Work-in-Progress: Emerging E/E-Architectures as Enabler for Automotive Honeypots

Niclas Ilg[1,2], Dominik Germek[1], Paul Duplys[3], Michael Menth[2]

[1]Corporate Research at Robert Bosch GmbH, Germany

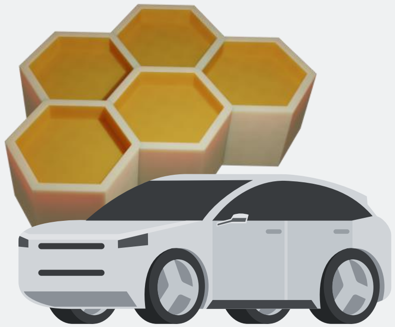
[2]University of Tuebingen, Germany

[3]Sector Mobility at Robert Bosch GmbH, Germany

BOSCH

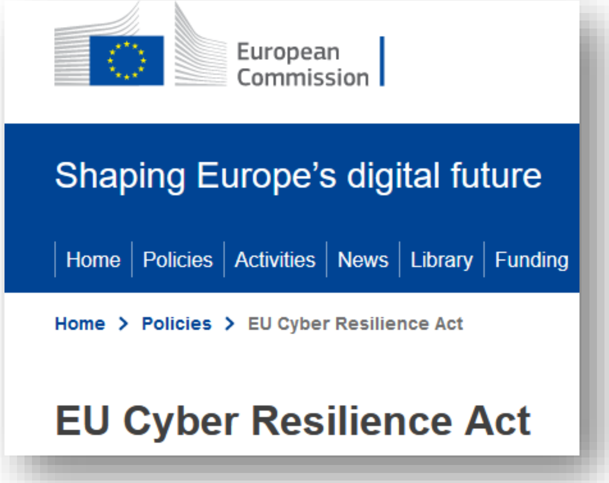
Emerging E/E-Architectures as Enabler for Automotive Honeypots

Agenda



1. Introduction
2. State of Automotive Honeypots
3. Opportunities for In-Vehicle Honeypots
4. Concept for Internet-deployed Honeypots
5. Q&A

Introduction
Regulations, norms, and real-world incidents



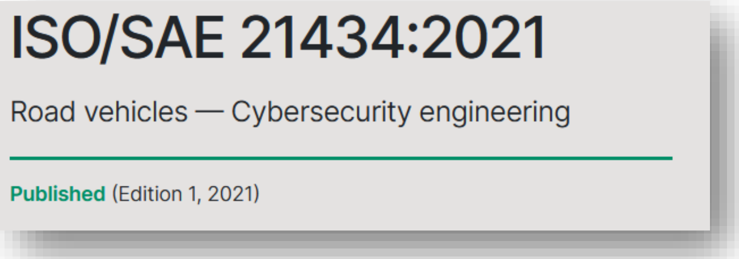
European Commission

Shaping Europe's digital future

Home | Policies | Activities | News | Library | Funding

Home > Policies > EU Cyber Resilience Act

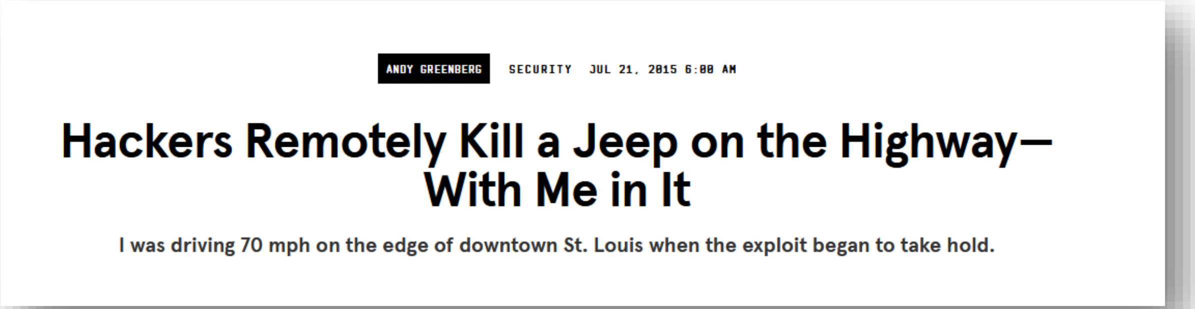
EU Cyber Resilience Act



ISO/SAE 21434:2021

Road vehicles — Cybersecurity engineering

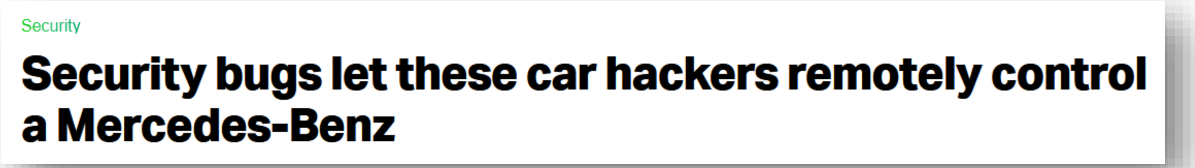
Published (Edition 1, 2021)



ANDY GREENBERG SECURITY JUL 21, 2015 6:00 AM

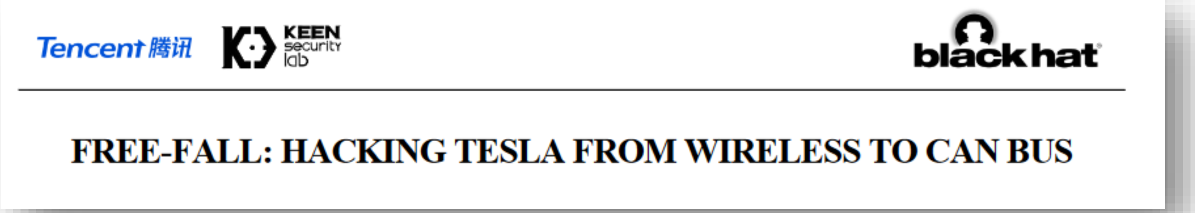
Hackers Remotely Kill a Jeep on the Highway—With Me in It

I was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.



Security

Security bugs let these car hackers remotely control a Mercedes-Benz



Tencent腾讯 KEEN security lab black hat

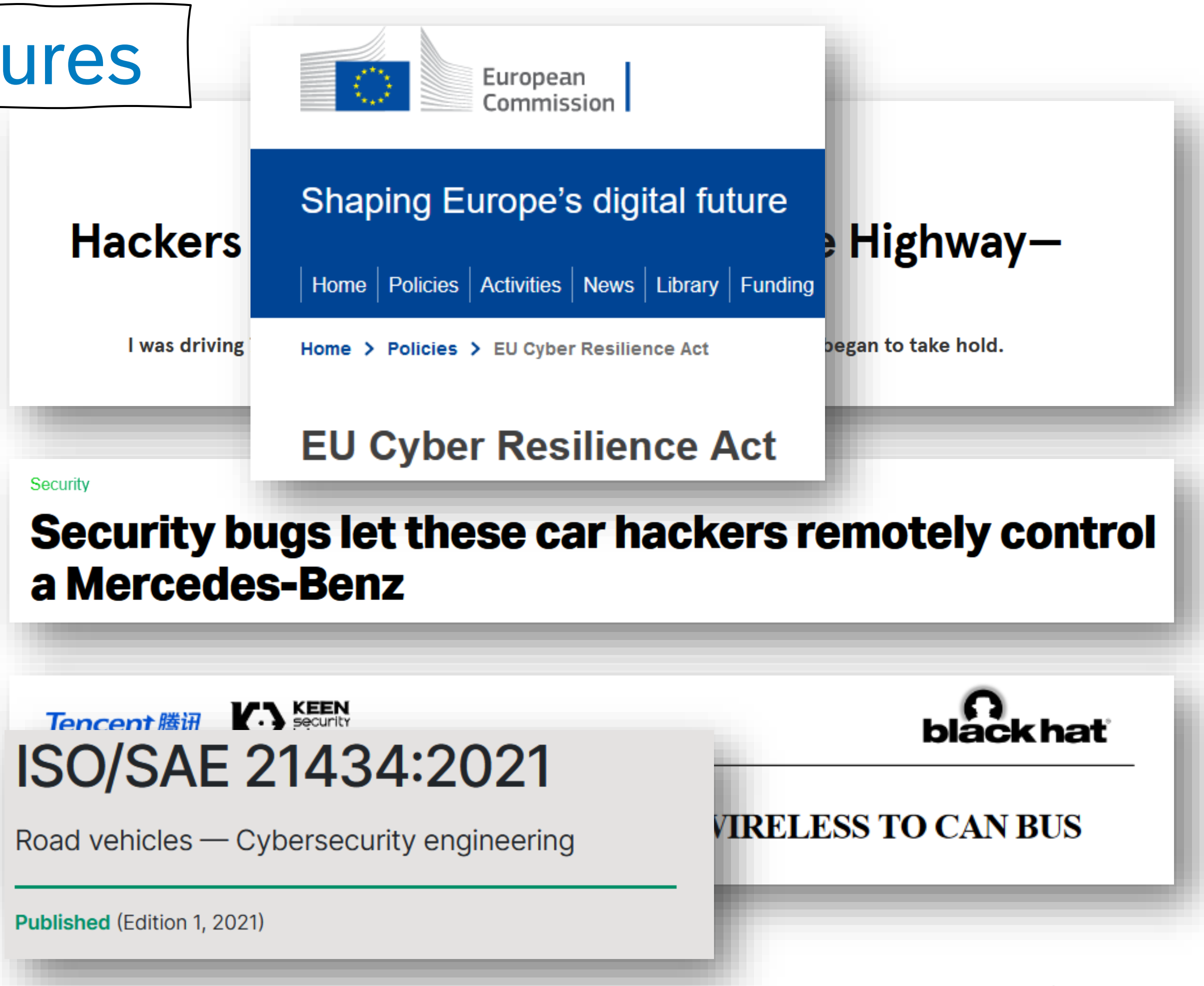
FREE-FALL: HACKING TESLA FROM WIRELESS TO CAN BUS

Introduction

Regulations, norms, and real-world incidents

& countermeasures

- Hardening (a lot)
- Upcoming efforts in intrusion detection (& prevention)
- Threat intelligence/attack landscape monitoring?


European Commission

Shaping Europe's digital future

Home > Policies > EU Cyber Resilience Act

EU Cyber Resilience Act

Hackers e Highway—

I was driving egan to take hold.

Security

Security bugs let these car hackers remotely control a Mercedes-Benz

ISO/SAE 21434:2021

Road vehicles — Cybersecurity engineering

Published (Edition 1, 2021)

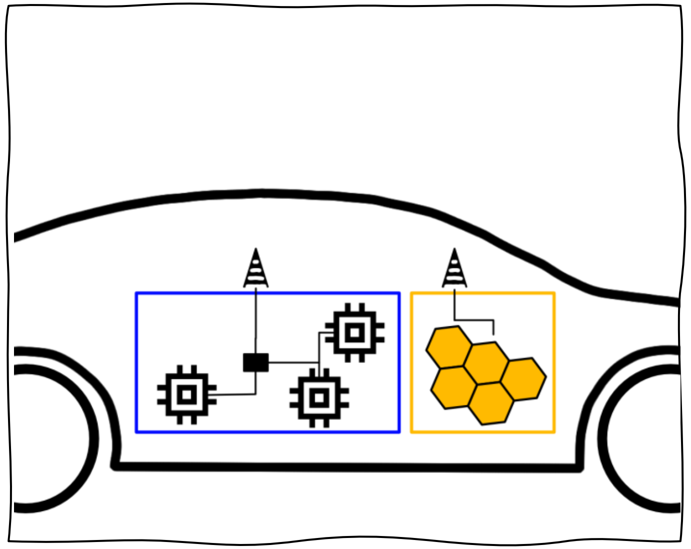
IRELESS TO CAN BUS

2

State of Research Automotive Honeypots

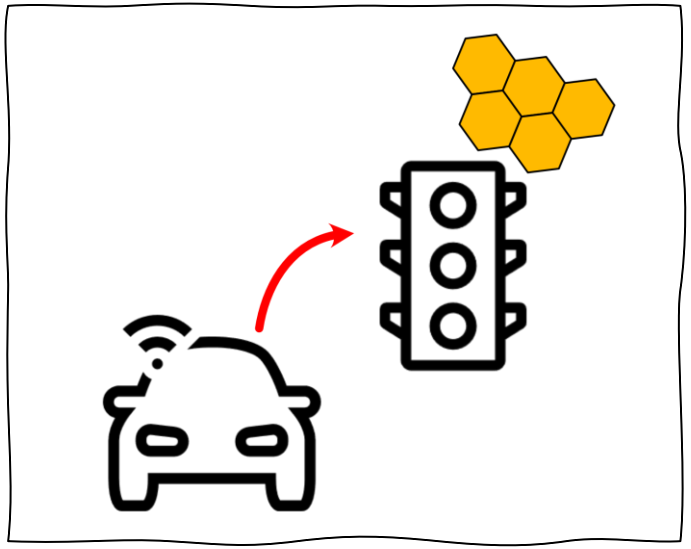
Research on Automotive Honeypots

State of Research



In-vehicle honeypot

- Realistic environment
- Separate hardware
- Real vehicle data



V2X honeypot

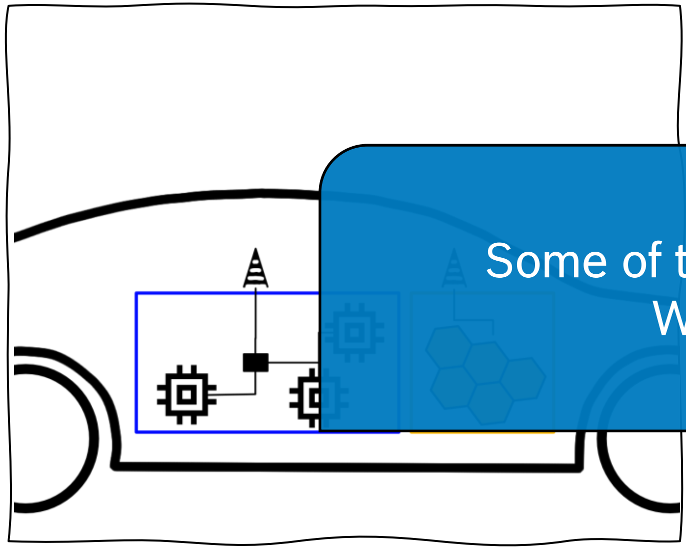
- Attacks on moving vehicles
- Infrastructure honeypots

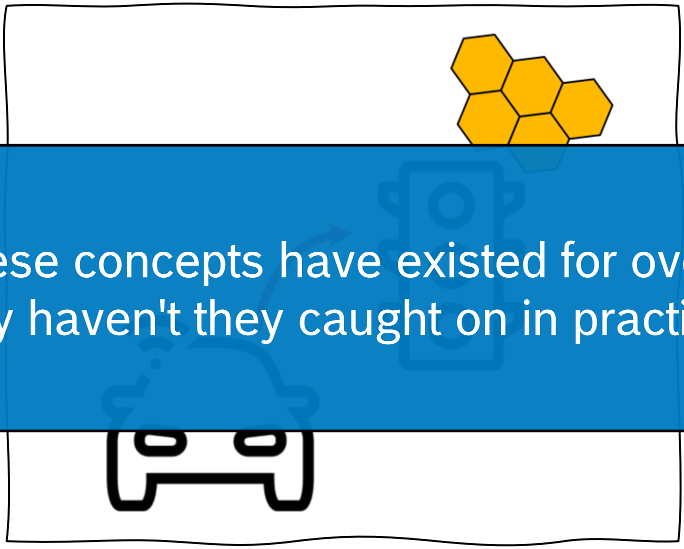
  e.g., charging stations for EVs

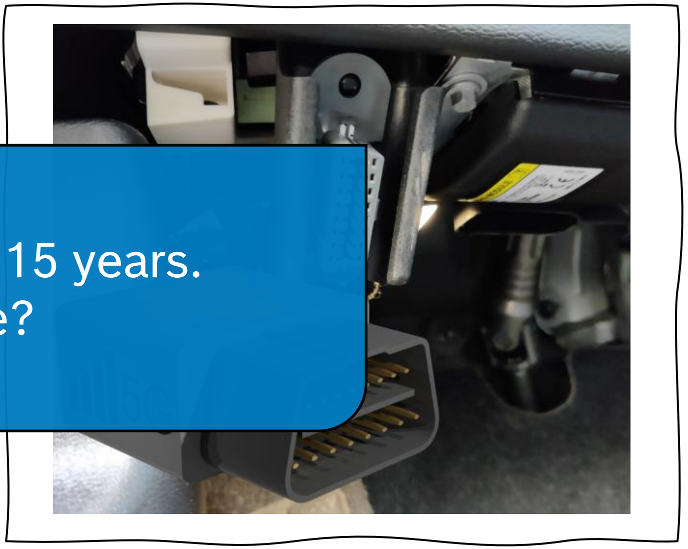
IoT honeypot

- OBD-II dongles (debug interface)
- IoT components on the Internet

Research on Automotive Honeypots
State of Research







Some of these concepts have existed for over 15 years.
Why haven't they caught on in practice?

In-vehicle honeypot

- Realistic environment
- Separate hardware
- Real vehicle data

V2X honeypot

- Attacks on moving vehicles
- Infrastructure honeypots

  e.g., charging stations for EVs

IoT honeypot

- OBD-II dongles (debug interface)
- IoT components on the Internet

Automotive Honeypot Research

Limitations of Current Approaches

Credibility

&

Accessibility

Limited data
&
Simulation quality

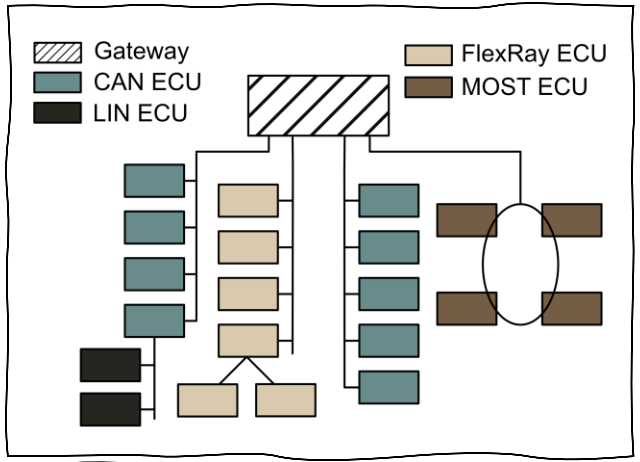
Utilization
of findings

3

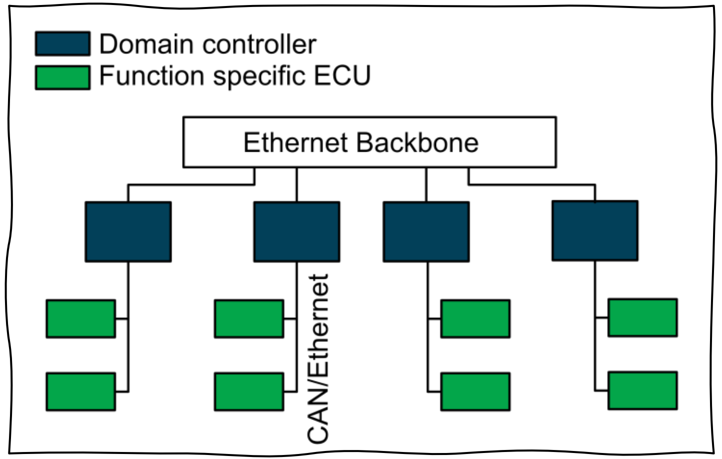
Opportunities for In-Vehicle Honeypots

BOSCH

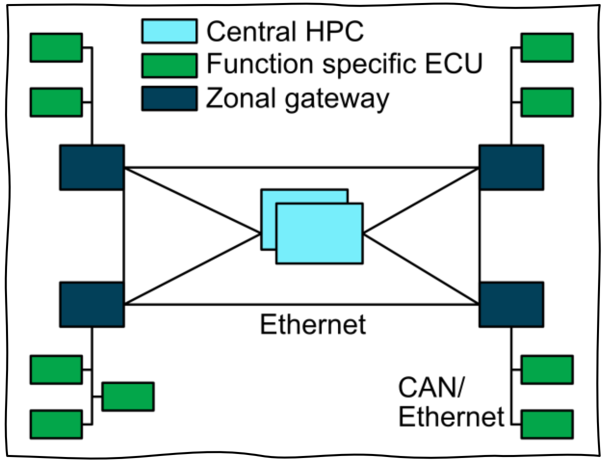
Emerging E/E-Architectures
From gateway to zone



Gateway architecture



Domain architecture



Zonal architecture

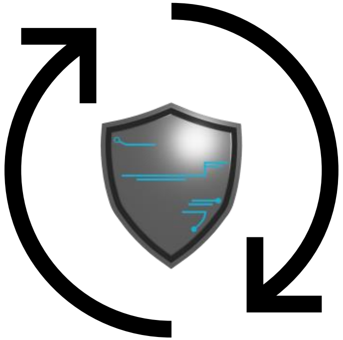
De-couple hardware and software

Centralize resources & increase performance

High Performance Computing

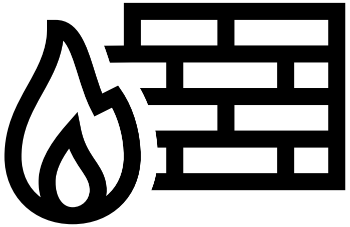
From gateway to zone

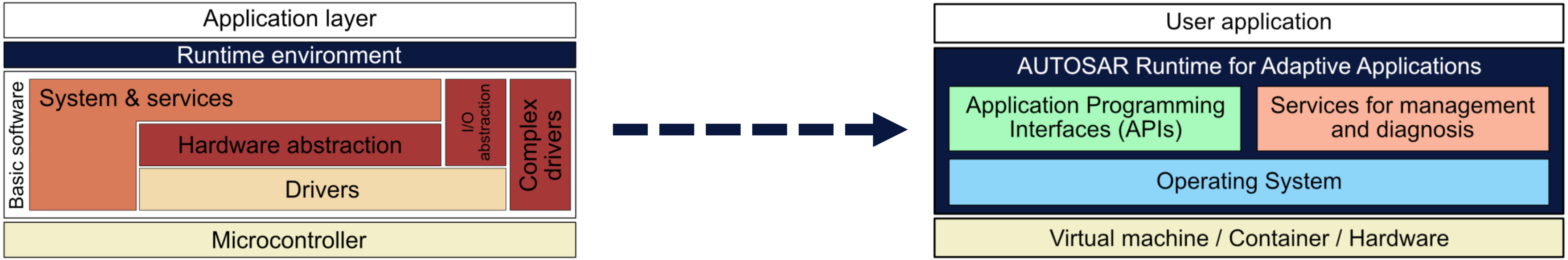
Security updates



Deployment resources

Network segmentation





Application layer

Runtime environment

Basic software

System & services

Hardware abstraction

I/O abstraction

Complex drivers

Drivers

Microcontroller

User application

AUTOSAR Runtime for Adaptive Applications

Application Programming Interfaces (APIs)

Services for management and diagnosis

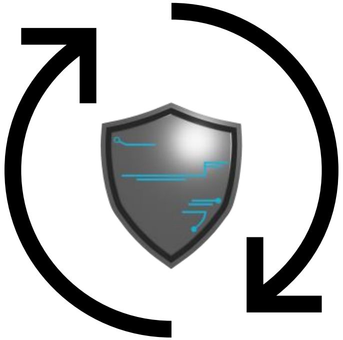
Operating System

Virtual machine / Container / Hardware

High Performance Computing

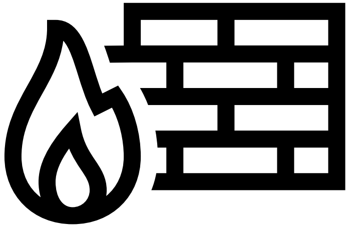
From gateway to zone

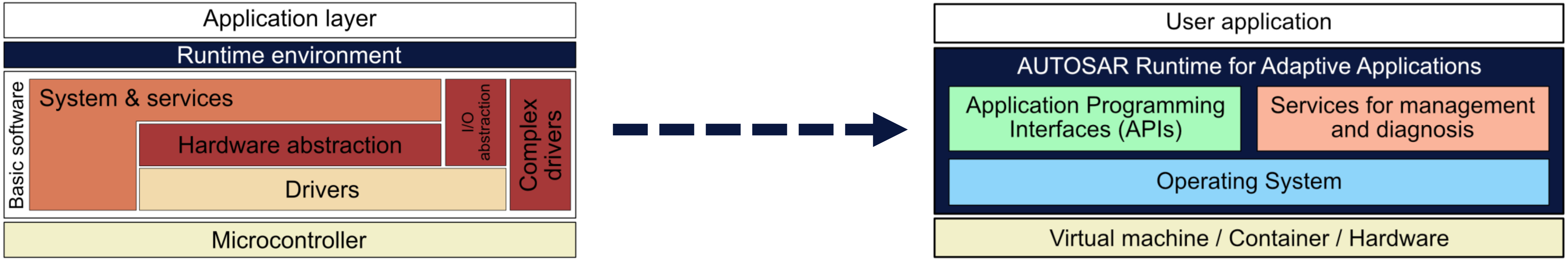
Security updates



Deployment resources

Network segmentation





Application layer

Runtime environment

Basic software

System & services

Hardware abstraction

I/O abstraction

Complex drivers

Drivers

Microcontroller

User application

AUTOSAR Runtime for Adaptive Applications

Application Programming Interfaces (APIs)

Services for management and diagnosis

Operating System

Virtual machine / Container / Hardware

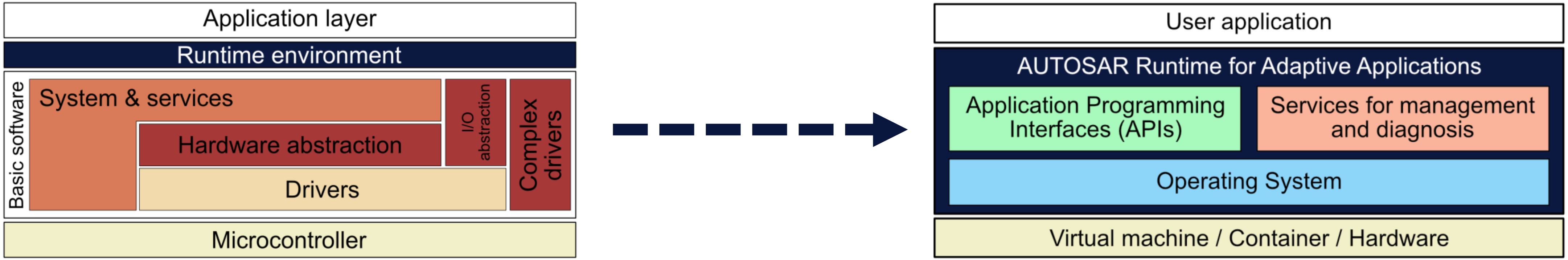
High Performance Computing

From gateway to zone

Security updates

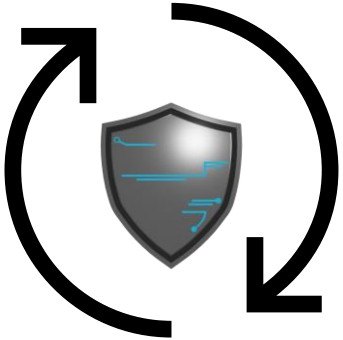
Deployment resources

Network segmentation



High Performance Computing
Remaining limitations

Security updates



Deployment resources

Network segmentation

How many incidents will an in-vehicle honeypot realistically register?

In-Vehicle honeypot as additional layer of intrusion detection.

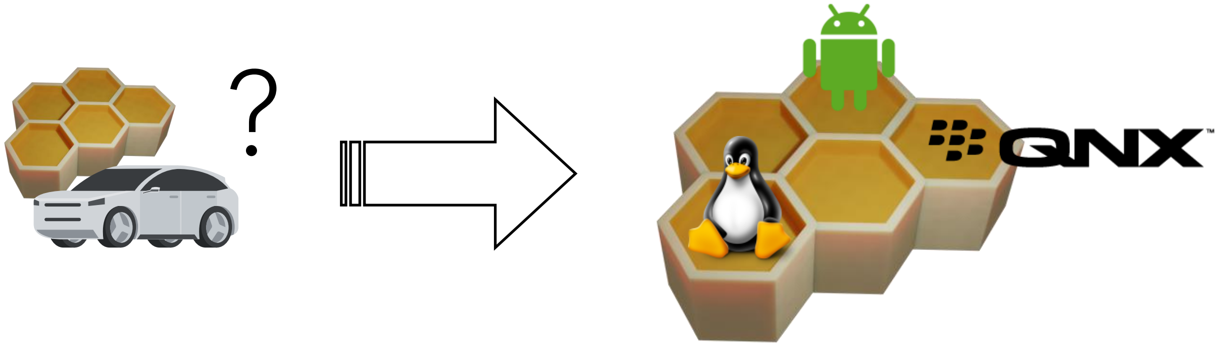
Different solution for threat landscape monitoring.

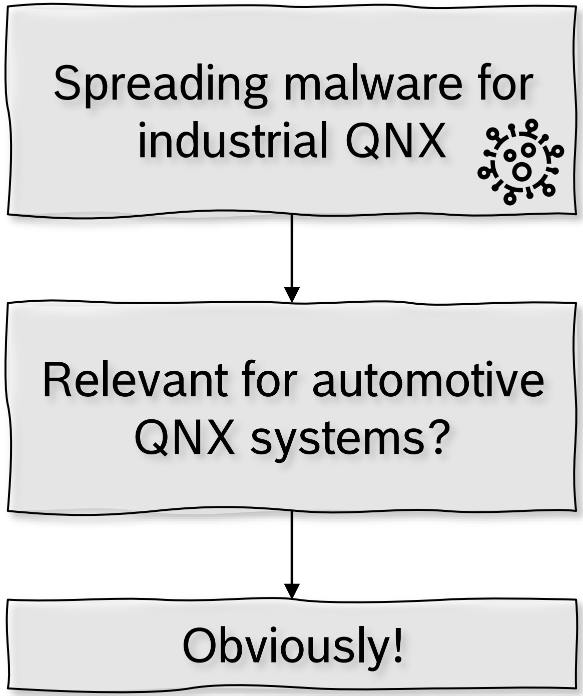
4

Concept for Internet-deployed Honeypots

Threat Landscape Monitoring
Internet deployments with LI Honeypots

- How do we convincingly place an automotive honeypot on the public Internet?




Spreading malware for industrial QNX

Relevant for automotive QNX systems?

Obviously!

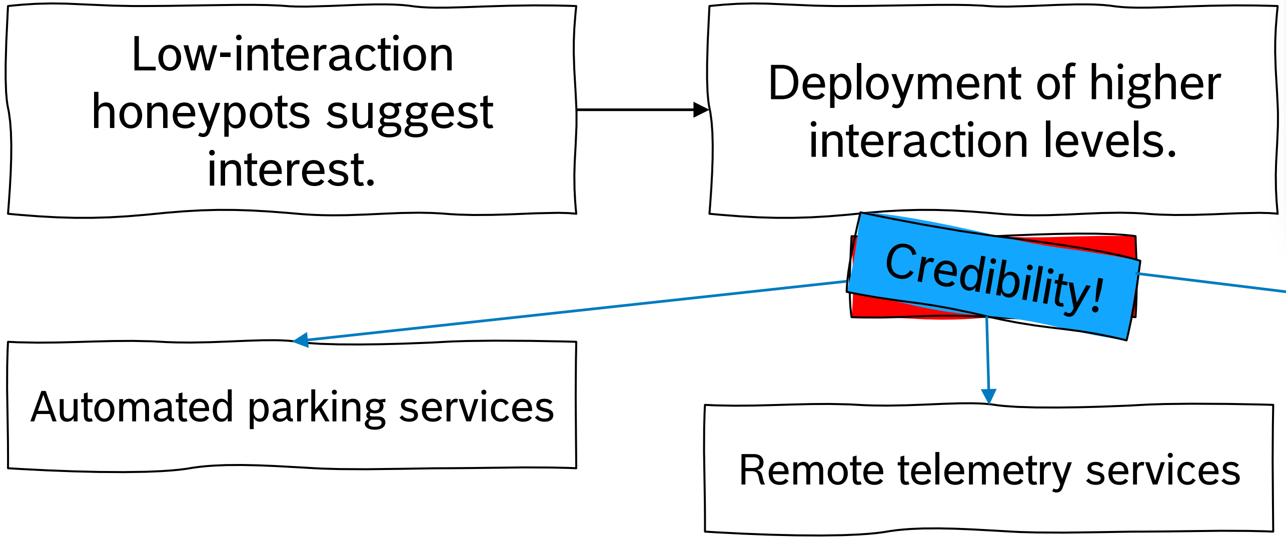
- Instead use low-interaction honeypot
  - Mimic systems and service also found in other domains ((I)IoT, mobile, IT)
  - Monitor general interest in related systems and services
  - Low development and maintenance effort

Threat Landscape Monitoring

Can we catch advanced attackers?

Medium- and high-interaction honeypots are a great tool for additional insights.

- High development and maintenance cost
- Low credibility on the public Internet (hopefully)



Low-interaction honeypots suggest interest.

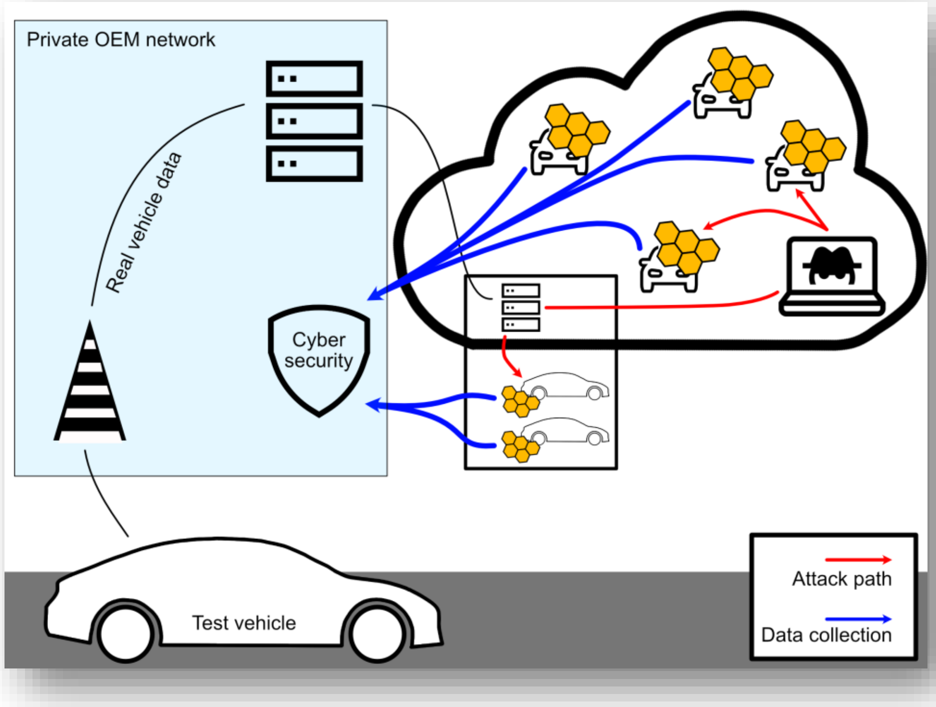
Deployment of higher interaction levels.

Credibility!

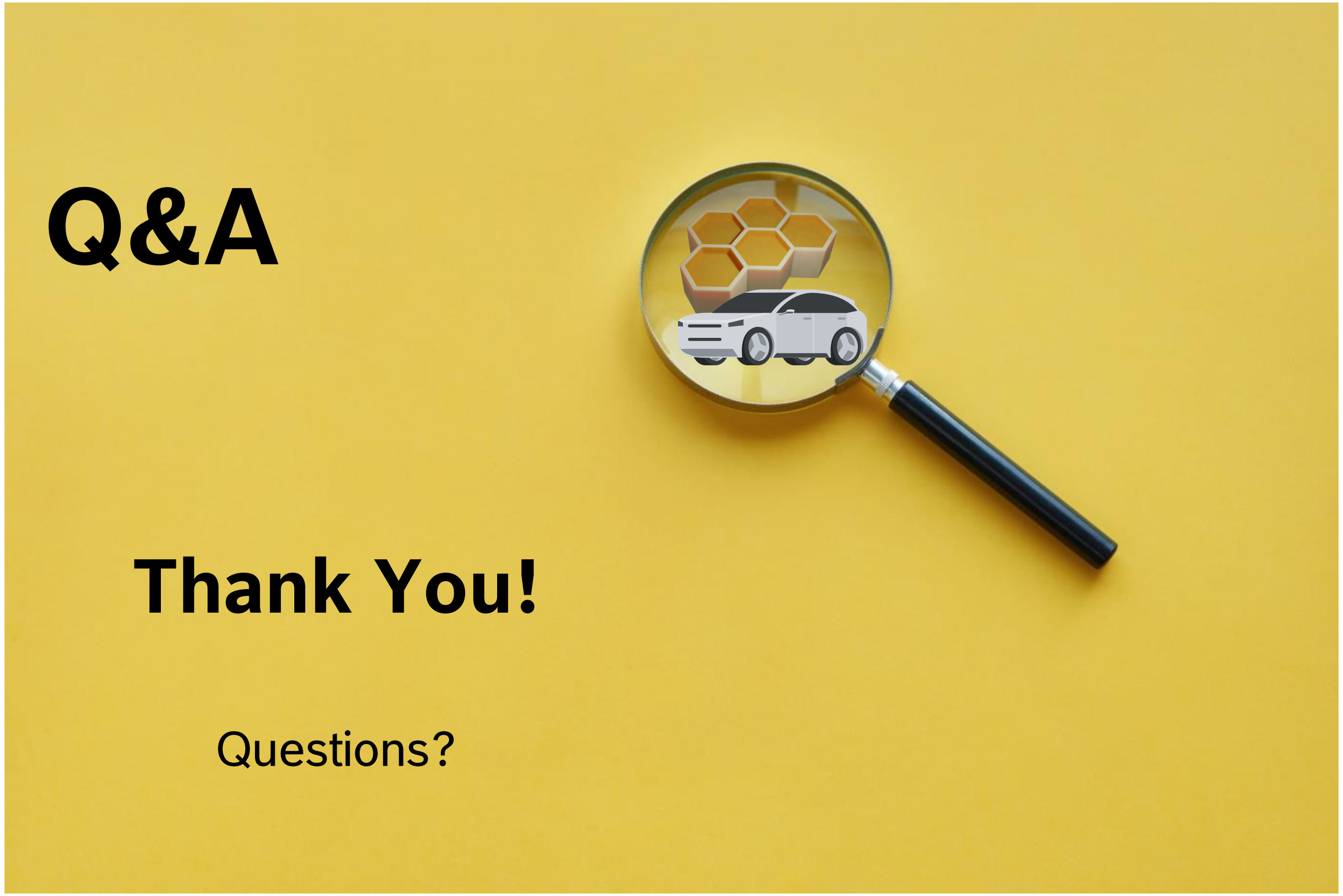
Automated parking services

Remote telemetry services

Test vehicle portals



5



Q&A

Thank You!

Questions?