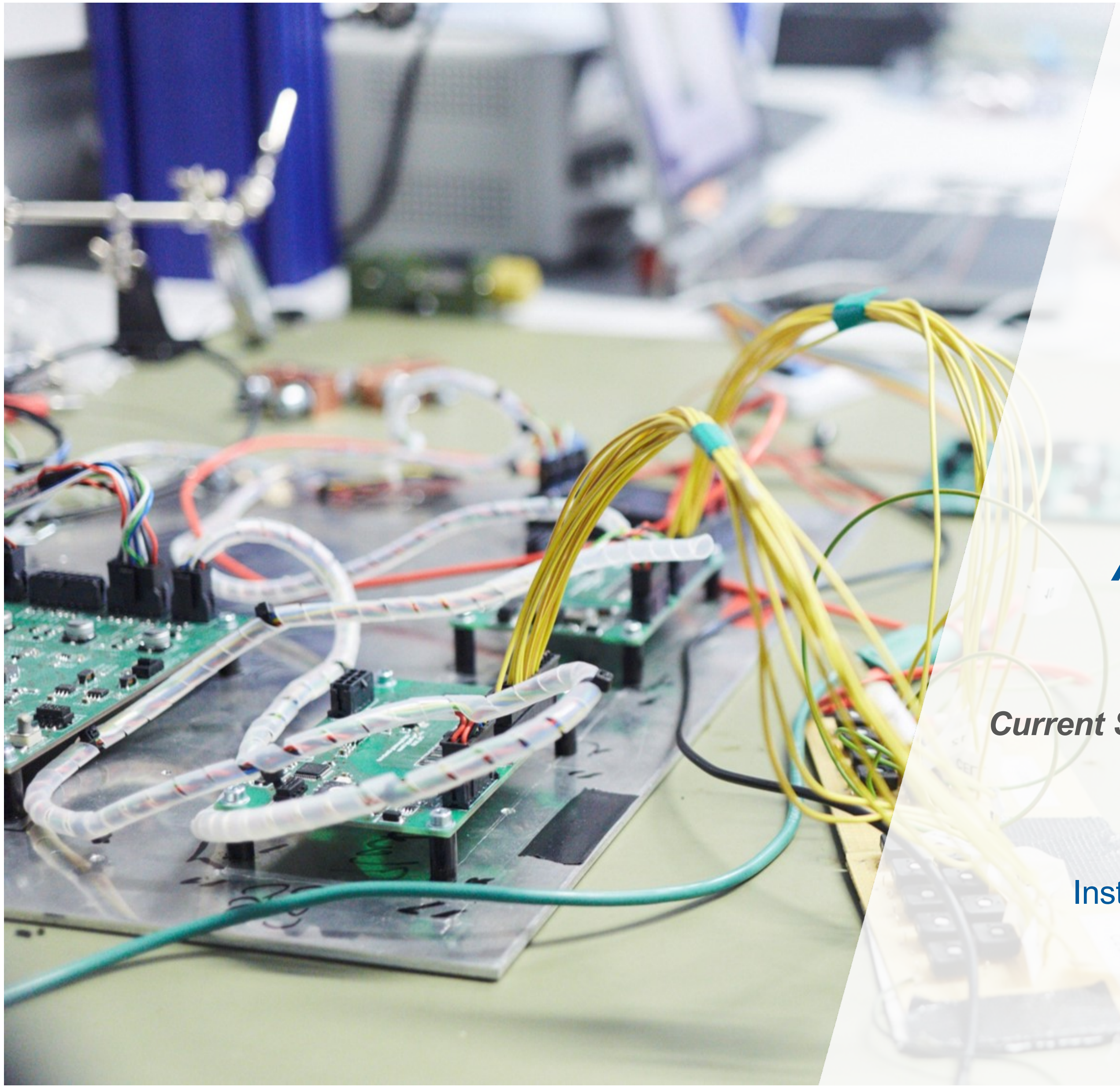


CARISSMA

Institute of Electric, Connected
and Secure Mobility

# Automotive Security – Quo Vadis?

## *Current Situation and Future Directions of Automotive Security*

Hans-Joachim Hof (hof@thi.de)

Institute of Electric, Connected, and Secure Mobility,
Technical University of Ingolstadt

Technische Hochschule Ingolstadt

IARIA

## *Prof. Dr.-Ing. Hans-Joachim Hof*

**Technical University of Ingolstadt** (current)
Vice President, Full Professor

**CARISSMA Institute of Electric, Connected, and Secure Mobility** (current)
Head of Research Group „Security in Mobility“

**Artificial Intelligence Network Ingolstadt** (current)
Member of the board

**German Chapter of the ACM and Gesellschaft für Informatik** (current)
Member of the board

**Munich University of Applied Sciences** (2011-2016)
Full Professor

**MuSe – Munich IT Security Research Group** (2011-2016)
Head

**International Academy, Research, and Industry Association** (2016)
Fellow

**Siemens AG, Corporate Technology** (2008-2011)
Research Scientist

**University of Karlsruhe now Karlsruhe Institute of Technology** (1996-2007)
Research staff, PhD student, student of Computer Science

# *Introduction*

- Quo vadis ((ˈkwəʊ ˈvɑːdɪs )
  - Latin: from the Vulgate version of John 16:5
  - Literal: „Where are you going?”
  - In a broader sense: ”what is going to happen next?”

- Outline
  - Introduction
  - Current Situation
  - Future Directions

# *Introduction*

*Comparing iPhone security and Tesla security*

**Apple iPhone 12**

Bildquelle: www.apple.de

**Tesla Model 3**

Bildquelle: www.tesla.com

# *Definition*

## *Scope of Automotive Security*

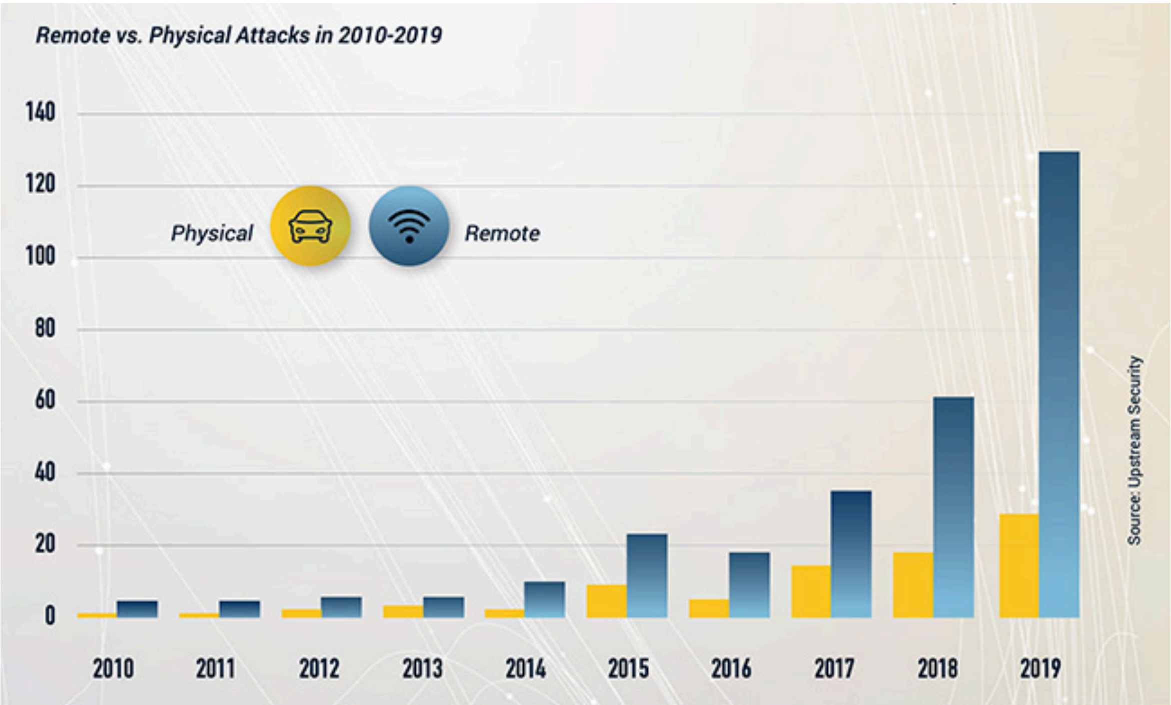
- **Automotive security refers to the security of vehicles as well as to the security of complex mobility systems that communicate with, supervise, or include vehicles.**

- **Complex mobility systems are systems of systems that facilitate the transportation of humans or goods.**

# Current Situation

## Automotive Cybersecurity Report 2020 by Upstream Security

- Number of attacks
  - 605% raise since 2016 (doubled from 2018 to 2019)
  - Numbers still very low
- Attack purpose
  - 57% of incidents in 2019 to disrupt business, steal property, or demand ransom
- Attack vectors
  - 30% keyless entry systems
  - 27% backend servers
  - 13% mobile apps
  - In 2019, 82% of attacks did not require physical access



# *Current Situation*

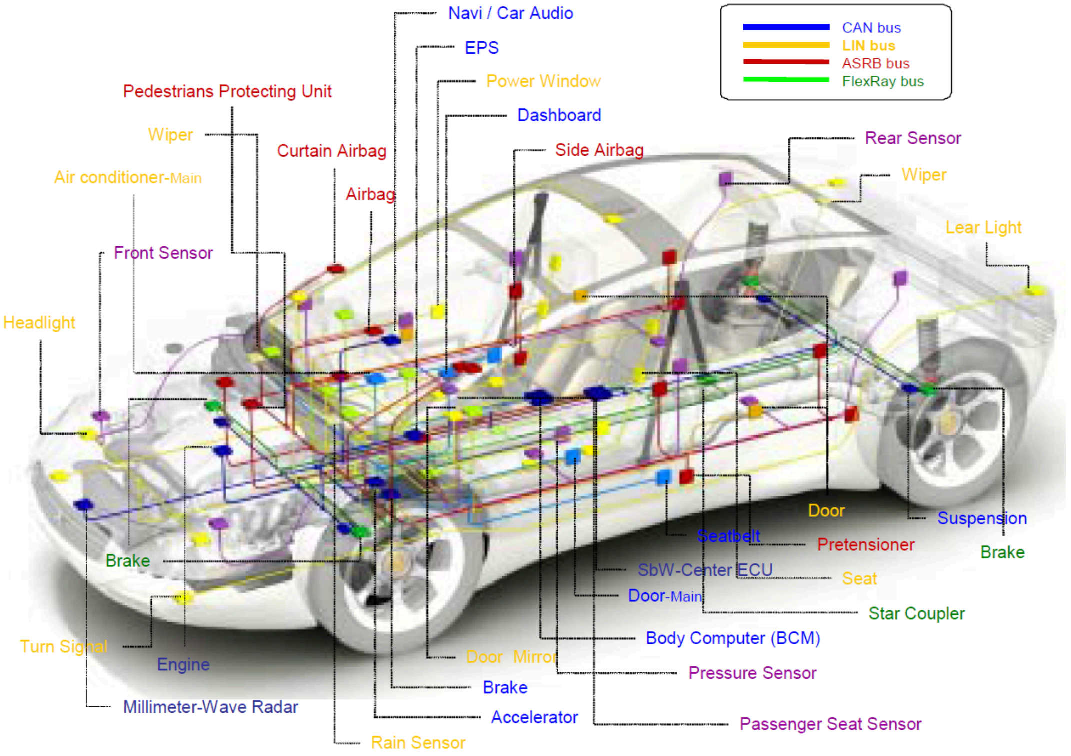
## *Cybersecurity in Automotive Report by McKinsey*

- **Report lists vulnerabilities throughout the complex mobility system**
- **In-vehicle vulnerabilities:** Demos of access to gain local and remote access to infotainment, telematics, and CAN bus (2018)
- **OEM back-end vulnerabilities:**
  - Malware infected the back end, making laptops installed in police cars unusable (2019)
  - Demo of unauthorized access to door control (2015)
- **Infrastructure**
  - EV home chargers controlled via hacked home WiFi (2018)

# *Current Situation*

## *Complexity*

- **Offence-Defence-Balance Theory: To be successful, defender needs to control all vulnerabilities, attackers need to exploit only one vulnerability**
- **Modern vehicles are complex systems:**
  - 150 ECUs
  - 100 Mio LOC, expected to be 300 Mio in 2030
  - Various interfaces
- **Low resources of many ECUs and their sheer number make key management and hardware support hard**



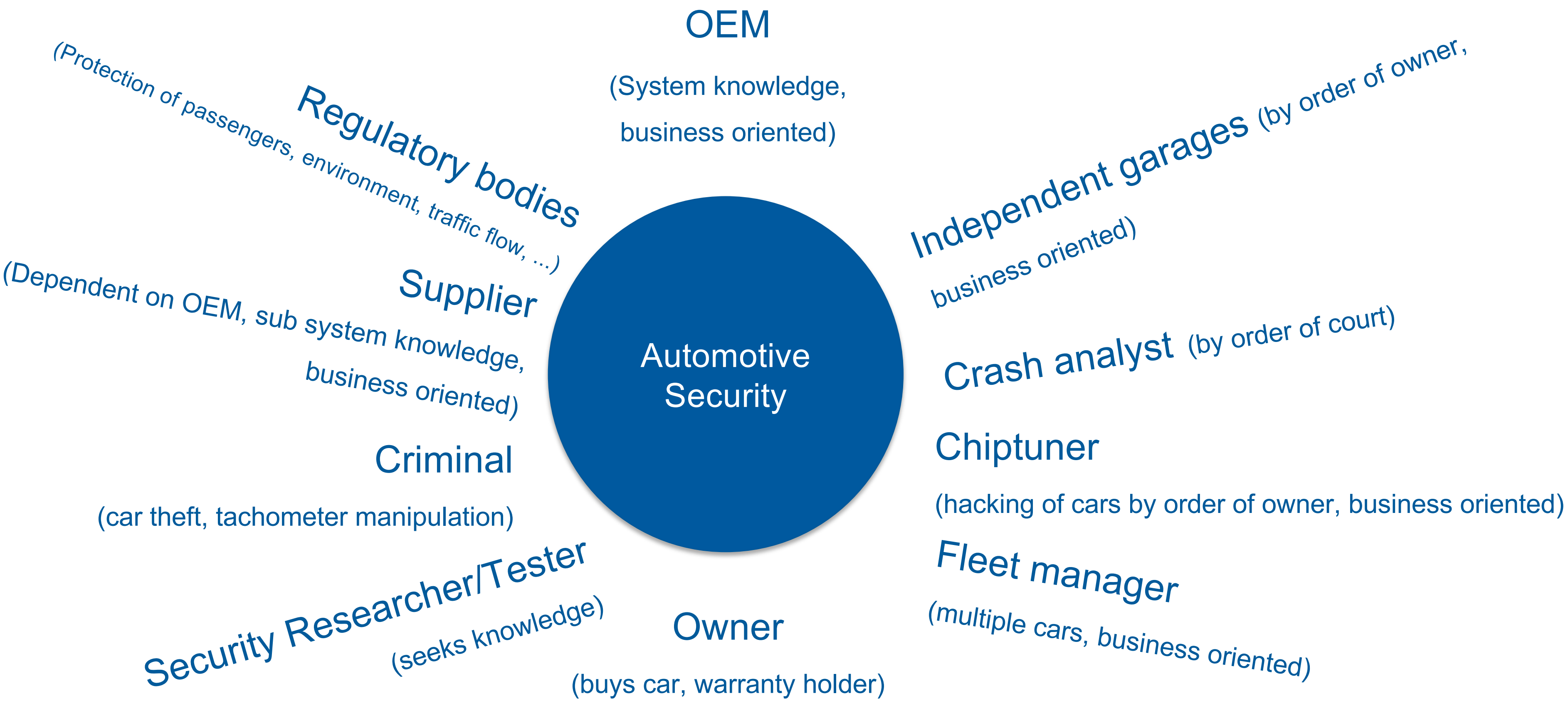
# *Current Situation*

## *Emerging Standards and Regulation*

- **Security not very well addressed by standards yet**
- **Latest standards (focus on security management)**
  - UNECE WP.29 (approved and published in June 2020)
  - ISO/SAE 21434 (to appear)
- **Gaps concerning technical standards**
- **McKinsey: „Unlike in other industries, cybersecurity has remained unregulated in the automotive industry beyond general IT regulations“**
  - Some countries/states lately addressed cybersecurity of cars (e.g., California)

# Current Situation

## Multiple Views on Automotive Security by Stakeholders



Automotive Security

OEM

(System knowledge, business oriented)

Regulatory bodies

(Protection of passengers, environment, traffic flow, ...)

Supplier

(Dependent on OEM, sub system knowledge, business oriented)

Criminal

(car theft, tachometer manipulation)

Security Researcher/Tester

(seeks knowledge)

Owner

(buys car, warranty holder)

Independent garages (by order of owner, business oriented)

Crash analyst (by order of court)

Chiptuner

(hacking of cars by order of owner, business oriented)

Fleet manager

(multiple cars, business oriented)

# *Current Situation*

## *Black Box Software and  Insufficient Security Testing*

- **Several suppliers that developed software, central security management sometimes missing**
- **Testing of software necessary, still some blackbox software**
  - In 2018, 63% of OEMs and suppliers test less than half of hardware, software, and other technologies for vulnerabilities [1]
- **Security engineering at supplier may be unclear**
  - 30% of OEMs and suppliers do not have an established product cybersecurity program or team [1]

**[1] SAE and Synopsys, „A Study of Automotive Industry Cybersecurity Practices“, 2018**

# *Current Situation*

## *Technology Shifts Affects Automotive Security*

- **Electric Cars**
  - Charging infrastructure extends complex mobility system (new attack vectors available)
  - Additional safety critical system: battery management system
- **Software systems more and more unique selling point**
  - E.g., autonomous driving, assistance systems, ...
  - Increases amout of software in vehicles
- **Connected vehicles**
  - Software systems use Internet services or communicate with other vehicles

## *Current Situation*

### *Safety and Security*

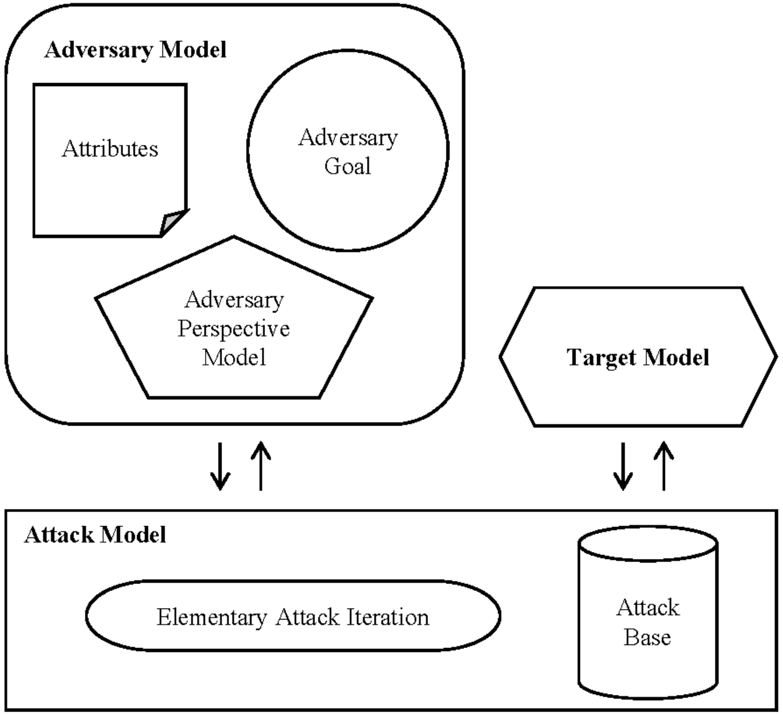
- **Safety engineering is an important aspect of modern automotive systems engineering**
  - Well-established standards and regulations

- **Security must respect safety aspects of a system**
  - Requires system-wide planning
  - Chance: design security engineering similar to safety engineering

# Examplary Project

## Using Adversary and Attack Modelling to Improve Automotive Security

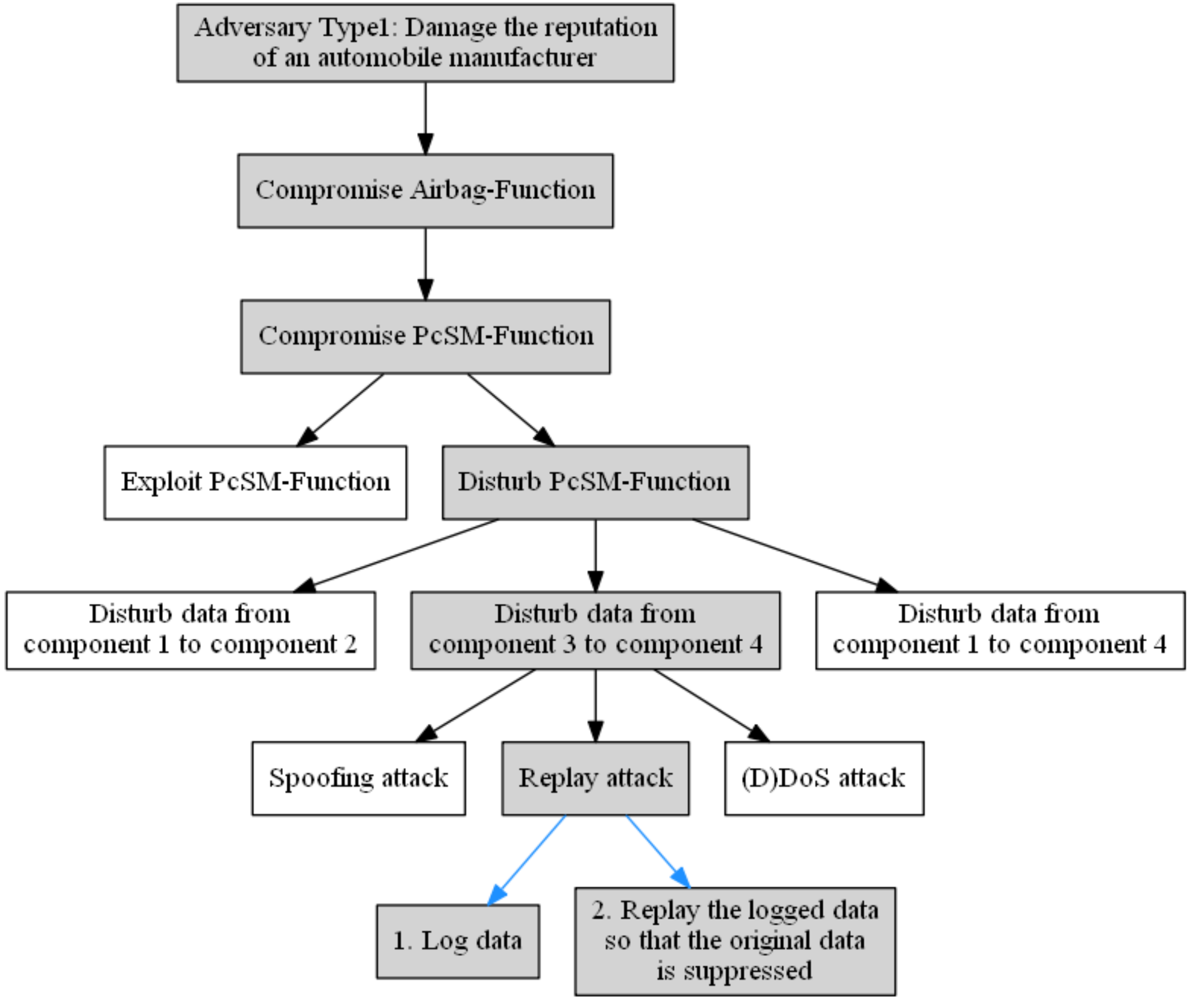
- **See talk of Tina Volkersdorfer on SECURWARE 2020**



# Example

## Model

- **Uses diagram similar to fault tree used in safety engineering**


Adversary Type1: Damage the reputation of an automobile manufacturer
Compromise Airbag-Function
Compromise PcSM-Function
Exploit PcSM-Function
Disturb PcSM-Function
Disturb data from component 1 to component 2
Disturb data from component 3 to component 4
Disturb data from component 1 to component 4
Spoofing attack
Replay attack
(D)DoS attack
1. Log data
2. Replay the logged data so that the original data is suppressed

# *Current Situation*

## *Long Product Life*

- **Vehicles tend to be long-living (>20 years) => Necessary to manage software for 20+ years**
- **Software update over the air still no default,**
- **Legacy system architecture does not support easy software updates**

# *Future Trends*

## *Large Scale Attacks*

- **Heavy reuse of software in automotive domain, sometimes low security level**
- **Fleets often include only a limited number of vehicle types => one vulnerability affects many vehicles**
- **Highly-connected fleets could be subject to attacks (see [1])**
- **Vehicle Security Operation Centers will be necessary for early detection and mitigation of attacks**

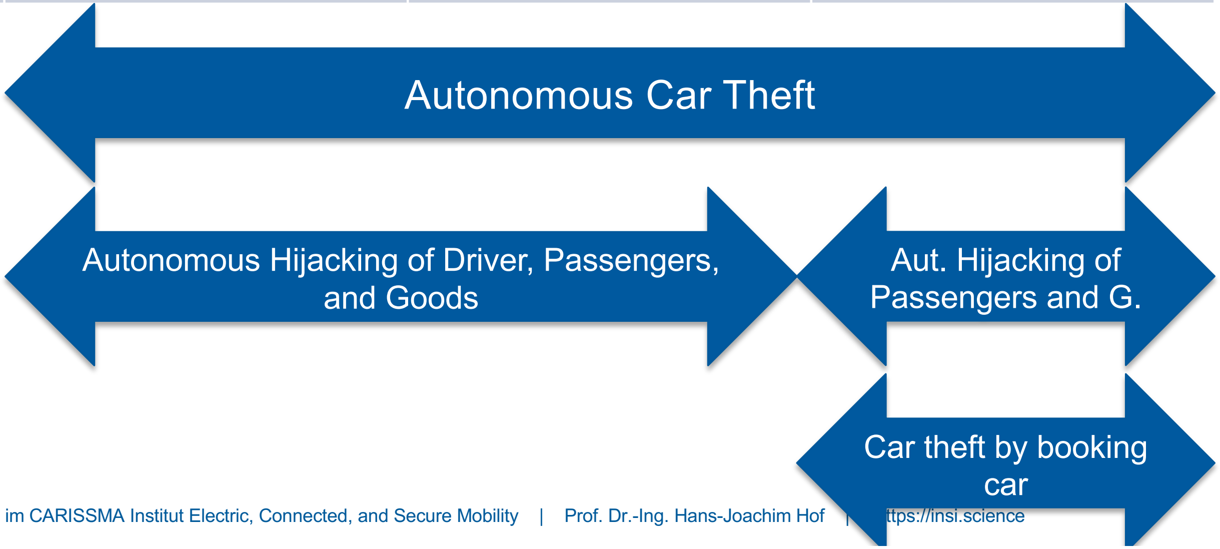
[1] Tobias Madl, Jasmin Brückmann, Hans-Joachim Hof: „CAN Obfuscation by Randomization (CANORa)“, 2nd ACM Computer Science in Cars Symposium (CSCS 2018) – Future Challenges in Artificial Intelligence & Security for Autonomous Vehicles, Munich, Germany, September 2018

# *Future Trends*

## *News Business Cases for Hackers*

- **Levels of Vehicle Automation based on SAE J3016:**

| Level 1 | Level 2 | Level 3 | Level 4 | Level 5 |
|---|---|---|---|---|
| Drive-Assistance | Partial Automated | Conditional Automation | High Automation | Full Automation |
| „Feet-off“ | „Hands-off“ | „Eyes-off“ | „Attention-off“ | „Driverless“ |
| Driver drives | Driver drives | Vehicle drives, human as backup | Vehicle drives | Vehicle drives |


Autonomous Car Theft

Autonomous Hijacking of Driver, Passengers, and Goods

Aut. Hijacking of Passengers and G.

Car theft by booking car

# Future Trends

## New System Architecture for Vehicles

- **Number of ECUs will be reduced, architecture will be less distributed and more centralized**
  - More complexity in software, less in hardware
  - Software security will become even more important (but security needs to be implementet on less devices)

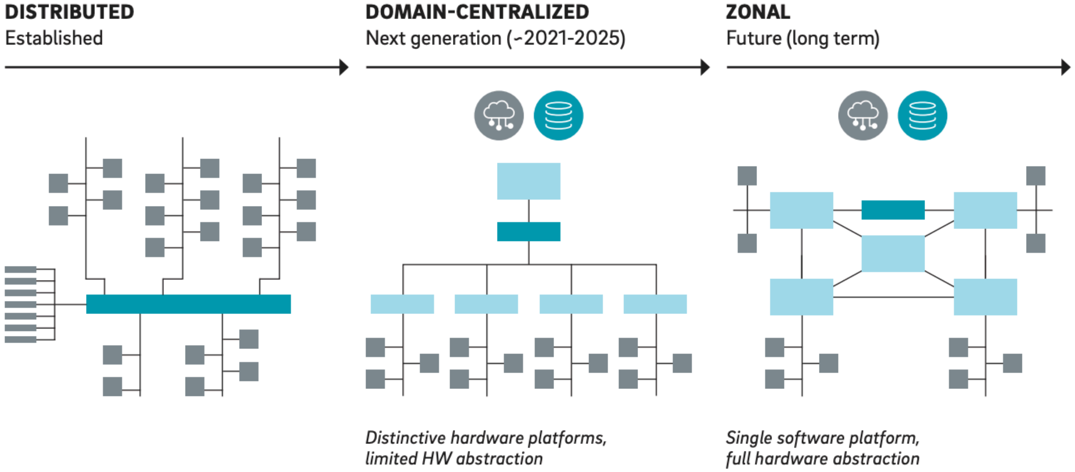

DISTRIBUTED
Established
DOMAIN-CENTRALIZED
Next generation (~2021-2025)
ZONAL
Future (long term)
Distinctive hardware platforms, limited HW abstraction
Single software platform, full hardware abstraction

Image source: Roland Berger, „Computer on wheels / Disruption in automotive electronics and semiconductors“, 2020

# Future Trends

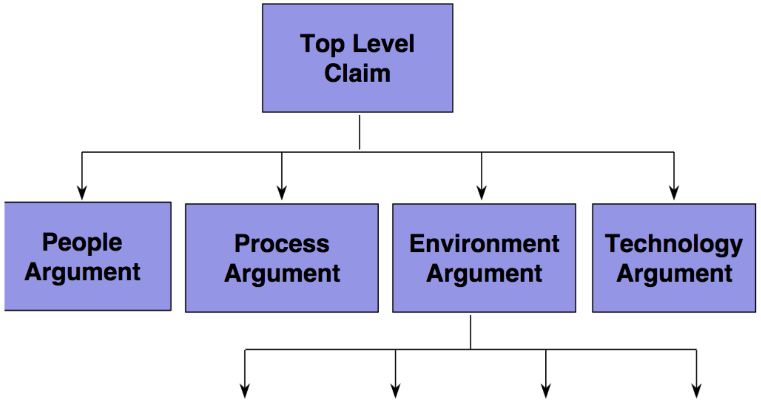
## New System Architecture for Vehicles

- **OEM will need to supply security platform**
  - Including identity management, authentication, key management, encryption, …
  - Hardware support for security
- **Software updates will be possible for most systems (finally)**

# *Future Trends*

## *Regulation and Laws*

- **Automotive security will likely be addressed by regulation in the near future**
- **In Europe, it is very likely that this will be driven by the EU**
- **Cybersecurity certification will be necessary for suppliers**



# *Future Trends*

## *Holistic Approach to Automotive Security Engineering*

- **Upcoming standards and regulations will require a holistic approach to automotive security**
- **There will be a security platform by the OEM that need to be used by suppliers**
- **As in IT, many security servies will be centralized**
  - Identity management
  - Single access point
  - ...
- **100% of software must be tested for vulnerabilities**

# *Future Trends*

## *Software Testing*

- **100% of automotive software must be tested for vulnerabilities**
- **More automation of testing is necessary – artificial intelligence may be of help**

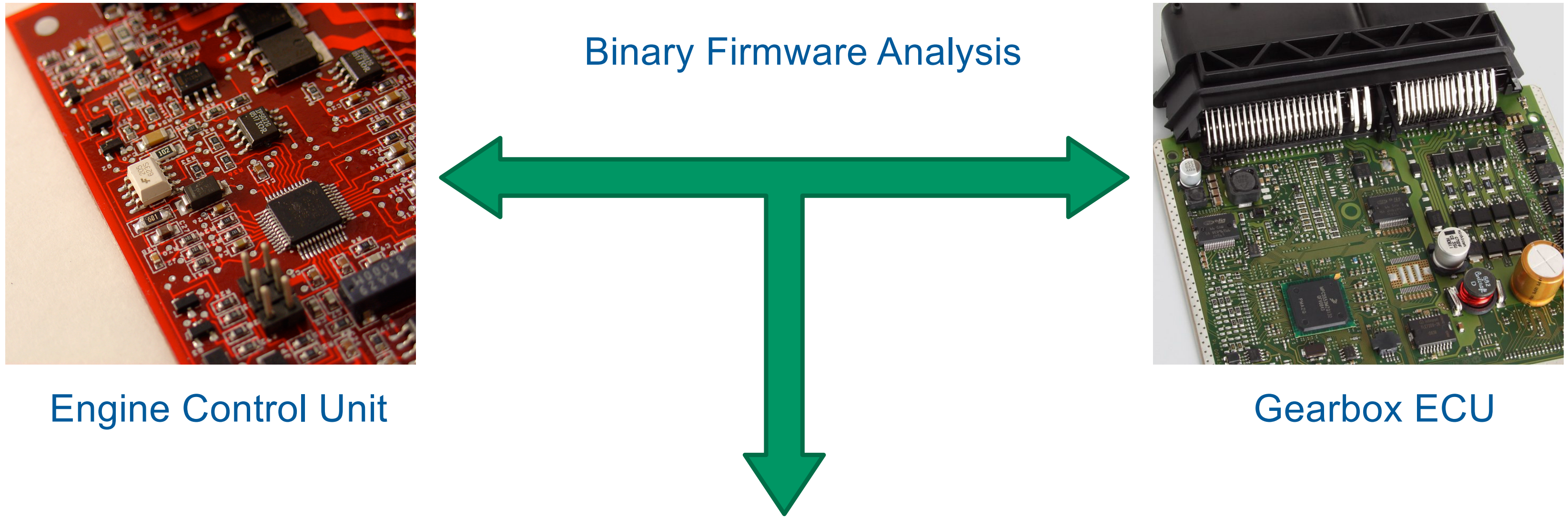
# *Future Trends*

## *Artificial Intelligence for Hacking and Testing Automotive Systems*

- **Not specific for automotive security**
- **However, tailored and planned systems may be more susceptible for this attack**
- **Research vision of my research group: Hackvisor = HACKbot + Security AdVISOR**
- **Hackbot: Autonomous detection of security vulnerablities**
  - Autonomous creation of security tests using attacker modelling and attack modelling
  - Autonomous creation of security tests by NLP analysis of ECU specifications
  - Autonomous penetration testing
  - Autonomous manual review

# *Autonomous Penetration Testing*

*Example*



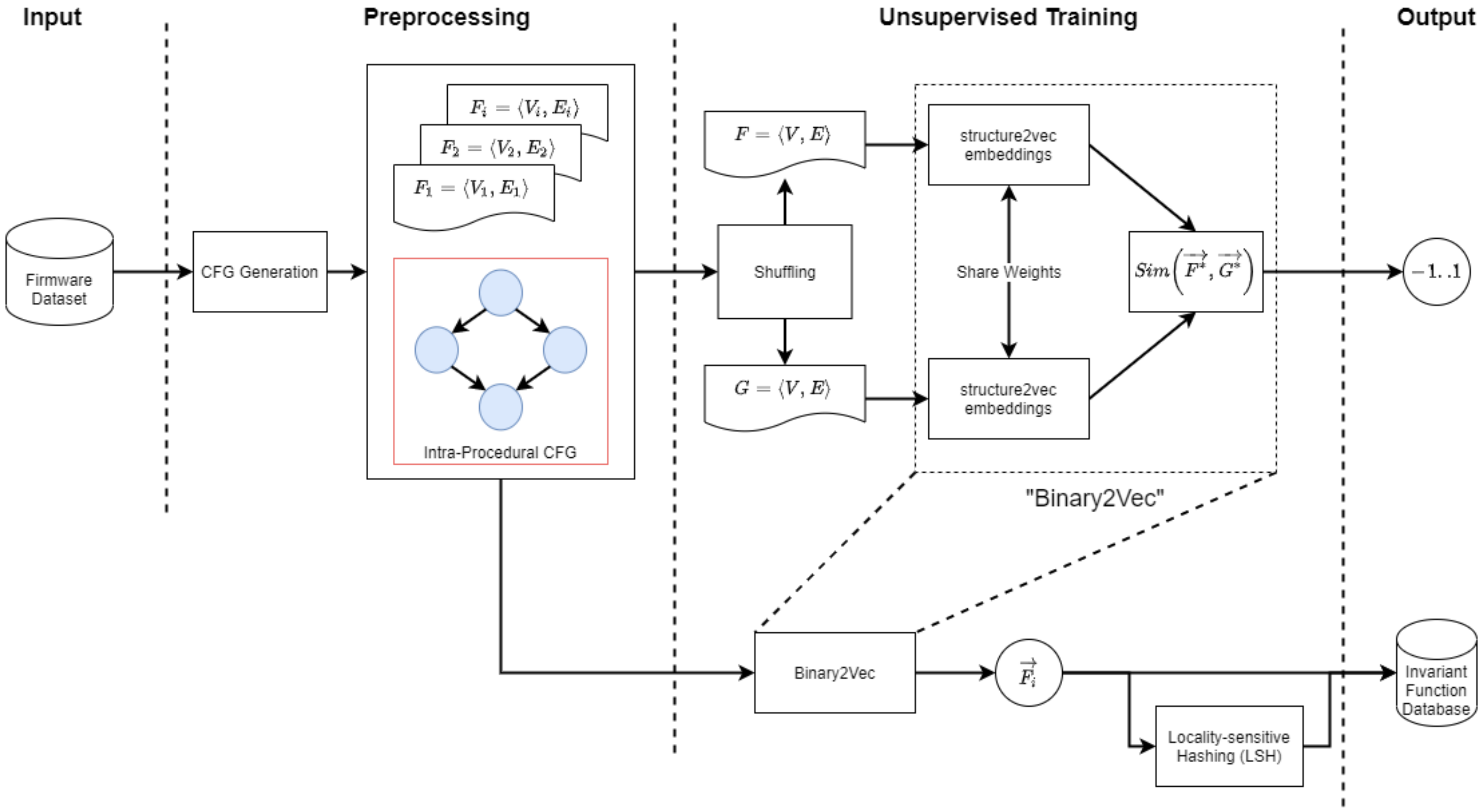
Binary Firmware Analysis

Engine Control Unit

Gearbox ECU

- **Detection of reused software blocks in automotive firmware**
- **Many be used to identify off-the-shelf software libraries (e.g., OSEK RTOS/AUTOSAR) to find known vulnerabilities**

# Preliminary Design


Input
Preprocessing
Unsupervised Training
Output
Firmware Dataset
CFG Generation
$F_i = \langle V_i, E_i \rangle$
$F_2 = \langle V_2, E_2 \rangle$
$F_1 = \langle V_1, E_1 \rangle$
Intra-Procedural CFG
Shuffling
$F = \langle V, E \rangle$
$G = \langle V, E \rangle$
structure2vec embeddings
Share Weights
structure2vec embeddings
$Sim\left(\overrightarrow{F^*}, \overrightarrow{G^*}\right)$
$-1..1$
"Binary2Vec"
Binary2Vec
$\overrightarrow{F_i}$
Locality-sensitive Hashing (LSH)
Invariant Function Database

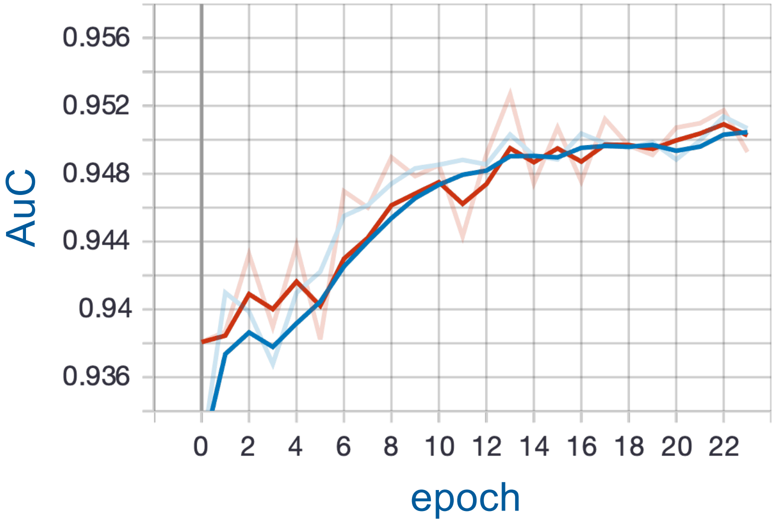
# *Preliminary results*

- **Trained on OpenSSL Cryptography Library with different configurations**
  - ARM, MIPS, x86
  - gcc 4.9, gcc 5.4, gcc 7.0
  - -O0, -O1, -O2, -O3

- **0.95 AUC classification performance**

- **Control-Flow-Graph Embeddings preserve algorithm identity over different architectures**

- **Next steps:**
  - Run trained network on Automotive Firmware Dataset
  - Generate Embeddings Dataset for commonly used software components



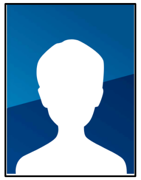
## *Summary and Outlook*

- **Automotive security not yet fully addressed in modern vehicles, attacks on all parts of complex mobility systems exist**
- **Missing legislation and (technical) standards for security in automotive domain**
- **Importance of automotive security will rise in the next years**
  - New business models for attackers
  - Regulation will demand automotive security
  - New system architectures will shift complexity from hardware to software
- **Security testing will be crucial for success, especially testing software of 3rd parties**
- **Automotive security will adapt many standard approaches from IT in the future**

# *Thank you – get in contact with us*

## *Research Group „Security in Mobility“*

**Prof. Dr. Hans-Joachim Hof**
Full Professor, head of research group
Vice President of Technical University of Ingolstadt
✉ hof@thi.de

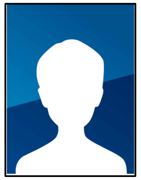


**Dominik Bayerl**
Research Staff
Automotive penetration testing, hacking,
Automotive software security
✉ dominik.bayerl@carissma.eu

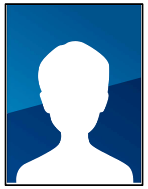
**Tina Volkersdorfer**
Research Staff
Security modelling, Security test generation
✉ tina.volkersdorfer@carissma.eu

**Marco Michl**
Research Staff
Security testing, penetration testing
✉ marco.michl@carissma.eu

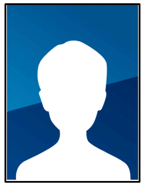
**Kevin Gomez Buquerin**
External PhD student
Automotive forensics
✉ extern.kevinklaus.gomezbuquerin@thi.de



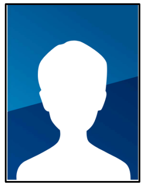
**Ludwig Sabitsch**
External PhD student
Autonomous security anti pattern detection in software



**Ricardo de Andrade**
Visiting researcher from Universidade de São Paulo
(virtuell)
CAN security



**Maximilian Gronau**
Student researcher
Automotive Software Testing



**Jakob Löw**
Student researcher
Automotive software testing