Hochschule Karlsruhe
University of
Applied Sciences

Institut für
Energieeffiziente Mobilität

Honeypots, Platform Security and about Trustworthiness of Cars –

Highlights for German-Japanese Cooperation Securing Automated Vehicles

Prof. Dr.-Ing. Reiner Kriesten, University of Applied Sciences, Karlsruhe, Germany - reiner.kriesten@h-ka.de

Short Biography

Full Professor, University of Applied Sciences Karlsruhe, Germany (since 2009)

- Member of Baden-Württemberg Center of Applied Research (BW-CAR)
- Foundation and speaker of the Institute of Energy Efficient Mobility (IEEM), currently around 20 employees
- Dean of the Master's degree program "Automotive Systems Engineering"
- Research Semester at the Royal Melbourne Institute of Technology (RMIT), Australia, research field Automotive Security (2016/2017)
- Around 40 publications within the last 5 years

SW, System and Embedded development in the automotive domain (since 2004)

- Automotive Gateway development, series projects
- Represenatitive AUTOSAR consortium WP10.1 for Robert Bosch GmbH
- Introduction of model-based development in series development

Academic staff at Karlsruhe Institute of Technology (KIT), PhD (2000-2003)

Studies of Industrial Mathematics at the KIT and Université Joseph Fourier de Grenoble

Sicherheit für vernetzte, autonome Fahrzeuge - Projekt SecForCARs

Project SecForCARs

- SecForCARs – **Sec**urity **For** **C**onnected **A**utonomous ca**R**s
- 13 Partner aus Akademia und Industrie, Projektvolumen ca. 11 Millionen Euro (2018-2021)
- Anschlussprojekt mit japanischer Seite (SIP-ADUS) zur automotiven gemeinschaftlichen Sicherheitsforschung (2022-2024)

SIP ADUS – Strategic Innovation Program
Automated Driving for Universal Services

funding by: Bundesministerium für Bildung und Forschung

funding by: Bundesministerium für Bildung und Forschung

Honeypots, Platform Security and about Trustworthiness of Cars

Motivation

CASE, EASCY…

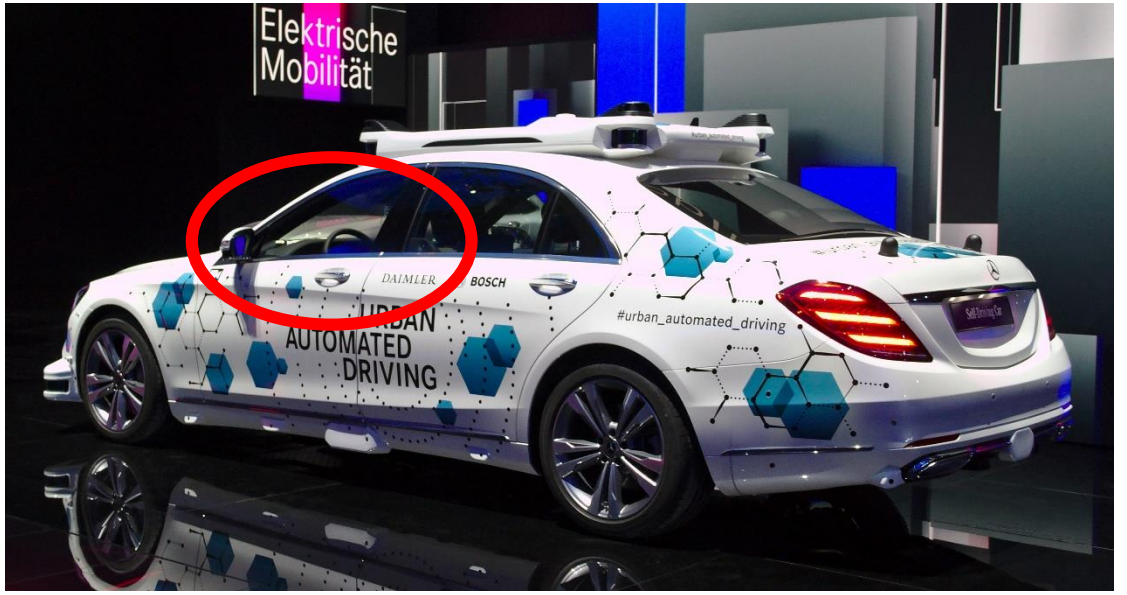
„Connected, Autonomous, Shared, Electric: Each of these points has the potential to disrupt our industry. The true revolution is indeed the composition of all these points.“

-translated from [1]

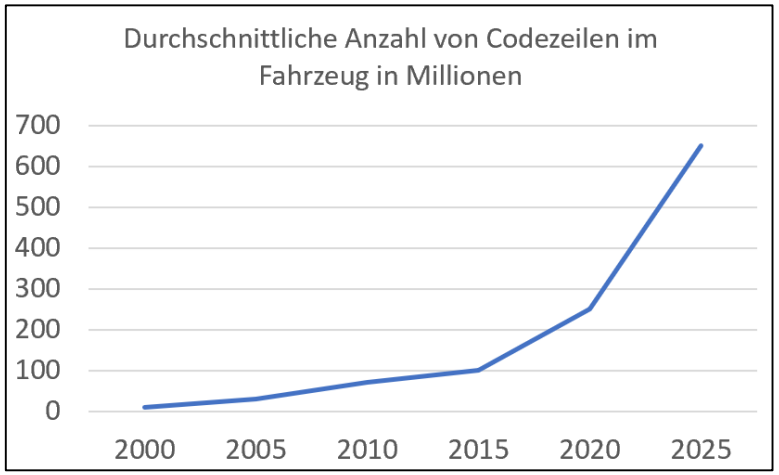
„The future car is electrified, autonomous, shard, connected and yearly updated – simple “eascy““

- translated from [2]

„A continuous trend in the automotive industry is – driven by the megatrends – is the rising significance from Software and their effects in vehicles. - translated from [3]



Source Fahrzeug: [4], Lines of Code: according to [3]



[1] Daimler. 2019. CASE-Intuitive Mobilität. https://www.daimler.com/case/. visited: 27. Mai 2019

[2]PWC: Die fünf Dimensionen der Transformation der Automobilindustrie, https://www.pwc.de/de/automobilindustrie/pwc_automotive_eascy-studie.pdf, visited 23.02.2023

[3] Themenpapier Cluster Elektromobilität Süd-West : Analyse der Aktivitäten und Entwicklungsfortschritte im Bereich der Fahrzeugelektronik mit Fokus auf fahrzeugeigene Betriebssysteme: https://www.e-mobilbw.de/fileadmin/media/e-mobilbw/Publikationen/Studien/ClusterElektromobilitaetSued-West-Themenpapier-Fahrzeugelektronik.pdf, visited 23.02.2023

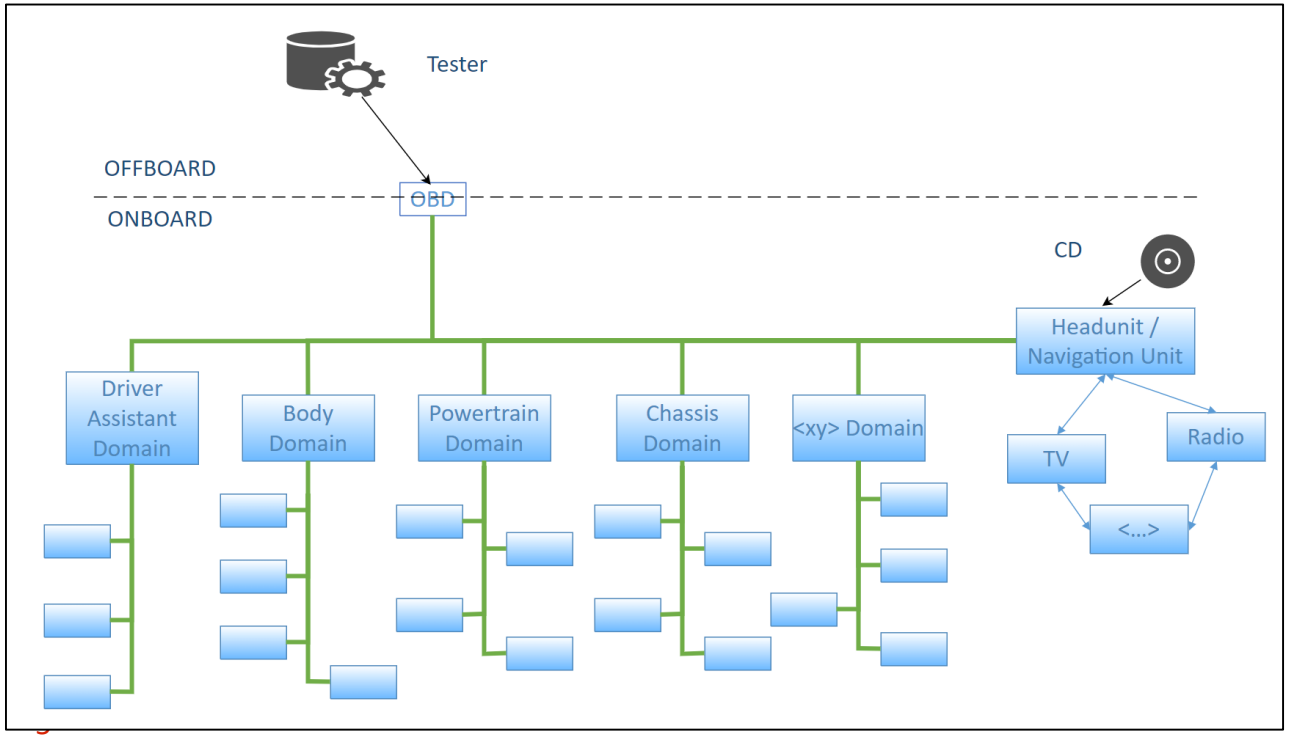
[4] Alex Migl, Mercedes-Benz W222 Urban Automated Driving at IAA 2019: https://de.wikipedia.org/wiki/Selbstfahrendes_Kraftfahrzeug#/media/Datei:Mercedes-Benz_W222_Urban_Automated_Driving_at_IAA_2019_IMG_0407.jpg, CC BY-SA 4.0, visited 23.02.2023

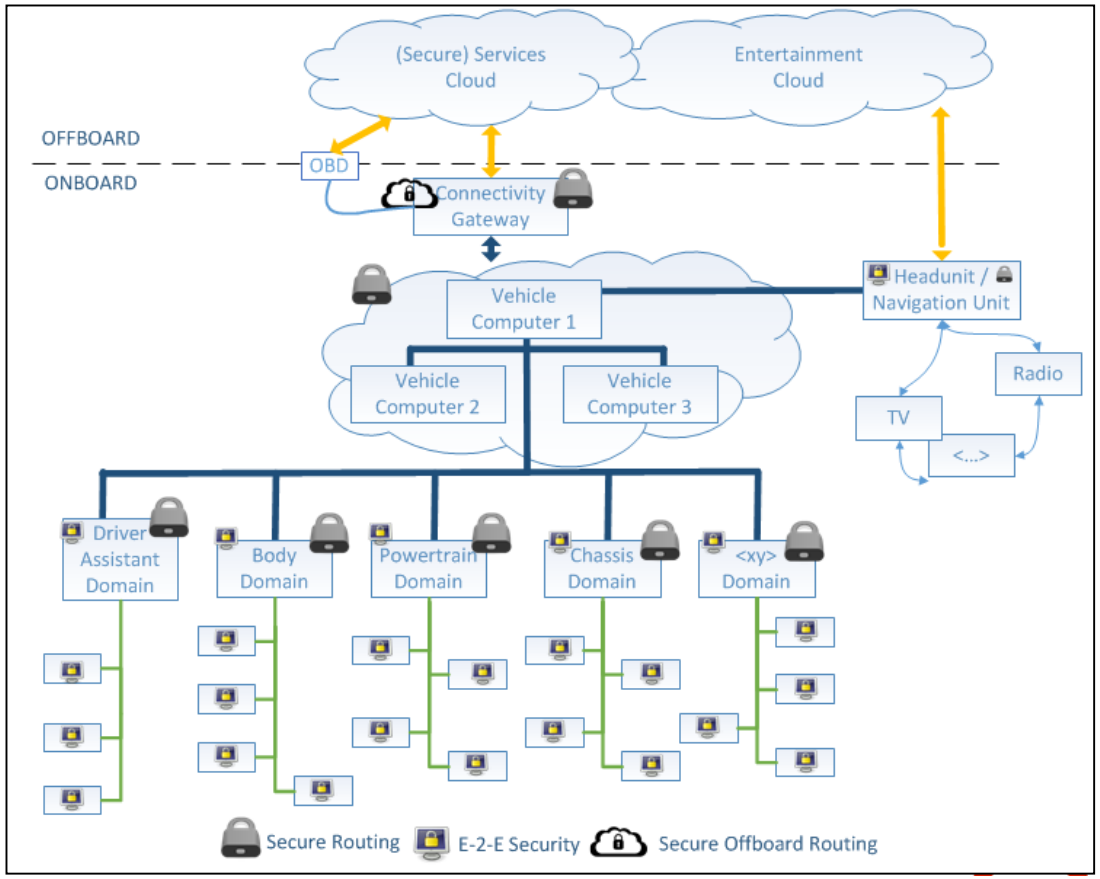
Honeypots, Platform Security and about Trustworthiness of Cars

Motivation

Automotive networks – Changes due to the megatrends

+ High-performance computer due to automated driving functions
+ Ethernet-Communication instead of „Plug & Play busses“ (CAN) and Embedded Switches
+ Separation offboard/Onboard/Infotainment due to security
+ …

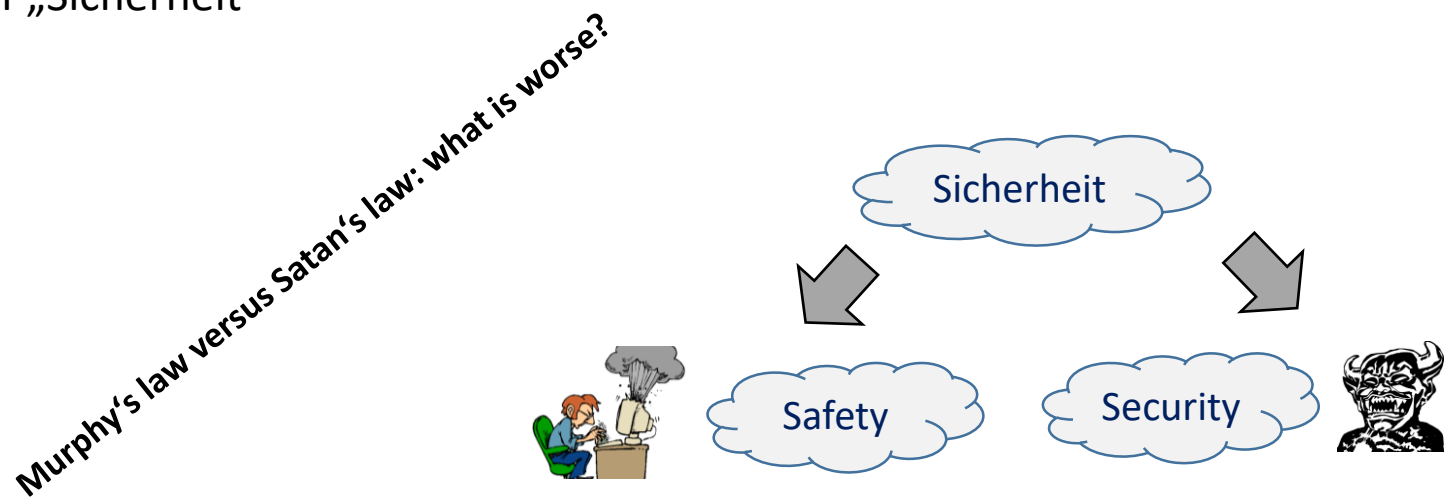




Honeypots, Platform Security and about Trustworthiness of Cars

Motivation

Definition of „Sicherheit“



Safety [„Betriebssicherheit“]:
„Anything that can go wrong *will* go wrong“

Security [„Angriffssicherheit“]:
Famous phrase: "Programming Satan's Computer“
Ross Anderson and Roger Needham, 2005

Honeypots, Platform Security and about Trustworthiness of Cars

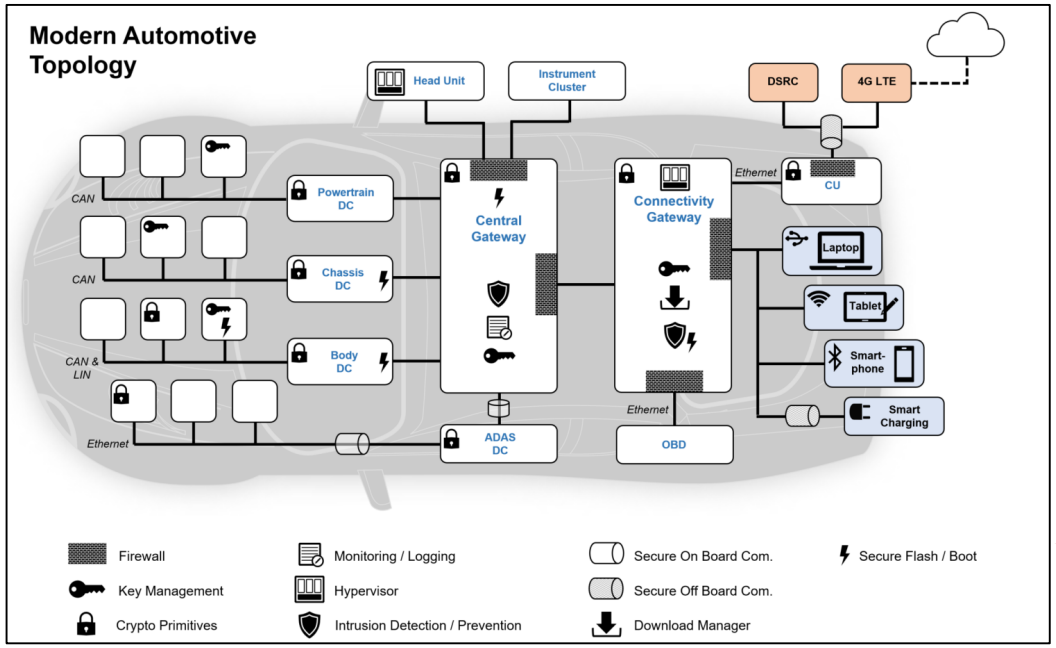
Motivation

Security of CASE megatrends – holistic concept and perimeter protection

+ Vorgehen auch in heutiger Cyber-Security State-of-the Art

+ Physikalische Angriffe in Fahrzeug sind zu modellieren, z.B. Car-Sharing oder Tuning/Diebstahl-Assets

Former defence arrangement Hiroshima



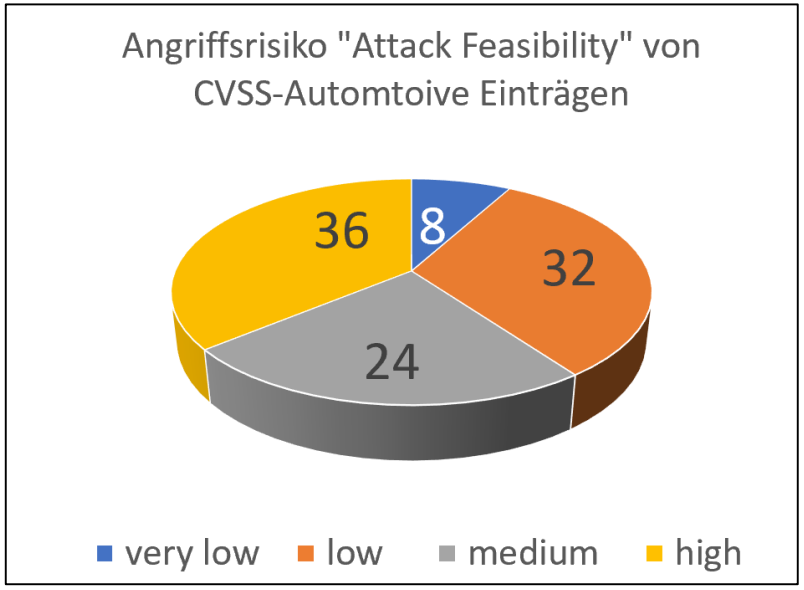
Source right: according to Lapczynski P. Secure Over the Air Software Updates, Vector Automotive Security Symposium 2016, Vector Informatik

Honeypots, Platform Security and about Trustworthiness of Cars

Motivation

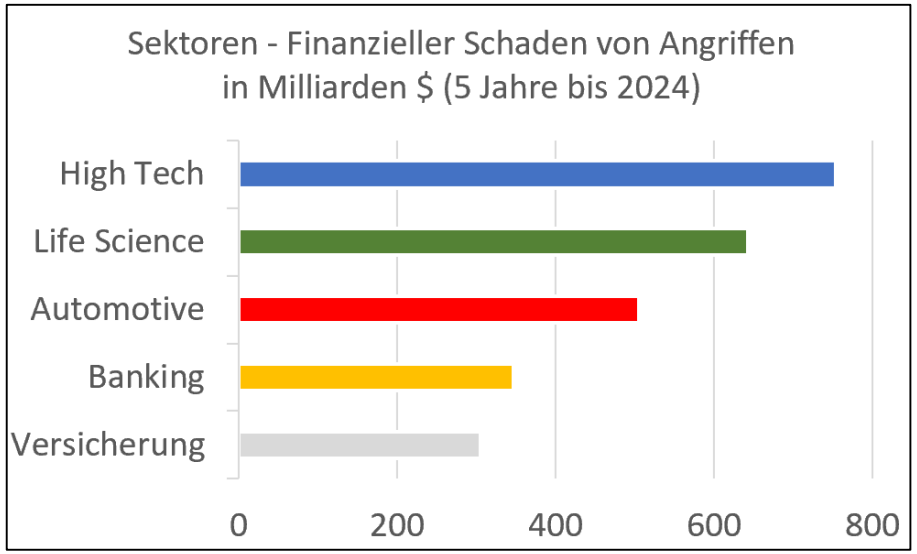
Relevance automotive Security – Facts and figures

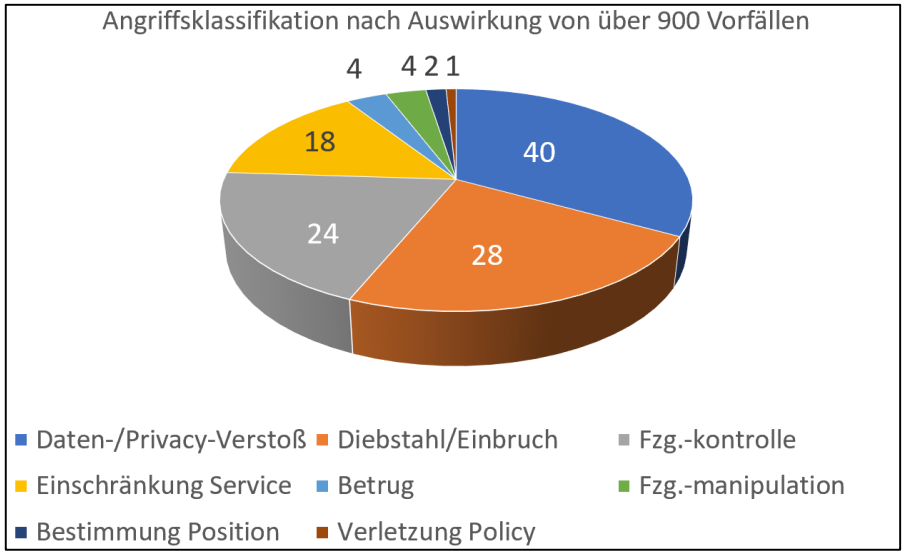
- Growth of globally connected vehicles from 2018 to 2023 of 134% from 330 millions to 775 millions [1]
- In 2025 a connected vehicle produces25 GB of data/h and up to 500 GB in case of a fully automated vehicle [3]
  → Forensics?
- 57% of all attacks have been black-hat attacks [3]



Bilder: according to[3]

[1] Juniper Research, CONNECTED CARS ~ HOW 5G, CONNECTED COMMERCE & BLOCKCHAIN WILL DISRUPT THE ECOSYSTEM, Whitepaper, https://www.juniperresearch.com/whitepapers/connected-cars-how-5g-connected-commerce-blockchain-will-disrupt-the-ecosystem, visited 2023-02-28
[2] Wevolver: High-Speed Data and Connected Cars, https://www.wevolver.com/article/high-speed-data-and-connected-cars, visited 2023-02-28
[3] Upstream Security: 2022 Global Automotive Cybersecurity Report, https://upstream.auto/2022report/





Honeypots, Platform Security and about Trustworthiness of Cars

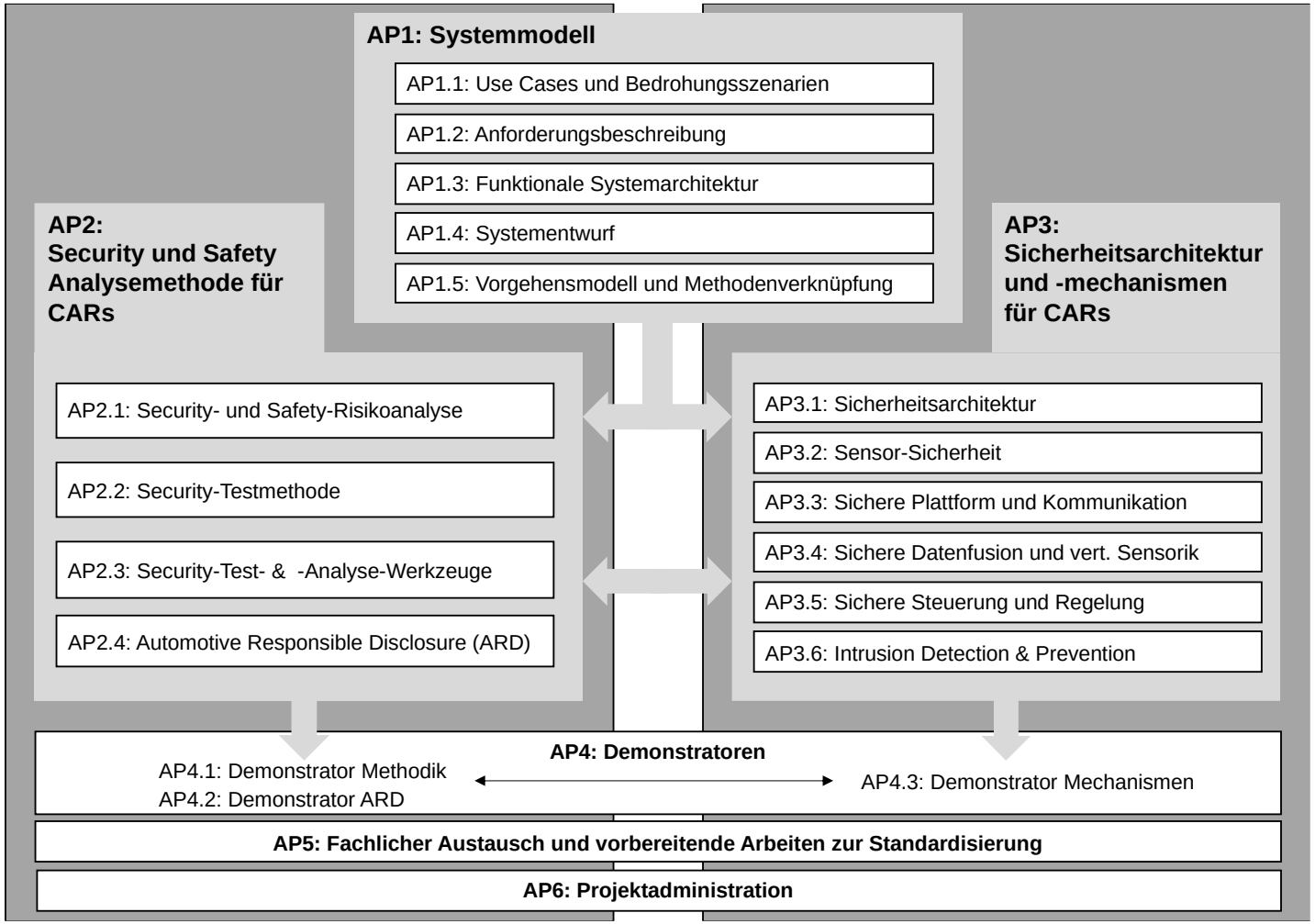
Project SecForCARs – Ziele und Struktur

SecForCARs
security for connected automated cars

The goal of the project is,

- to perform research on methods, principles and tools to protect critical automotive communication. The focus is put on the distributed control systems in the car which lead from the automotive sensors over the data being processed by the electronic control units and which lead to actions in actuators like brakes or steering wheels
- We want to extend the functional vehicle architecture with new, innovative security mechanisms which harden the control systems and significantly impede security attacks on it.
- ....

→ **Holistic approach in regard to „eascy“**



Results and Demonstrators: https://www.youtube.com/@secforcars8167

Honeypots, Platform Security and about Trustworthiness of Cars

Project SecForCARs – Kooperation mit japanischen Partnern

- Project Structure

WP2 Threat Intelligence

WP3 Vehicular Honeypots

WP4 Platform and Hardware Security

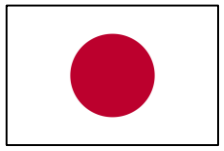
WP5 Security Composition for Automotive Systems of Systems

Lead: Japan | Lead: Germany

WP1: WS Organization
WP6: Exchange and Dissemination
WP7: Project Administration

Goals:

- International relations, novel partners, visibility
- Strategic exchange and knowledge transfer
- Market opener for industrial partners, also academia
- Participation on new challenges for the security challenges



funding by:
Bundesministerium für Bildung und Forschung

SIP ADUS – Strategic Innovation Program
Automated Driving for Universal Services

Honeypots, Platform Security and about Trustworthiness of Cars

Project SecForCARs – Kooperation mit japanischen Partnern

– Project Structure

WP2 Threat Intelligence

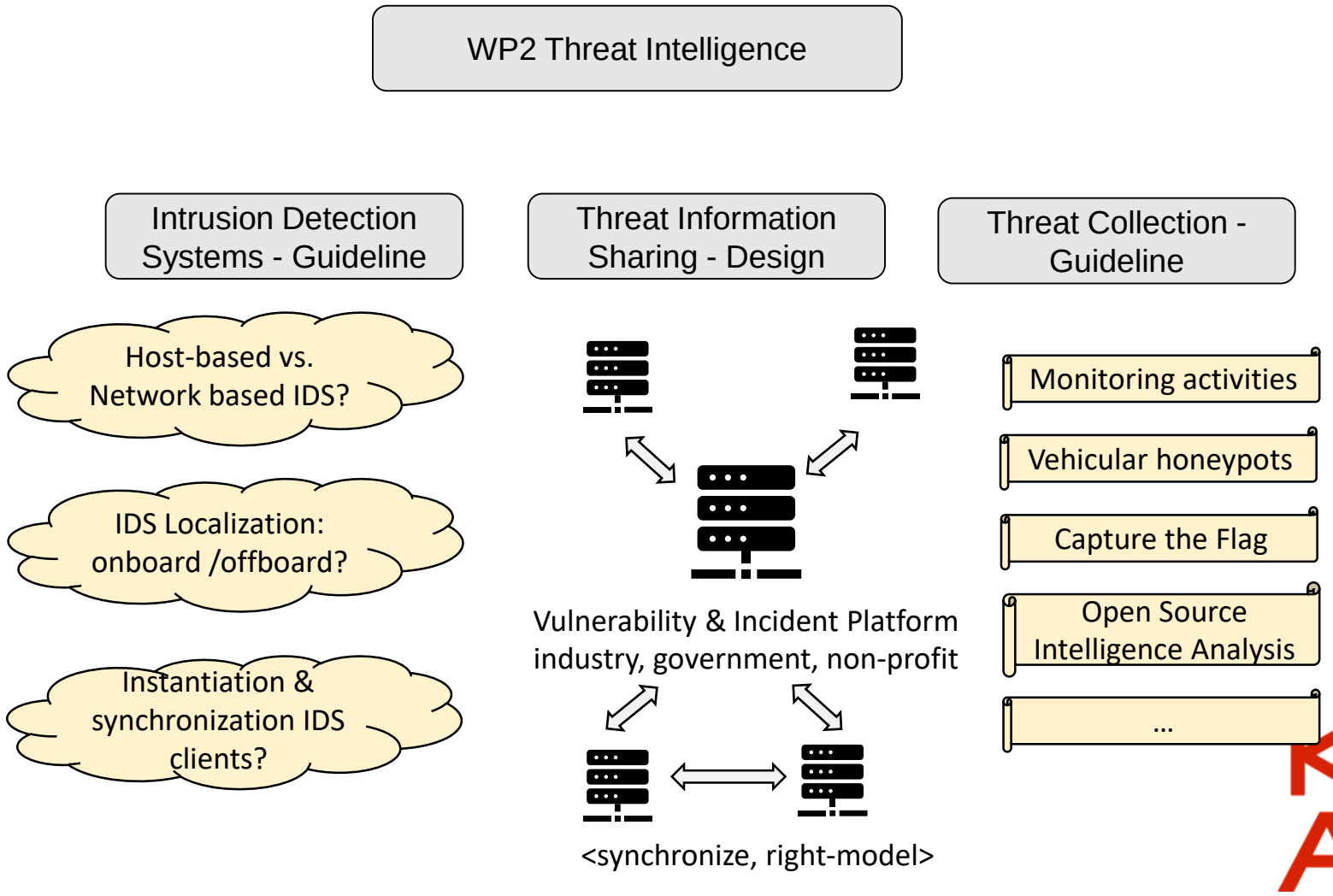
WP3 Vehicular Honeypots

WP4 Platform and Hardware Security

WP5 Security Composition for Automotive Systems of Systems

Lead: Japan | Lead: Germany

WP1: WS Organization
WP6: Exchange and Dissemination
WP7: Project Administration



Honeypots, Platform Security and about Trustworthiness of Cars

Project SecForCARs – Kooperation mit japanischen Partnern

– Project Structure

WP2 Threat Intelligence

WP3 Vehicular Honeypots

WP4 Platform and Hardware Security

WP5 Security Composition for Automotive Systems of Systems

Lead: Japan | Lead: Germany

WP1: WS Organization
WP6: Exchange and Dissemination
WP7: Project Administration

WP3 Vehicular Honeypots

[…] a honeypot is a computer security mechanism set to detect, deflect, or, in some manner, counteract attempts at unauthorized use of information systems. Generally, a honeypot […] appears to be a legitimate part of the site which contains information or resources of value to attackers. It is actually isolated, monitored, and capable of blocking or analyzing the attackers. [Wikipedia 2023]

Automotive: e.g. focus on connected devices (telematics units, OBD-diagnostics devices….), in particular legacy devices

- Discover (malicious) connected devices
- Analyse and formalize behaviour
- Build honeypot based on behaviour of discovered devices
- Record and analyse attackers

Honeypots, Platform Security and about Trustworthiness of Cars

Project SecForCARs – Kooperation mit japanischen Partnern

– Project Structure

WP2 Threat Intelligence

WP3 Vehicular Honeypots

WP4 Platform and Hardware Security

WP5 Security Composition for Automotive Systems of Systems

Lead: Japan | Lead: Germany

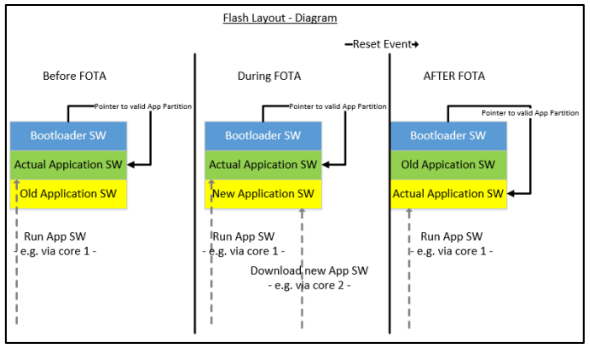
WP1: WS Organization
WP6: Exchange and Dissemination
WP7: Project Administration

WP4 Platform and Hardware Security

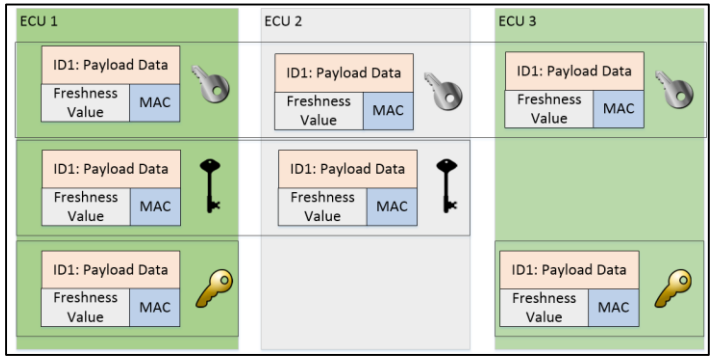
Why Platform and HW security? → Example Use Cases: Over-the-Air (OTA) services and updates
– Remote Feature Activation, Features on Demand, Car Access
– Update capabilities
Functional features
– Rights issuing, offline authentication, online/offline delegation, online revocation
Security Goals: End-2-end authenticity, confidentiality, (availability)

….exemplary design choices….

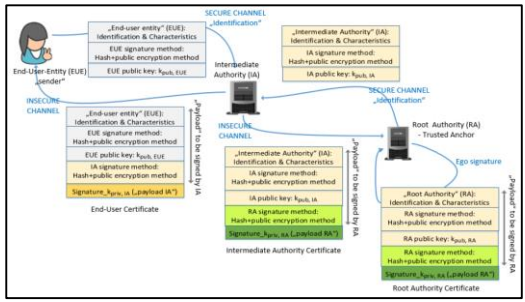
Flash-strategy: in-place versus A/B (here: A/B)



Security onboard network communication – VLAN approach



Chain of trust & key revocation concept



Honeypots, Platform Security and about Trustworthiness of Cars

Project SecForCARs – Kooperation mit japanischen Partnern

- Project Structure

WP2 Threat Intelligence

WP3 Vehicular Honeypots

WP4 Platform and Hardware Security

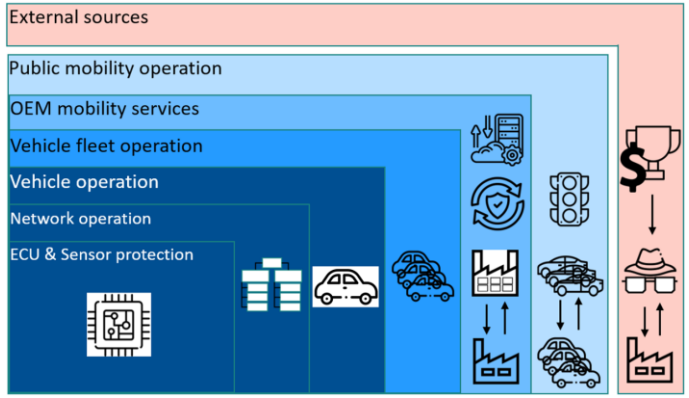
WP5 Security Composition for Automotive Systems of Systems

Lead: Japan | Lead: Germany

WP1: WS Organization
WP6: Exchange and Dissemination
WP7: Project Administration

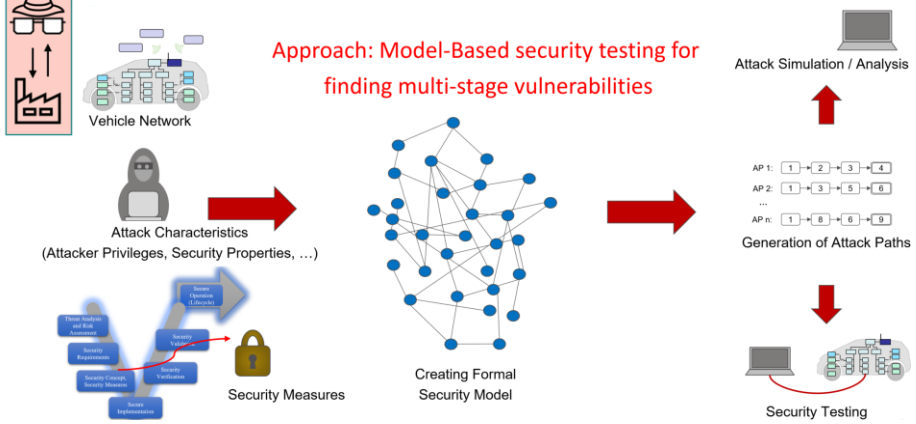
WP5 Security Composition for Automotive Systems of Systems

- Automotive Mobility involves many layers, from HW, SW to onboard network to OEM and fleet applications to mobility, IoT and public mobility infrastructure
- Which security artefact on which layer? Synchronisation? Common holistic approach? Trust?



….exemplary research topic…

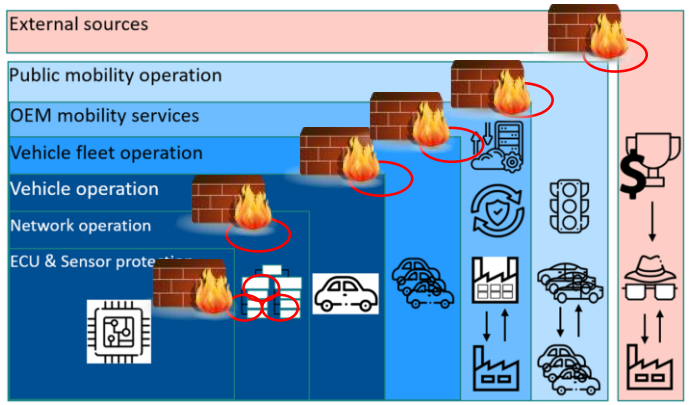
Automated modelling and detection of risks
Of multi-path attacks



Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive

– Exemplary security artefact: Automotive Firewall



… some definitions…

Firewall: system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules (*)

+ non-cryptographic security operations: security algorithms which can be realized without provision of cryptographic primitives, no TPM/ HSM hardware

– (-): gating speed: additional checks within µs → usage of dedicated communication chips

E-2-E security: the way of ensuring that data transmitted through an information system stays secure and safe from origin point to destination. (**)

– (-): firewalls don't provide E-2-E security

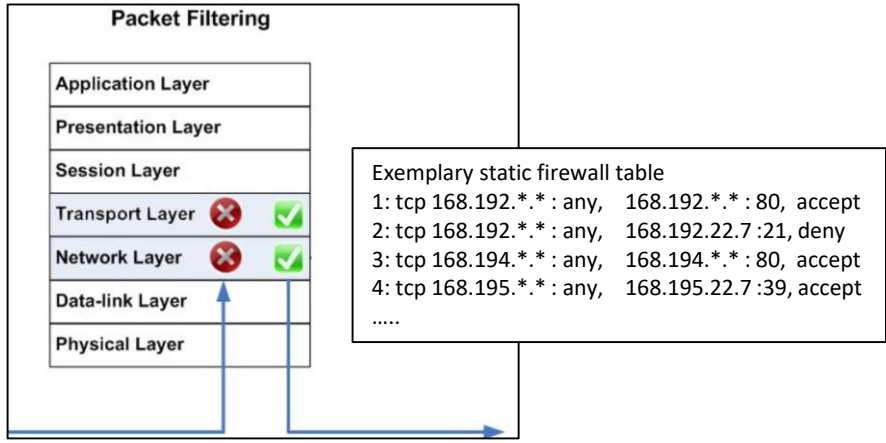
(*) according to: *Boudriga, Noureddine (2010). Security of mobile communications. Boca Raton: CRC Press. pp. 32–33*
(**) according to Heimdal Cyber Security Glossary: https://heimdalsecurity.com/glossary/end-to-end-security (27.01.2017)

Source: https://commons.wikimedia.org/wiki/File:Suzuki_alto_body2_-_AIMS.JPG. CC 3.0 license. 03.03.2023

Honeypots, Platform Security and about Trustworthiness of Cars

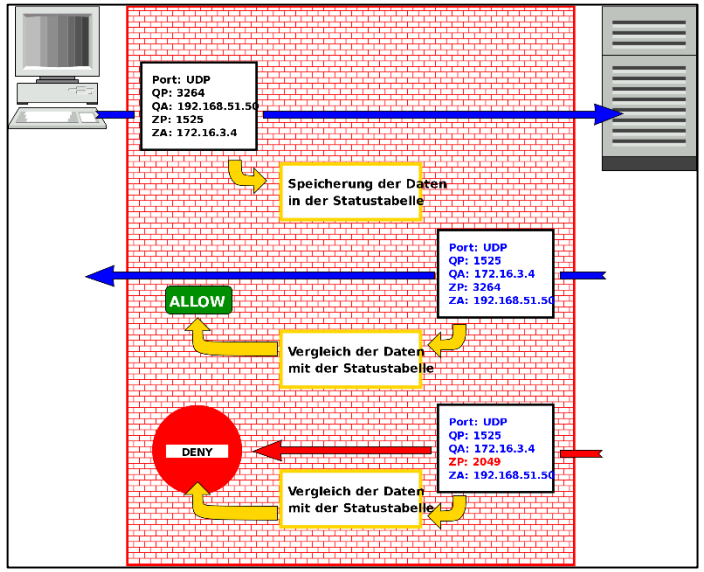
Firewalls – a technical dive

- Types of IT firewalls: often static or dynamic package filters
  - Static filters decide based on TCP/IP address
  - Dynamic or stateful filters include history on decision



- Difference to “Access Control Systems”?
  - access control not restricted only from “outside” unity, e.g. for programs
  - possess more flavours / approaches to allow resource admissions, e.g.
    - Identity based access control (IBAC)
    - Role based access control (RBAC)
- Use Case vehicle?

Which firewalls? How? Where?
Are access control systems useful? Which roles may exist?



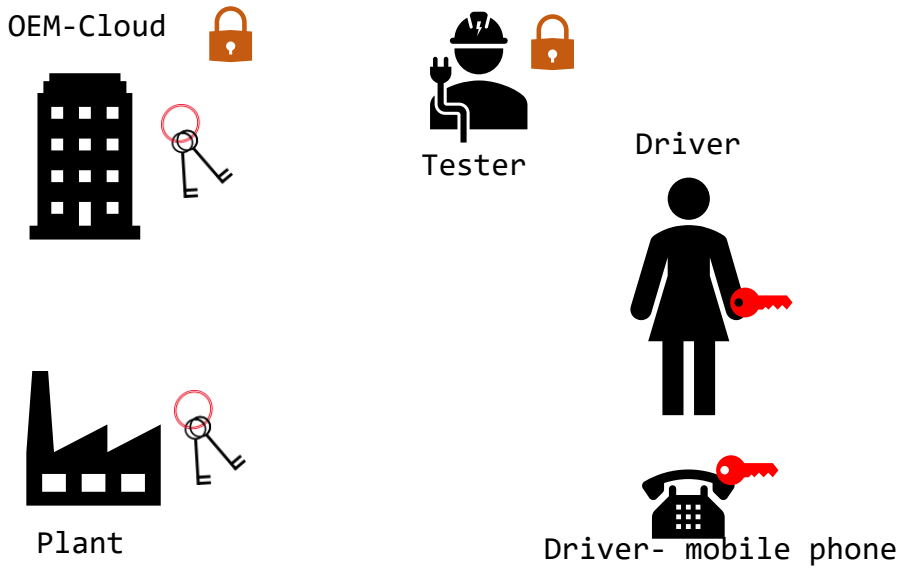
Packet Filtering: Wikipedia: https://upload.wikimedia.org/wikipedia/commons/6/67/OSI_Packet_Filter.jpg, CC3.0 license, 03.03.2023
Dynamic Package Filtering: https://de.wikipedia.org/wiki/Firewall#/media/Datei:Stateful_inspection_udp.svg

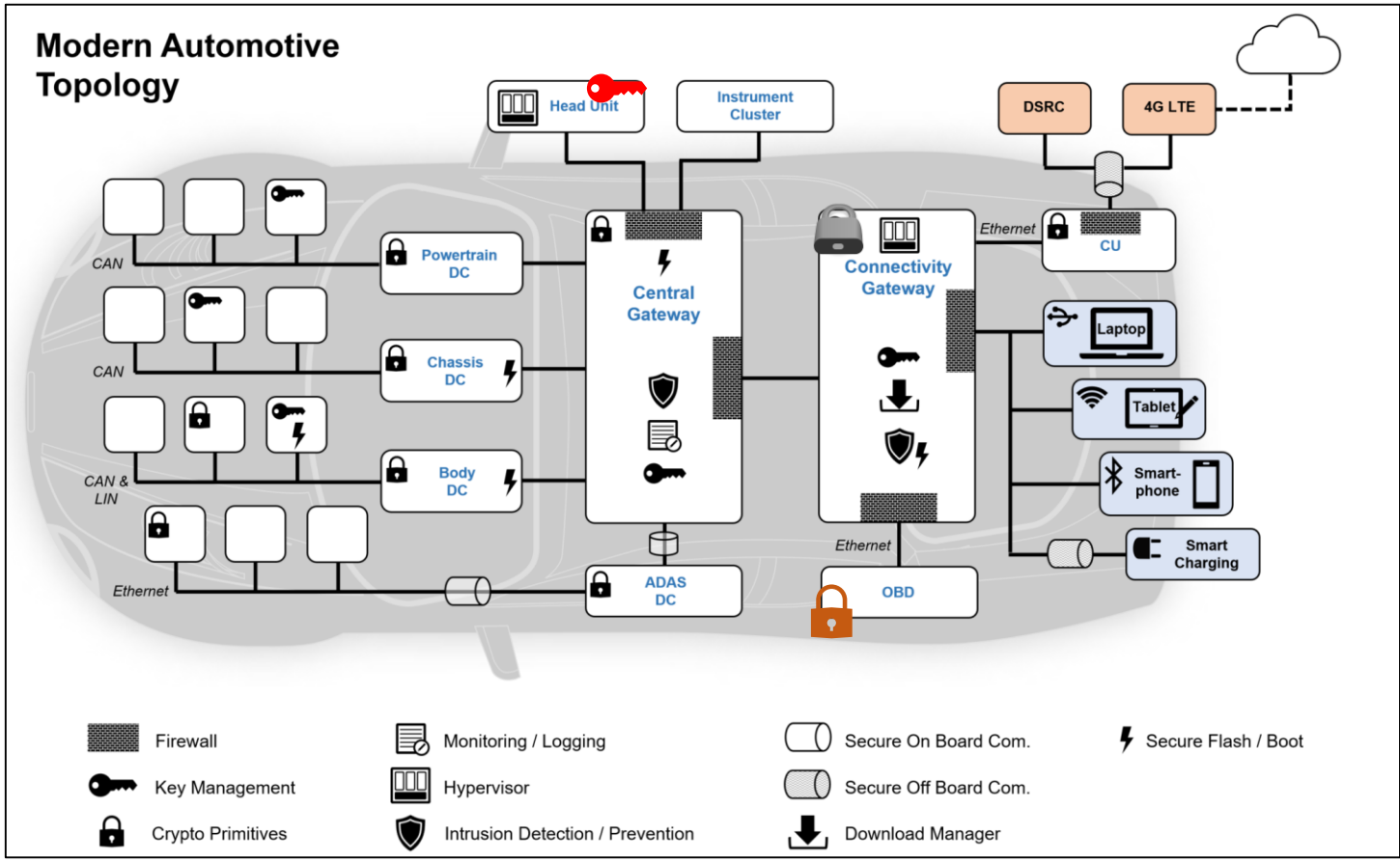
Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive

- Identity based access control system: key(less) entry / go
- Role based access control systems:
  - OTA services – diagnostics, SW updates
  - Traditional diagnostics via OBD
  - Key injection at plant
  - and many more…

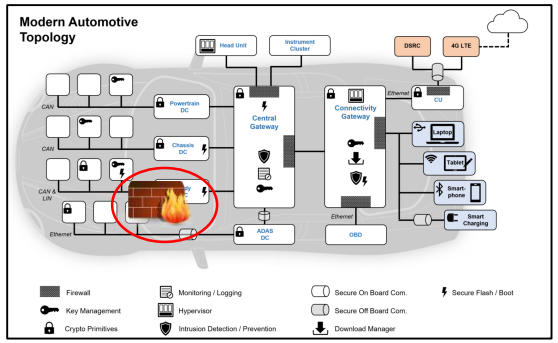
- Necessity of cryptographic material
- Unequal to firewall setup





Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive



Onboard Car communication – firewall techniques, role-based access hot topic

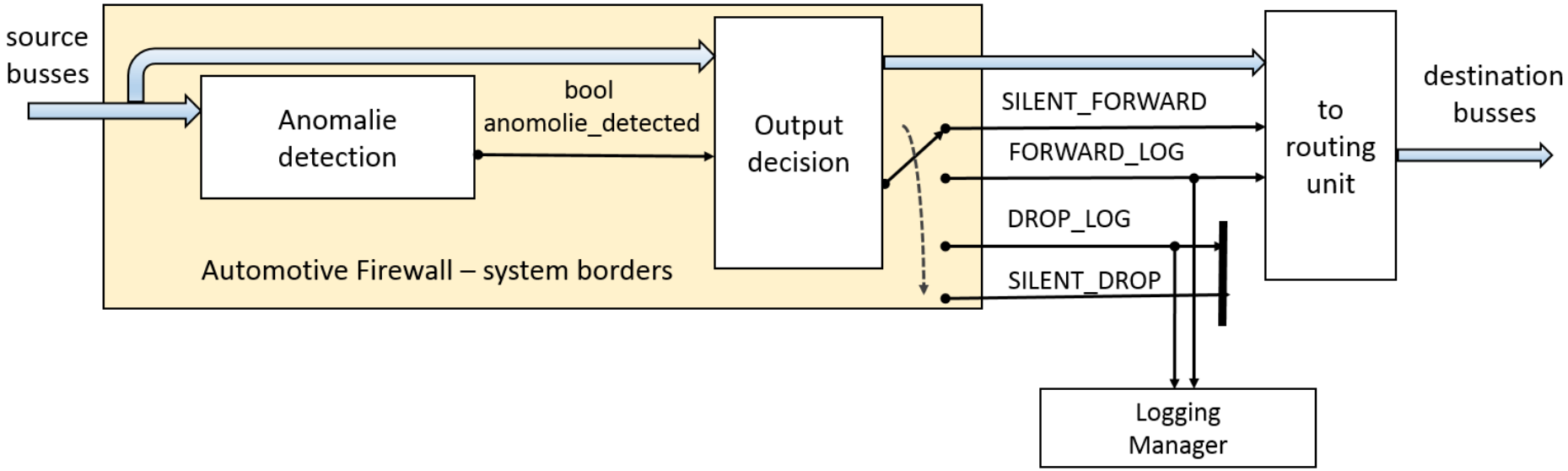
System definition firewall – grey box

Intermediate classification of incoming messages:

+ binary classification "*anomaly detected*" vs. "*no anomaly detected*"

Final decision: forwarding and/or logging of message

+ further action based on classification and message/event significance, see picture



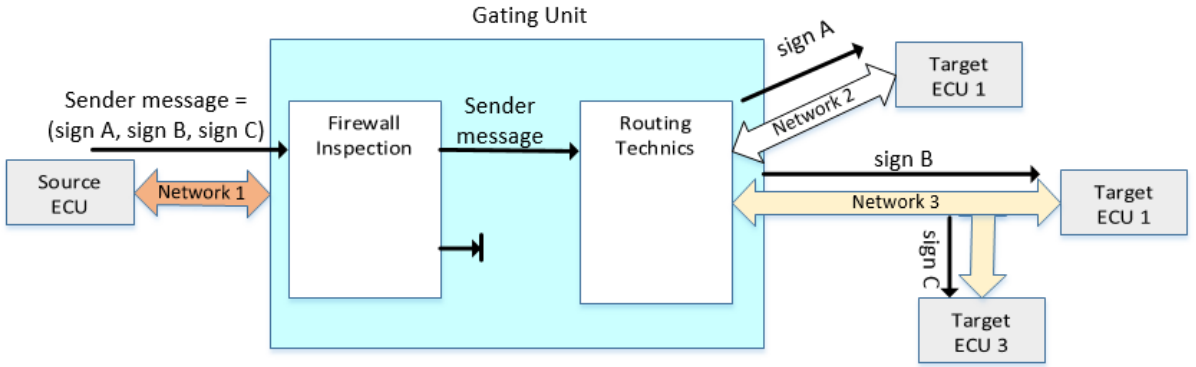
Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive

Firewall unit versus routing unit – overall gating system definition

Variants: routing technologies of messages may vary due to

- different bus protocols on sender / receiver sides (CAN, Ethernet,…)
- signal / frame routing in case of identical sender / receiver protocols



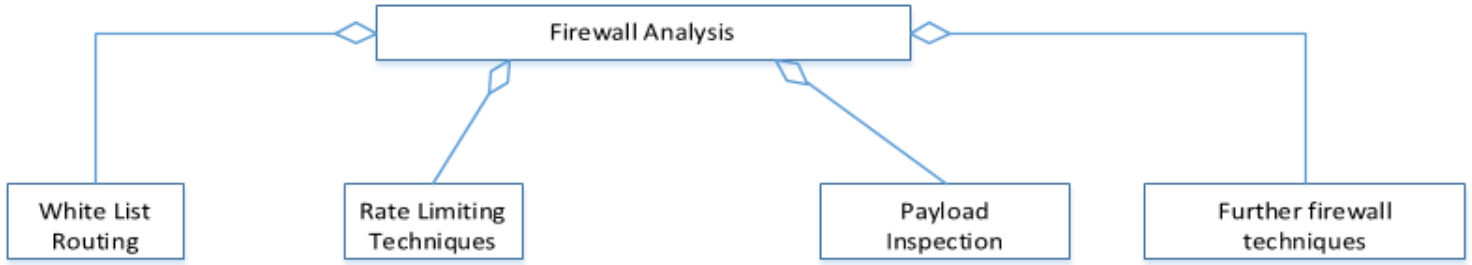
Firewall techniques rely on the inspection of the sender network, routing techniques can be seen to be applied later (in case of *FORWARD<_LOG>* decision)

in case of signal routing the substitution values of individual signals on destination busses have to be specified

Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive

Firewall implementation includes techniques like *white list routing*, *rate limiting* or *payload detection*



- additional techniques apply in IT security, e.g. usage of *black lists*
- → often not transferable or implicitly realized, e.g. CAN controller module is configured in form of (receive) message objects with defined (white list) CAN-ID

- Comparison to IT: automotive implementations correspond to “static package filtering”

- Further checks based on cryptographic means are regarded to be E-2-E security

Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive

Automotive Firewall – features:: white list routing

White list routing

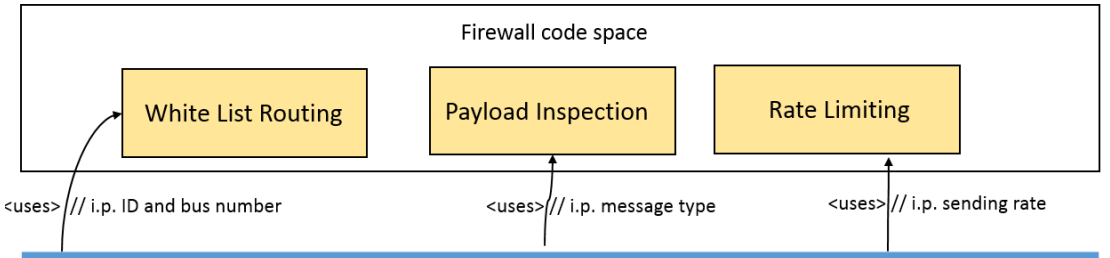
- only messages with known identifier pass firewall (”*header inspection*”)
- additional check of sender bus origin

Analysis

- suited against attempts to send malicious messages with *unknown* IDs
- *not* suited against attempts to send malicious messages with *known* IDs

Implementation

- usage of *routing table* (see picture)
- header inspection engine may be separated in implementation from payload inspection engine due to different ownership and update/configurability issues

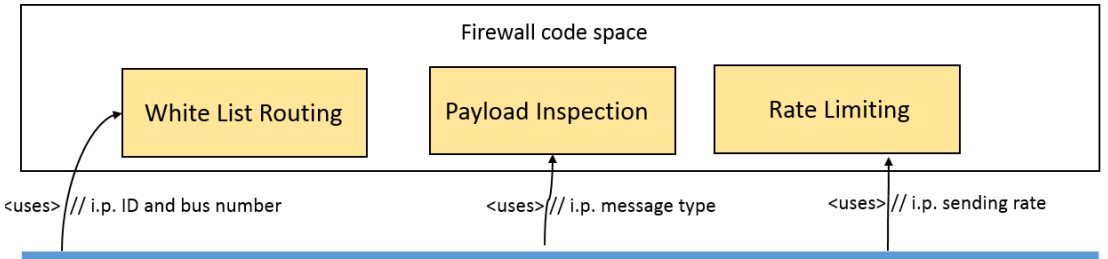


ROUTING TABLE – PARAMETRIZATION FILE

ID	sender busses	dest. busses	charact. <x1>	message type (send bus)	sending type (send bus)	message rate (send bus 1)	charact. <x3>
ID212	A, B	C	…	normal	cyclic	14 msg/sec	…
ID 65	A	B	…	normal	cyclic on event	14 msg/sec	…
ID 443	C	B	…	diagnostics	sporadic	50 msg/sec	…
…	…	…	…	…	…	…	…

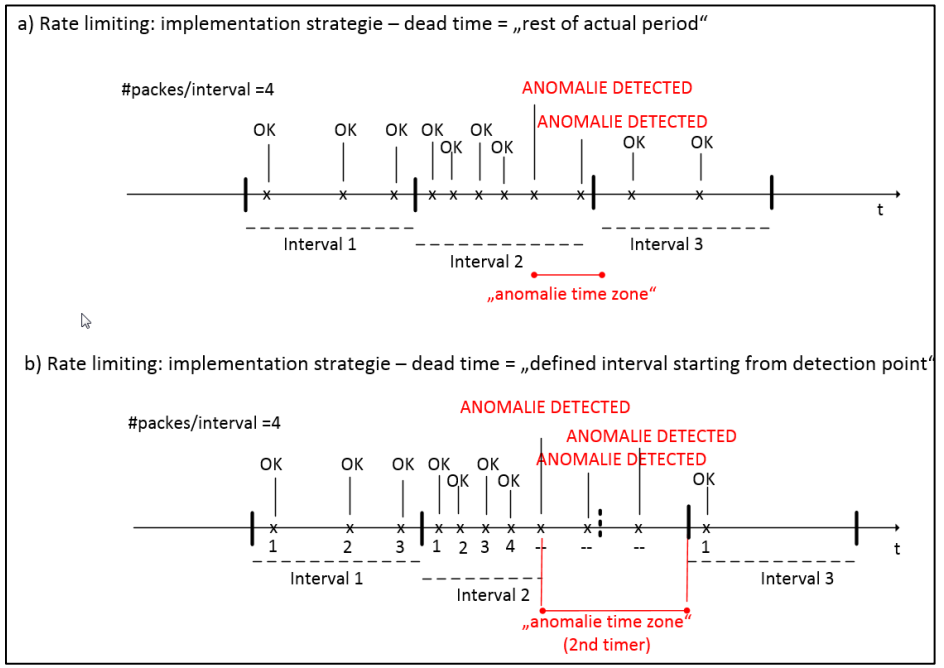
Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive



ROUTING TABLE – PARAMETRIZATION FILE

ID	sender busses	dest. busses	charact. <x1>	message type (send bus)	sending type (send bus)	message rate (send bus 1)	charact. <x3>
ID212	A, B	C	...	normal	cyclic	14 msg/sec	...
ID 65	A	B	...	normal	cyclic on event	14 msg/sec	...
ID 443	C	B	...	diagnostics	sporadic	50 msg/sec	...
...	...	...	...	...	...	...	...



Automotive Firewall – features:: Rate Limiting Techniques

- techniques to control the traffic rate within a (destination) network
- vehicle context: detect messages "being sent above typical rate“

Analysis

- suited against attempts to send/spam malicious messages with *known* IDs, in particular against *Denial-of-Service* (DoS) attacks
- efficient implementations possible (counter)
- not suited against sending malicious content to destination – e.g. attacker sends first message after recovery

Implementation

- possible usage of *routing table* with entry field *“#messages / time interval”*, see picture
- dead-time to be defined after a positive anomaly detection, see picture

Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive

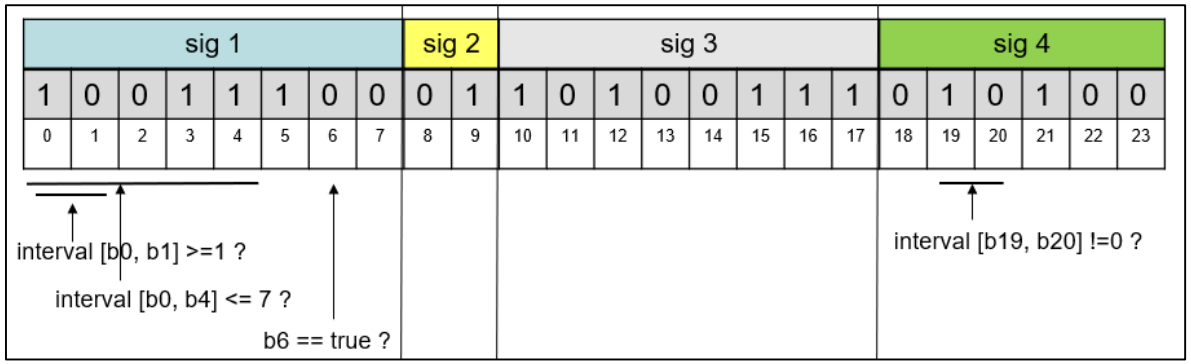
Automotive Firewall – features:: payload inspection

Payload inspection

- inspection of semantical data (complementary to “header inspection”)
- Possible signal value range and message structure must be known in advance
- different treatment of „*normal communication messages*“ and messages with nested protocols, e.g. *diagnostics messages*

Analysis

- suited against change/ insertion to non-useful semantical values (by attacker)
  - can be seen as “low-level analogon” to *Message Authentication Codes* (MAC)
  - “carefully falsified values” by attacker are not detected by payload analysis

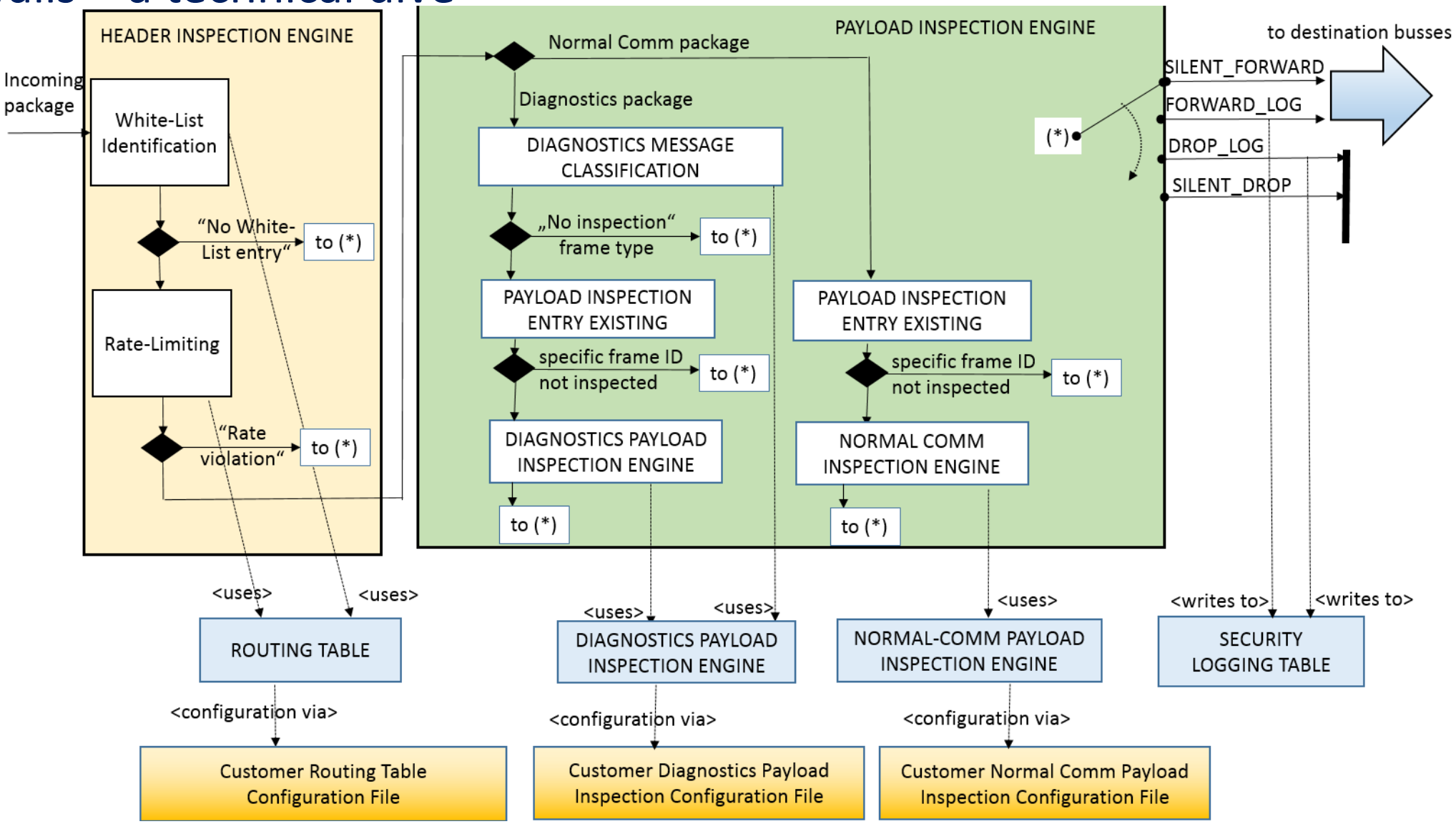


Normal communication frames

- signal sizes within a message may vary – need to investigate arbitrary bit intervals
- interval investigation options: bitwise comparison or range comparison
- investigation of multiple intervals should be possible
- investigation of multiple schemes within an interval should be possible

Honeypots, Platform Security and about Trustworthiness of Cars

Firewalls – a technical dive



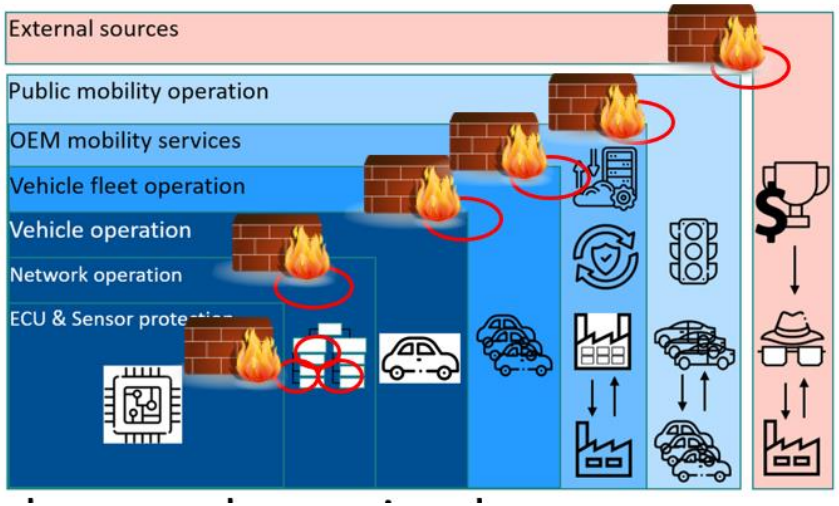
Honeypots, Platform Security and about Trustworthiness of Cars

Conclusion and challenges

<u>Firewalls and access techniques</u>:

Different trends to secure access onboard-site and offboard-site

+ Usage of access control and cryptographic means offboard-site, usage of efficient firewalls onboard
+ Onboard: conglomeration of different security artefacts hardens access to ECUs, function manipulation and data
+ Efficiency for onboard routing leads to adapted communication controllers (Ethernet, CAN,…)



Honeypots, Platform Security and about Trustworthiness of Cars

Conclusion and challenges

General view on automotive security

+ Holistic approach in automotive security which comprises multiple aspects of security, see e.g. WP definitions
+ Technical dive into firewalls shows only small part WP5

Outlook:

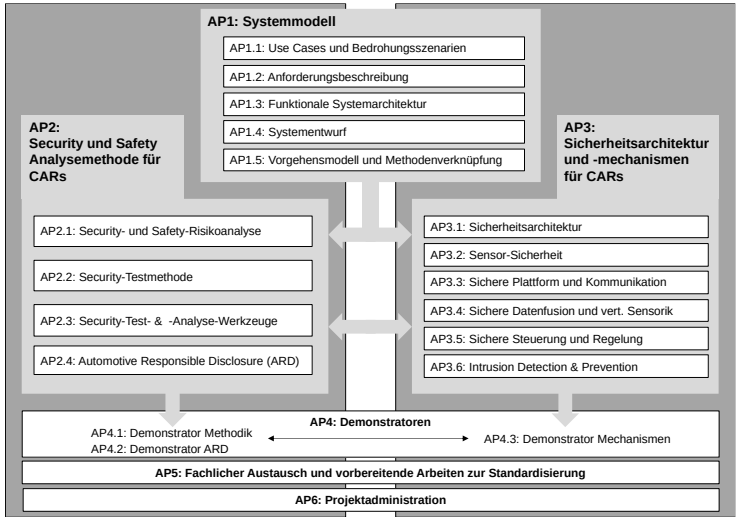
+ Further rising security significance due to megatrends
+ Privacy issues so far not really in focus, topic which will change due to “Shared” megatrend

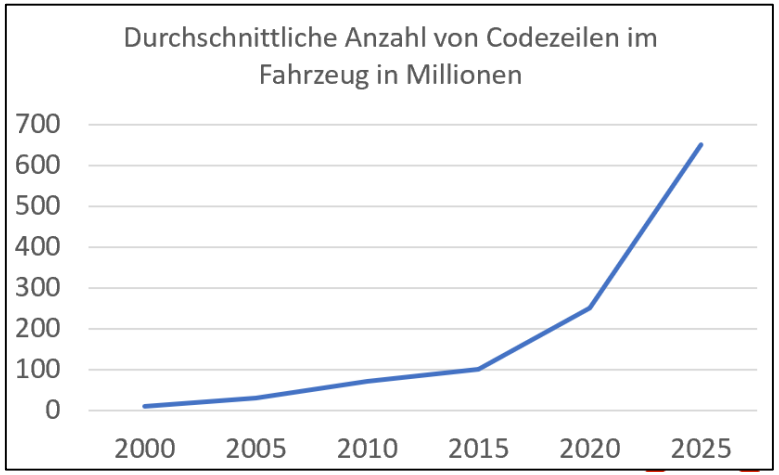
WP2 Threat Intelligence

WP3 Vehicular Honeypots

WP4 Platform and Hardware Security

WP5 Security Composition for Automotive Systems of Systems





Sicherheit für vernetzte, autonome Fahrzeuge - Projekt SecForCARs

Project SecForCARs – Kooperation mit japanischen Partnern

Funding: Research was performed within the SecForCarsproject, funded by German „Bundesministerium für Bildungund Forschung“ (BMBF)

SecForCARs
security for connected automated cars

Bundesministerium
für Bildung
und Forschung

Thank you