciously using writeMemoryByAddress commands to tamper with targeted areas containing software
- Physical attacker
  - Directly connecting to the non-volatile memory pins grants full access to the memory

# TRUSTED BOOT COUNTER-MEASURES

## SECURE BOOT

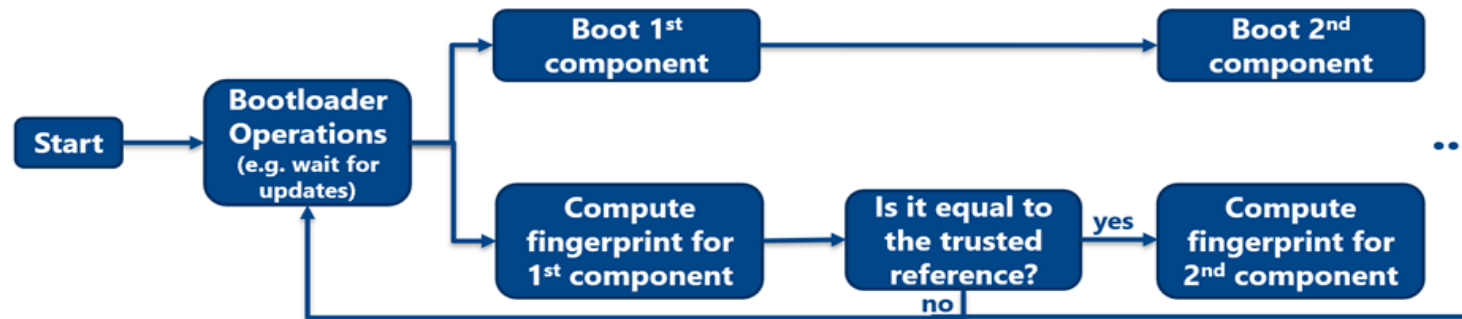
- System only boots if the integrity of the flash memory has been validated
- Validation is done by computing a cryptographic fingerprint during the flashing procedure and storing it for reference



# TRUSTED BOOT COUNTER-MEASURES

## AUTHENTICATED BOOT

- System boots and starts checking the integrity of the flash memory in parallel
- Validation is done by computing a cryptographic fingerprint during the flashing procedure and storing it for reference



+	-
<ul style="list-style-type: none"><li>▪ boot time is not significantly increased</li><li>▪ tampering can be detected</li></ul>	<ul style="list-style-type: none"><li>▪ malicious software may compromise the other components during the verification process</li></ul>