CREATING SECURITY ZONES FOR SOME/IP

Jan Schäferling, Pramod Shreenarasi

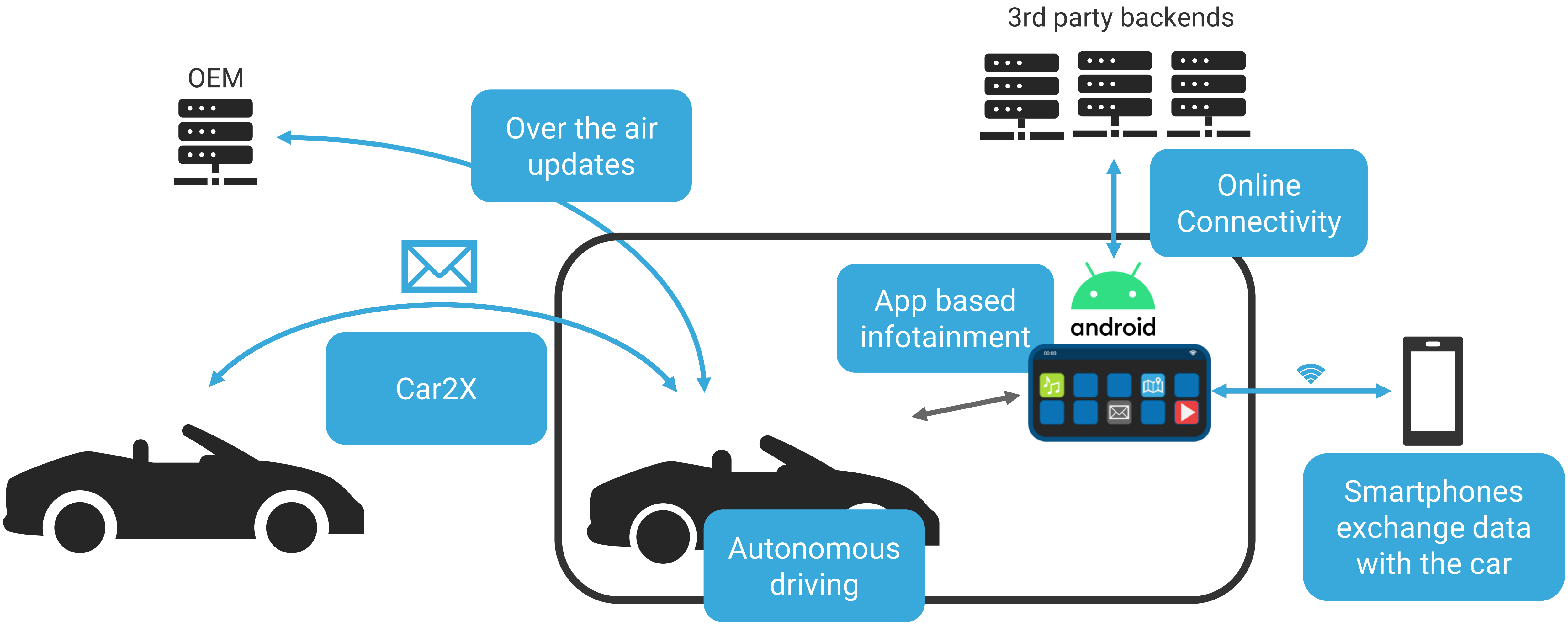
CREATING SECURITY ZONES FOR SOME/IP

TABLE OF CONTENTS

- Introduction
- Definition & Purpose
- Potential Solutions
- Summary

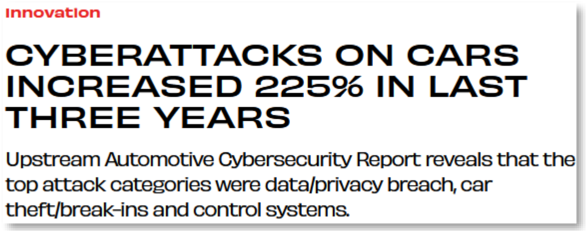
INTERCONNECTIVITY OF MODERN CARS

CONNECTIVITY IS THE MAIN DRIVER OF NEW FEATURES



NEW POSSIBILITIES ADD RISK, TOO

BLACK HAT HACKERS FOCUS INCREASINGLY ON ECUS AND TELEMATICS

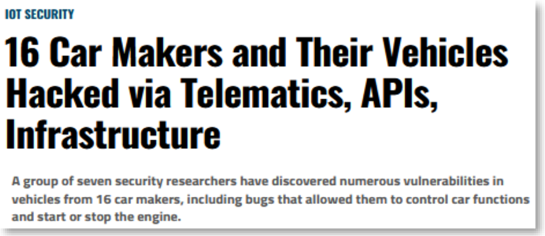


Innovation

CYBERATTACKS ON CARS INCREASED 225% IN LAST THREE YEARS

Upstream Automotive Cybersecurity Report reveals that the top attack categories were data/privacy breach, car theft/break-ins and control systems.

https://www.israel21c.org/cyberattacks-on-cars-increased-225-in-last-three-years/

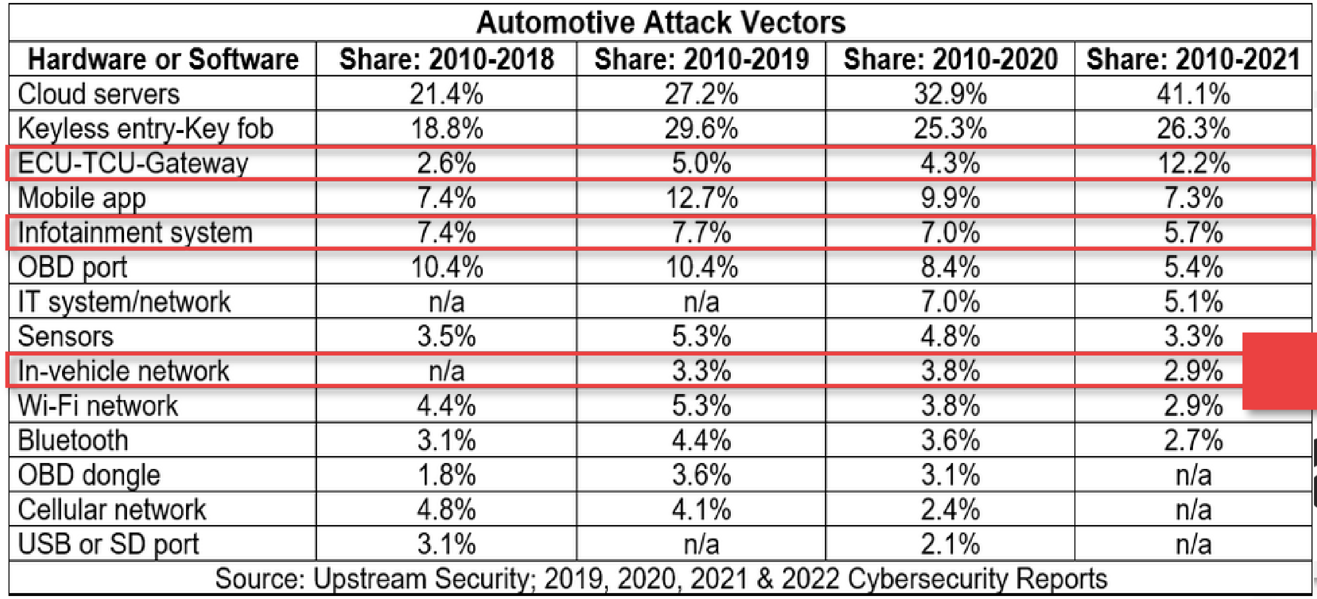


IOT SECURITY

16 Car Makers and Their Vehicles Hacked via Telematics, APIs, Infrastructure

A group of seven security researchers have discovered numerous vulnerabilities in vehicles from 16 car makers, including bugs that allowed them to control car functions and start or stop the engine.

https://www.securityweek.com/16-car-makers-and-their-vehicles-hacked-telematics-apis-infrastructure/

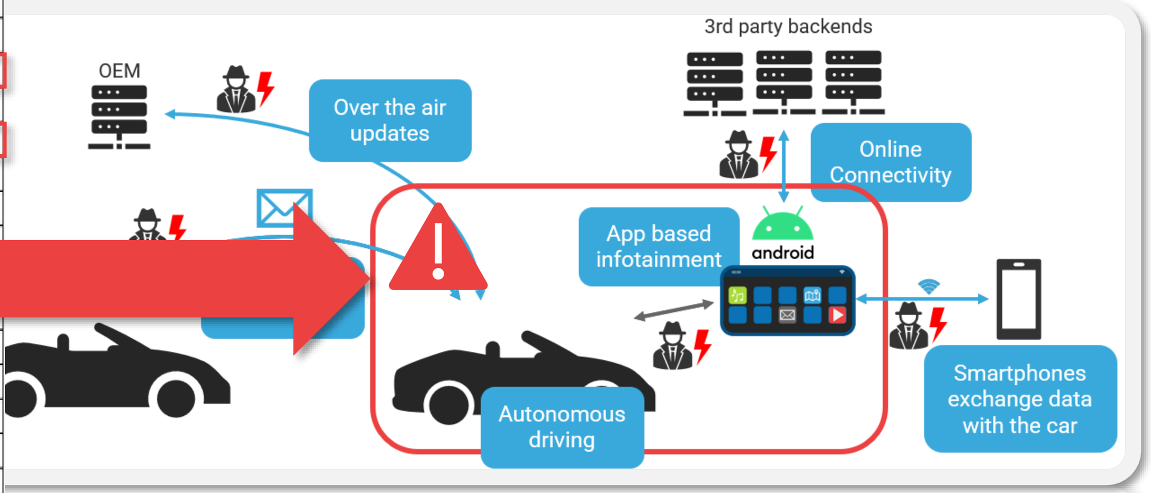


Automotive Attack Vectors

Hardware or Software	Share: 2010-2018	Share: 2010-2019	Share: 2010-2020	Share: 2010-2021
Cloud servers	21.4%	27.2%	32.9%	41.1%
Keyless entry-Key fob	18.8%	29.6%	25.3%	26.3%
ECU-TCU-Gateway	2.6%	5.0%	4.3%	12.2%
Mobile app	7.4%	12.7%	9.9%	7.3%
Infotainment system	7.4%	7.7%	7.0%	5.7%
OBD port	10.4%	10.4%	8.4%	5.4%
IT system/network	n/a	n/a	7.0%	5.1%
Sensors	3.5%	5.3%	4.8%	3.3%
In-vehicle network	n/a	3.3%	3.8%	2.9%
Wi-Fi network	4.4%	5.3%	3.8%	2.9%
Bluetooth	3.1%	4.4%	3.6%	2.7%
OBD dongle	1.8%	3.6%	3.1%	n/a
Cellular network	4.8%	4.1%	2.4%	n/a
USB or SD port	3.1%	n/a	2.1%	n/a

Source: Upstream Security; 2019, 2020, 2021 & 2022 Cybersecurity Reports

https://www.embedded.com/automotive-cyberattacks-grow-more-varied-despite-improving-defenses/



NEW THREATS IN AUTOMOTIVE & EXAMPLES

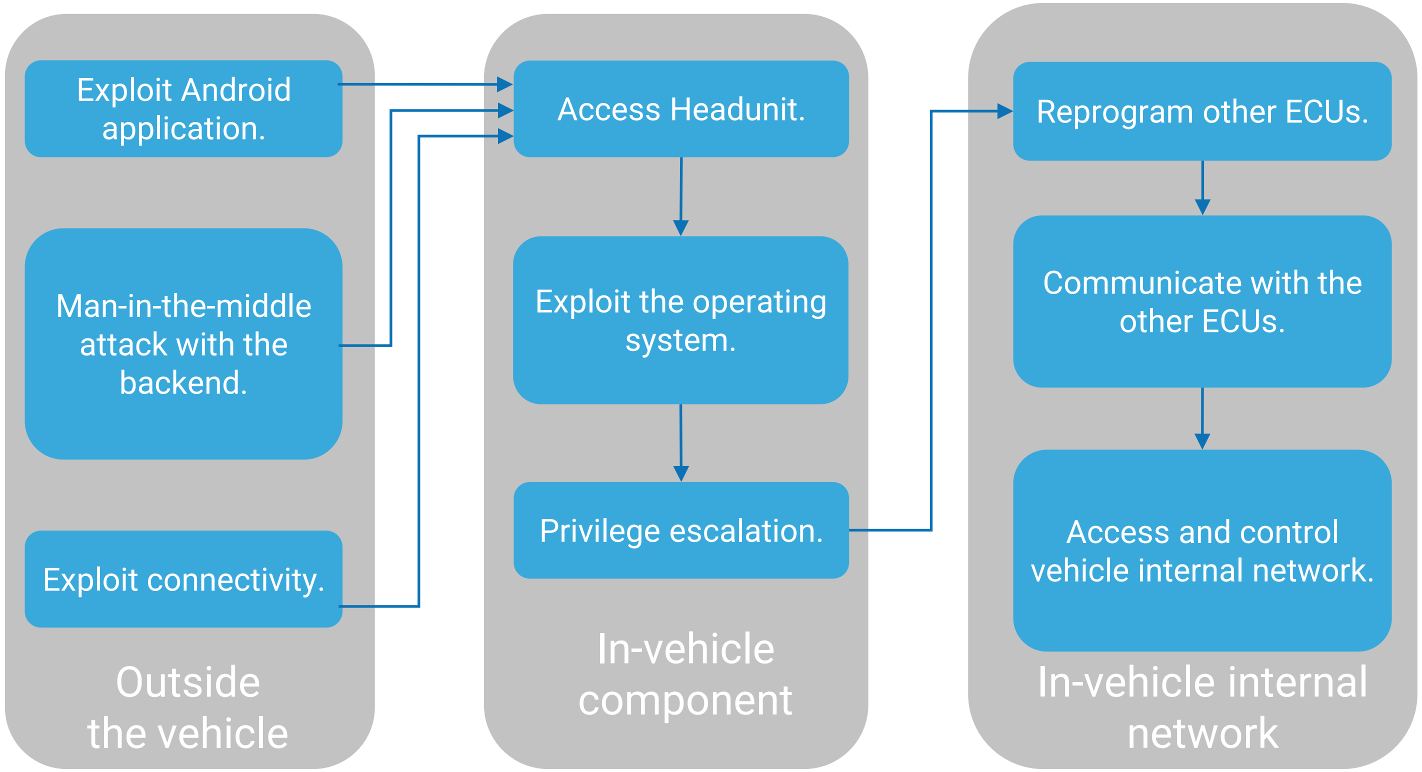
WITH THE NEW USE CASES, NEW THREATS ARE POSSIBLE.

Example Threats:

Headunits / Telematics:

- Exploitable Browser.
- USB weaknesses.
- BT weaknesses!
- WIFI weakness!
- GSM.
- Time-to-check to time-of-use.
- Weaknesses in remote protocols.
- Proprietary Tier-1 protocols.
- Debug protocols, DLT inject, …

Example attack chain.


Exploit Android application.
Man-in-the-middle attack with the backend.
Exploit connectivity.
Outside the vehicle
Access Headunit.
Exploit the operating system.
Privilege escalation.
In-vehicle component
Reprogram other ECUs.
Communicate with the other ECUs.
Access and control vehicle internal network.
In-vehicle internal network

CREATING SECURITY ZONES FOR SOME/IP

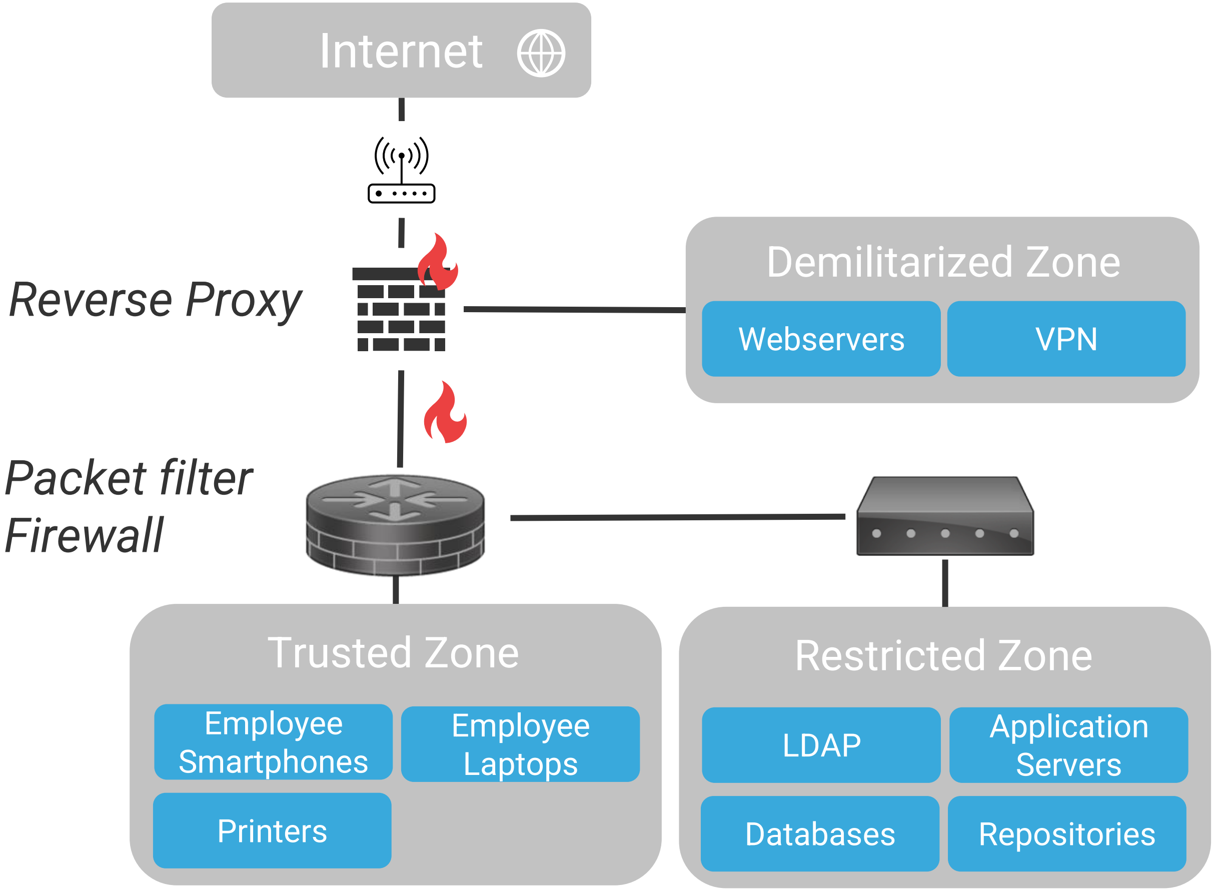
#1 | Definition & Purpose

SECURITY ZONES

ENTERPRISE NETWORKS DEFINE MULTI-LEVEL SECURITY ZONES

“network security technique that divides a network into smaller, distinct sub-networks with limited access to the internal network.”

- Smaller attack surface.
- Better performance.
- Better access control.
- Isolated sub-networks.



Inspired by IT infrastructure

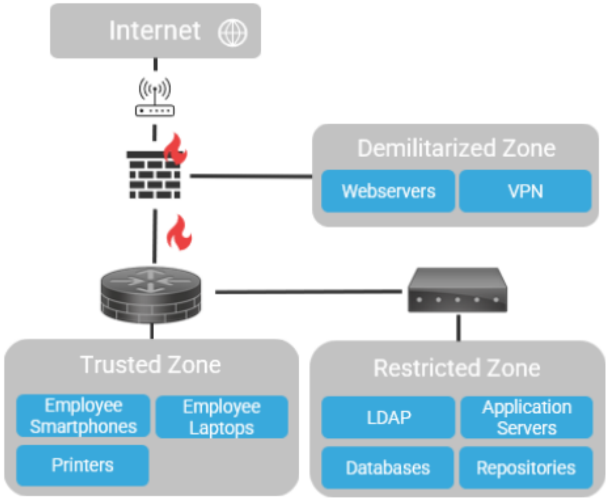
SECURITY ZONES

ZONES CAN BE ESTABLISHED IN AUTOMOTIVE

IT-World

Protocols

- HTTP
- SMTP
- LDAP
- FTP
- ….



Internet

Demilitarized Zone

Webservers

VPN

Trusted Zone

Employee Smartphones

Employee Laptops

Printers

Restricted Zone

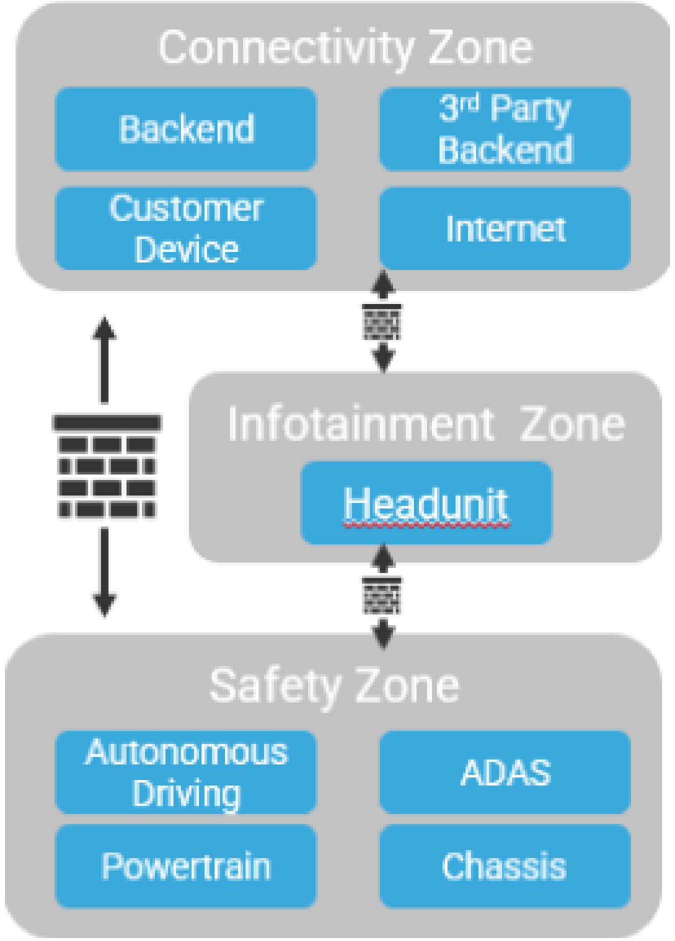
LDAP

Application Servers

Databases

Repositories

Automotive



Connectivity Zone

Backend

3rd Party Backend

Customer Device

Internet

Infotainment Zone

Headunit

Safety Zone

Autonomous Driving

ADAS

Powertrain

Chassis

Protocols

- SOME/IP
- PDU
- …

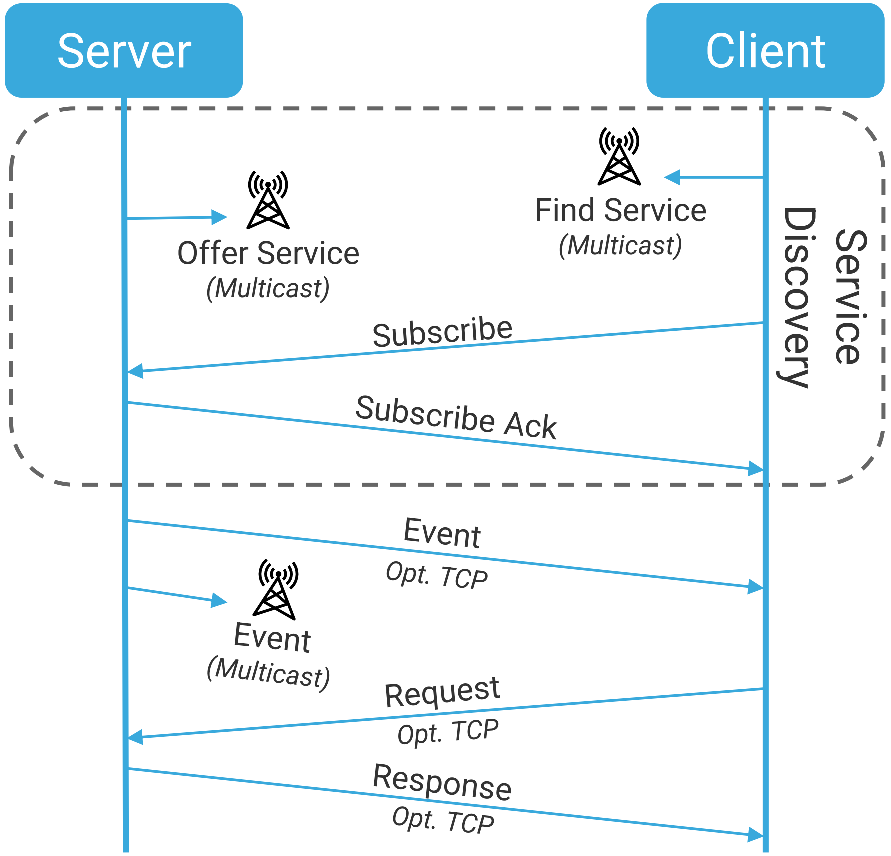
SOME/IP BASICS

Basic Info:

- Scalable service-oriented MiddlewarE over IP (SOME/IP).
- Most used Service-Oriented middleware in automotive

Relevant Characteristics:

- Automatic negotiation of configuration parameters required by TCP/IP stack via service discovery.
- Unicast and multicast communication possible.
- Payload integrity via optional E2E protection.



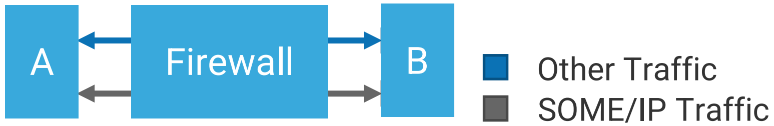
Main communication characteristics of SOME/IP

CREATING SECURITY ZONES FOR SOME/IP

#2| Potential Solutions

STATELESS FIREWALL

Schema

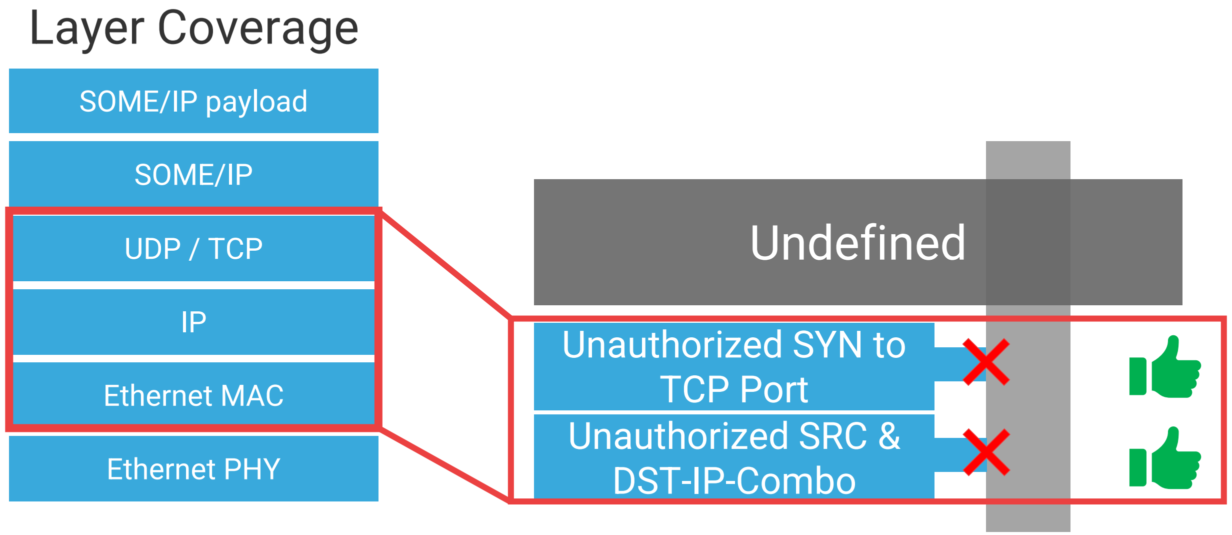


Characteristics

- IP-Packet based.
- Used in IT.
- Hardware or Software.
- Use case: Prevent unauthorized access.
- Built in in most operating systems.
- Typically statically configured in automotive.

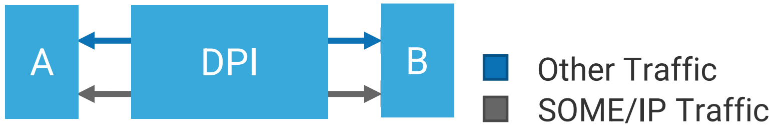
Shall be used as a base for specific security solutions.

Behaviour on exemplary scenarios



DEEP PACKET INSPECTION

Schema



A

DPI

B

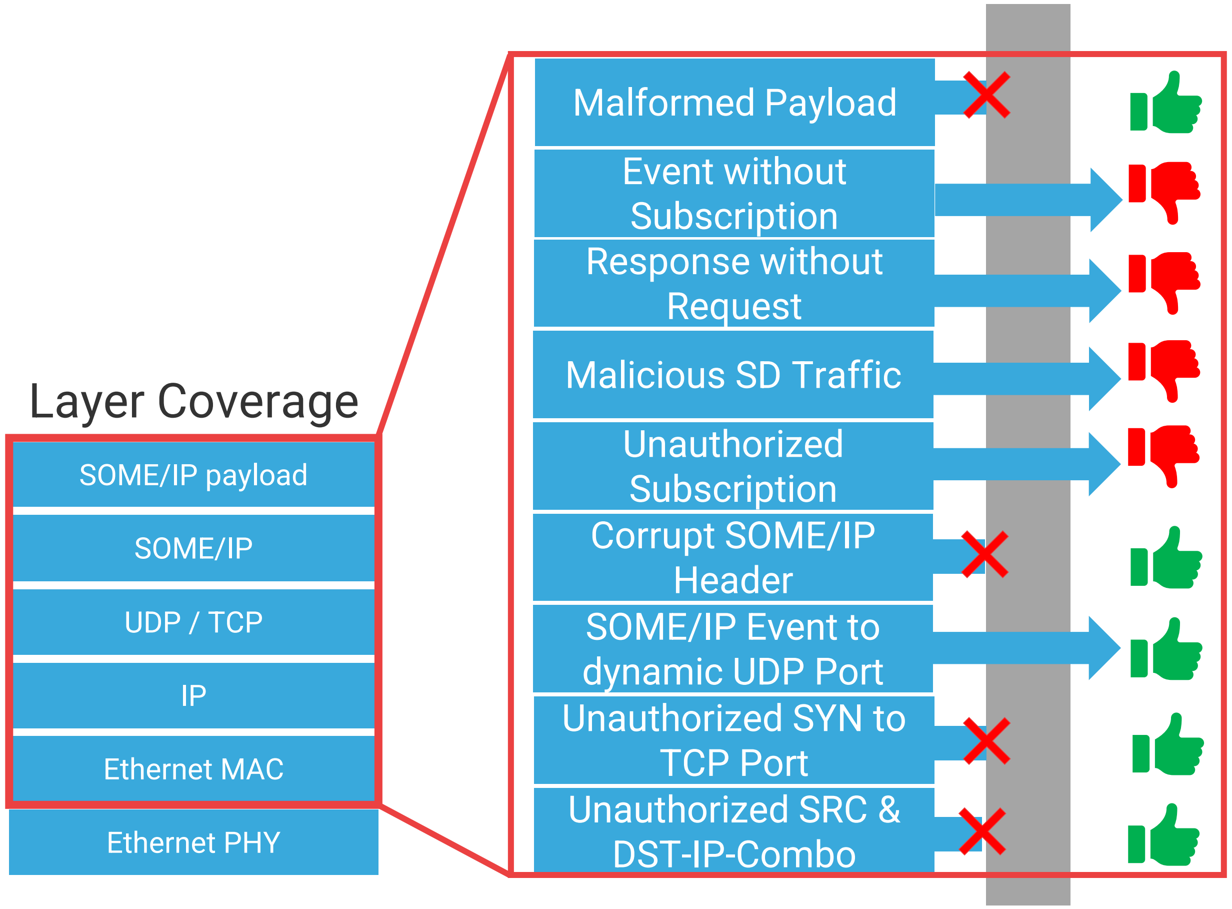
■ Other Traffic

■ SOME/IP Traffic

Characteristics

- Stateful firewall.
- Passive analysis of incoming packets.
- Can inspect packets from all protocols.
- Brings highest General Security.
- Can be partially implemented in HW until L4.

Behaviour on exemplary scenarios



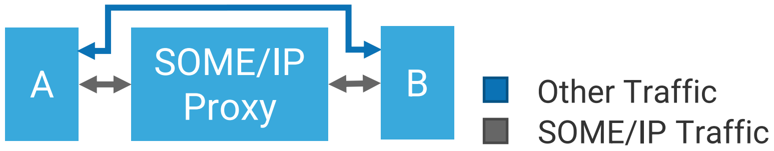
Layer Coverage

- SOME/IP payload
- SOME/IP
- UDP / TCP
- IP
- Ethernet MAC
- Ethernet PHY

Malformed Payload	✗	👍
Event without Subscription	→	👎
Response without Request	→	👎
Malicious SD Traffic	→	👎
Unauthorized Subscription	→	👎
Corrupt SOME/IP Header	✗	👍
SOME/IP Event to dynamic UDP Port	→	👍
Unauthorized SYN to TCP Port	✗	👍
Unauthorized SRC & DST-IP-Combo	✗	👍

SOME/IP PROXY

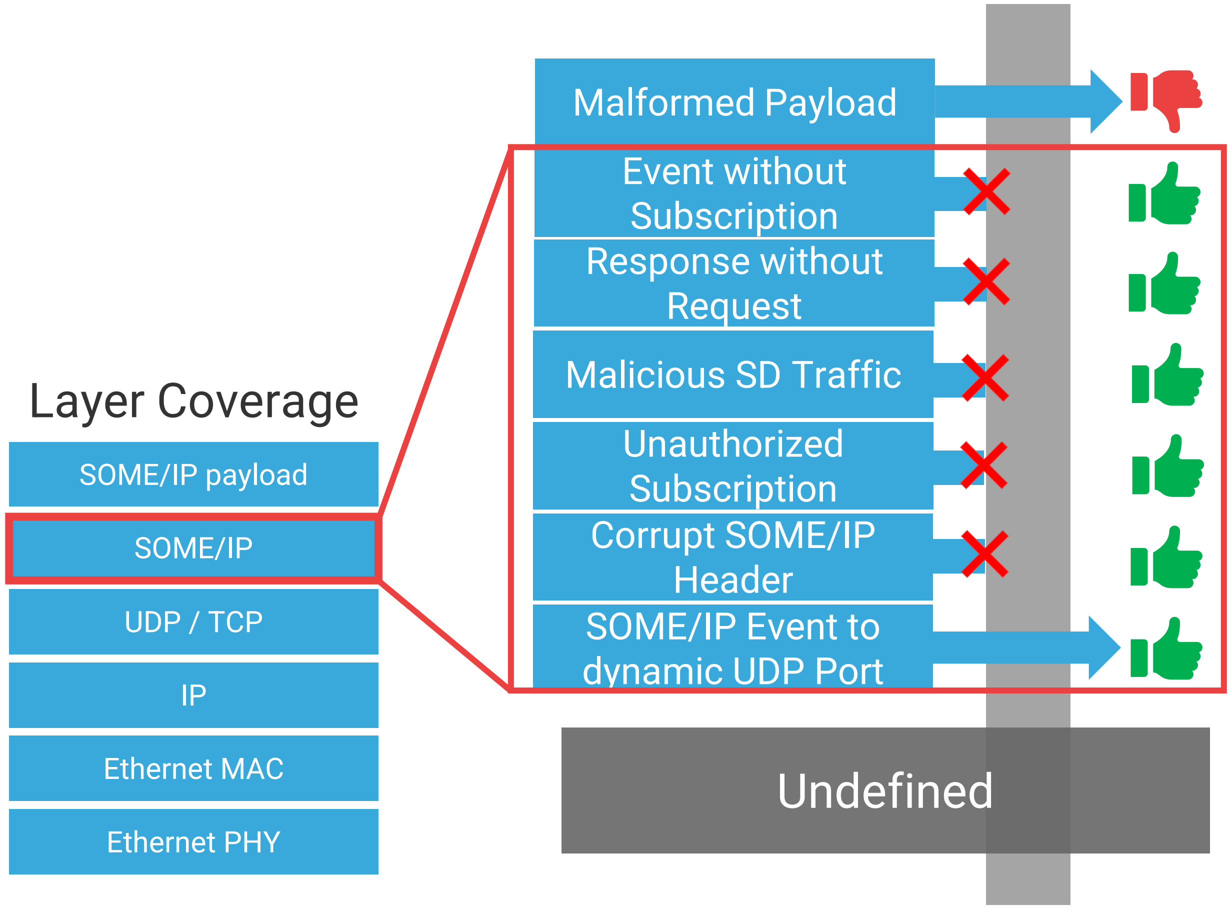
Schema



Characteristics

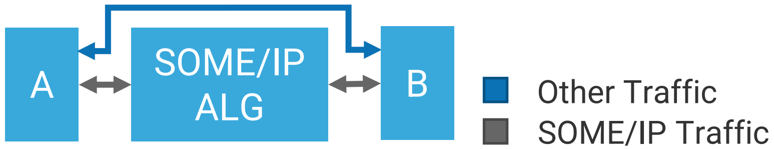
- Interface between security zones.
- SOME/IP (SD)-Packet based.
- Dynamic adaption of scope based on Service Discovery.
- Can only be implemented in Software.
- Keeps SOME/IP header and payload untouched.
- Does not break E2E.
- Scope: Only SOME/IP traffic.

Behaviour on exemplary scenarios


Layer Coverage
SOME/IP payload
SOME/IP
UDP / TCP
IP
Ethernet MAC
Ethernet PHY
Malformed Payload 👎
Event without Subscription ✗ 👍
Response without Request ✗ 👍
Malicious SD Traffic ✗ 👍
Unauthorized Subscription ✗ 👍
Corrupt SOME/IP Header ✗ 👍
SOME/IP Event to dynamic UDP Port 👍
Undefined

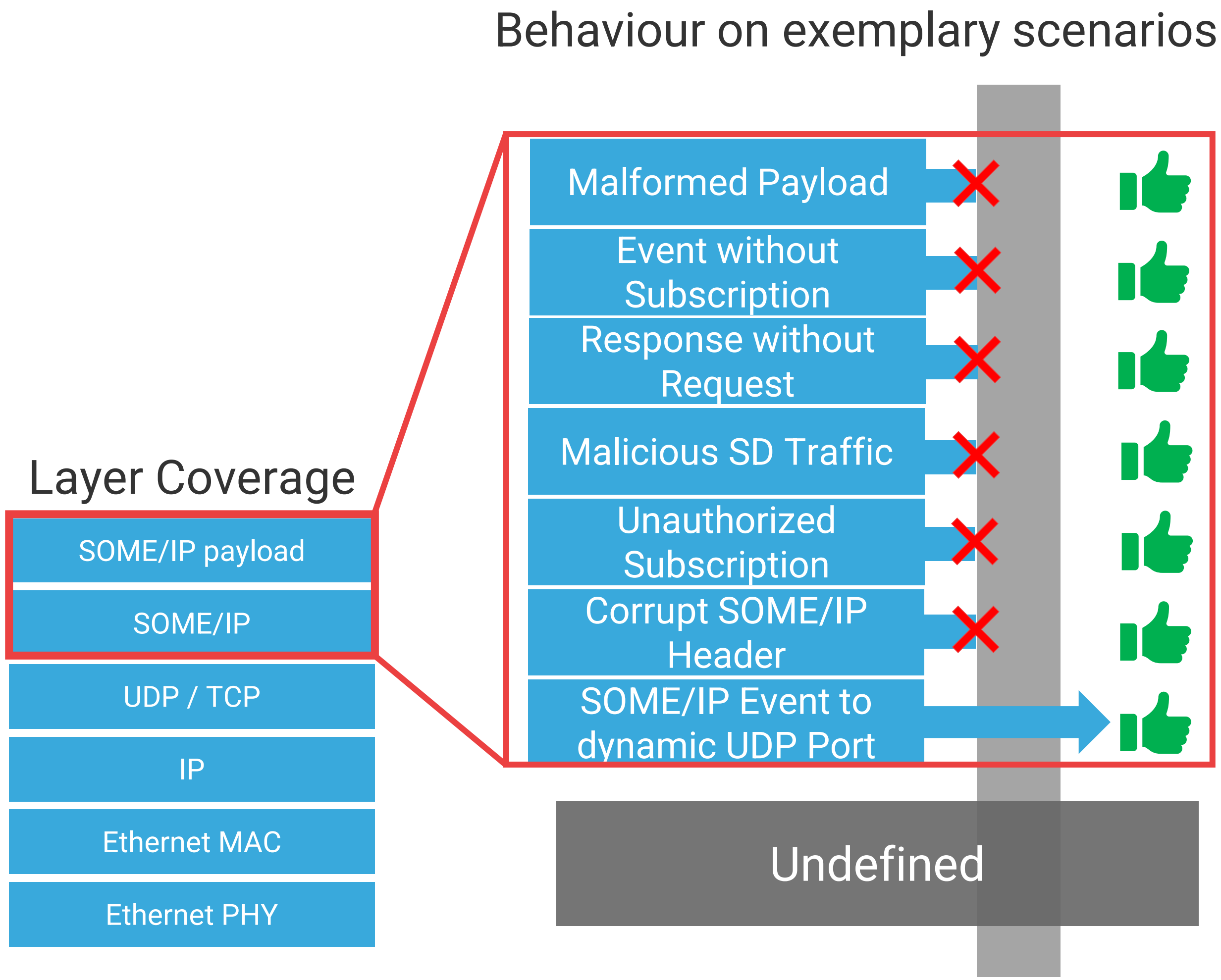
SOME/IP APPLICATION LAYER GATEWAY

Schema



Characteristics

- Supports payload dissection.
- Can inspect/modify messages, including payload.
- Brings highest SOME/IP Security.
- Also brings highest latency…



Behaviour on exemplary scenarios

Layer Coverage

SOME/IP payload
SOME/IP
UDP / TCP
IP
Ethernet MAC
Ethernet PHY

Malformed Payload ✗ 👍
Event without Subscription ✗ 👍
Response without Request ✗ 👍
Malicious SD Traffic ✗ 👍
Unauthorized Subscription ✗ 👍
Corrupt SOME/IP Header ✗ 👍
SOME/IP Event to dynamic UDP Port 👍

Undefined

CREATING SECURITY ZONES FOR SOME/IP

ATTRIBUTES TO CONSIDER WHEN EVALUATING POTENTIAL SOLUTIONS

Effectiveness

SOME/IP (SD)-Header-Support
The solution shall be able to dissect SOME/IP (SD)-traffic.

Statefullness
High level Use-Cases require the solution to keep track of the communication.

Protocol coverage
It can be beneficial, if the solution can inspect lower levels of communication.

SOME/IP-Payload-Support
Helps preventing injection of corrupt messages

Dynamic configuration / adaption (SW-Def. Vehicle)
The core idea of SOME/IP is to not predefine the communication parameters but to negotiate them during runtime

Efficiency

Performance *(better, if high)*
The solution shall be able to handle as many

Resource-Utilization *(better, if low)*
The solution shall be ressource-saving regarding CPU, memory and IO.

Reusability *(better, if high)*
A solution should be preferred over a similar one, when it provides additional, beneficial features (e.g., support for other protocols in use)

Complexity *(better, if low)*
If an existing solution can be used directly or slightly modified, it shall be preferred to creating a new solution.

Safety
Startup Performance
E2E Protection

CREATING SECURITY ZONES FOR SOME/IP

EVALUATION-RESULTS OF POTENTIAL SOLUTIONS

	Firewall	DPI	Proxy	ALG
Layer coverage	2-4	2-7 (payload)	2-7 (no payload)	2-7 (payload)
Data analysis	passive	passive	active	active
Implementation Method	HW / SW	HW / SW / Both	SW	SW
Effectiveness	+	++	+++	++++
Efficiency	++++	+++	+++	+
Show stopper				🚫 Breaks E2E Harms startup

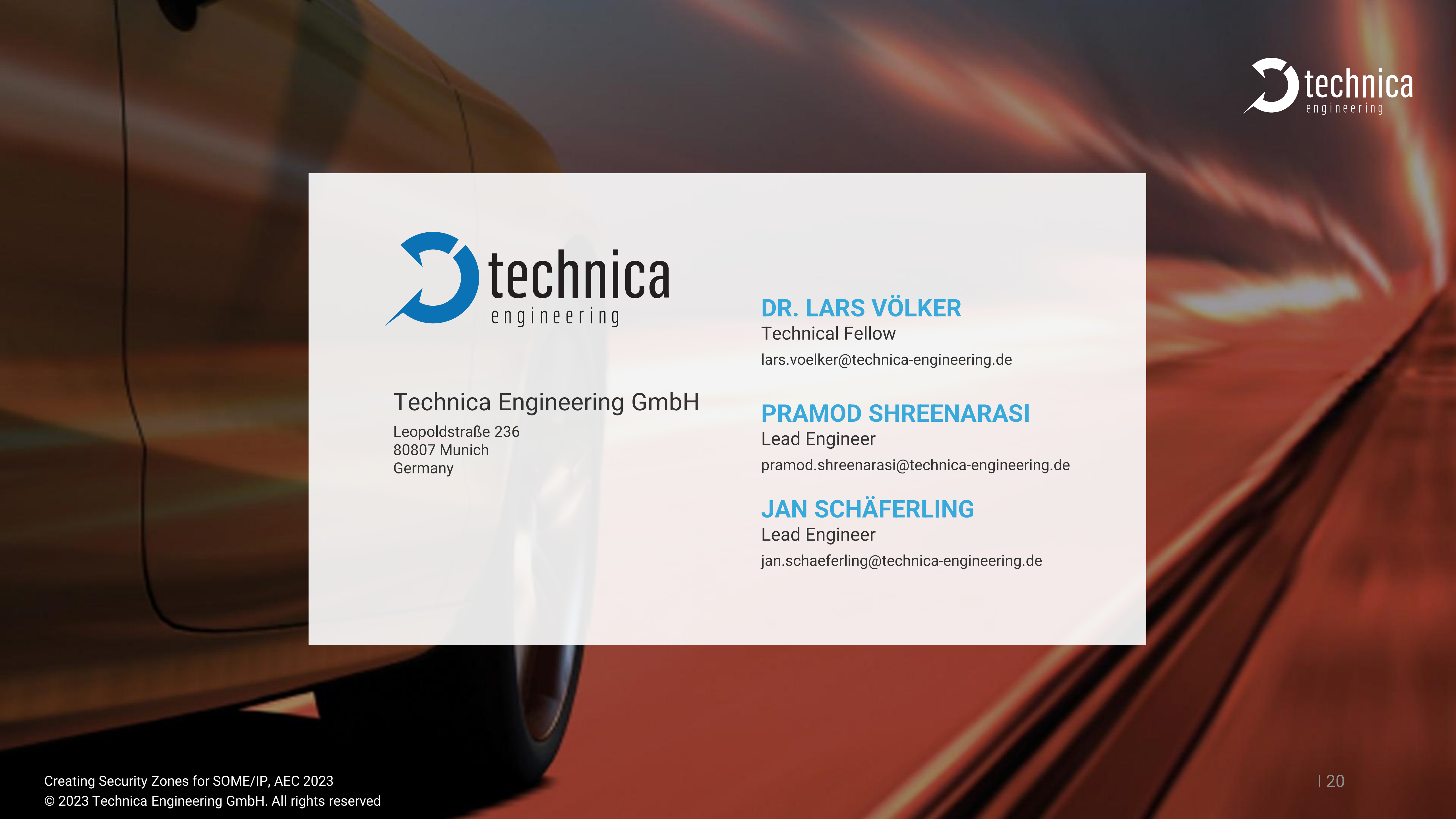
CREATING SECURITY ZONES FOR SOME/IP

#3 | SUMMARY

SUMMARY

WHAT TO LOOK OUT FOR?

- Protection against external attacks are very important.
- Security zones can prevent the attacker from accessing the vehicle internal network.
- Use the concept “Defence in depth” to separate the Security zones using Firewall and a SOME/IP-Proxy.
- Everything else is overload and might even harm safety.



Technica Engineering GmbH

Leopoldstraße 236
80807 Munich
Germany

DR. LARS VÖLKER
Technical Fellow
lars.voelker@technica-engineering.de

PRAMOD SHREENARASI
Lead Engineer
pramod.shreenarasi@technica-engineering.de

JAN SCHÄFERLING
Lead Engineer
jan.schaeferling@technica-engineering.de