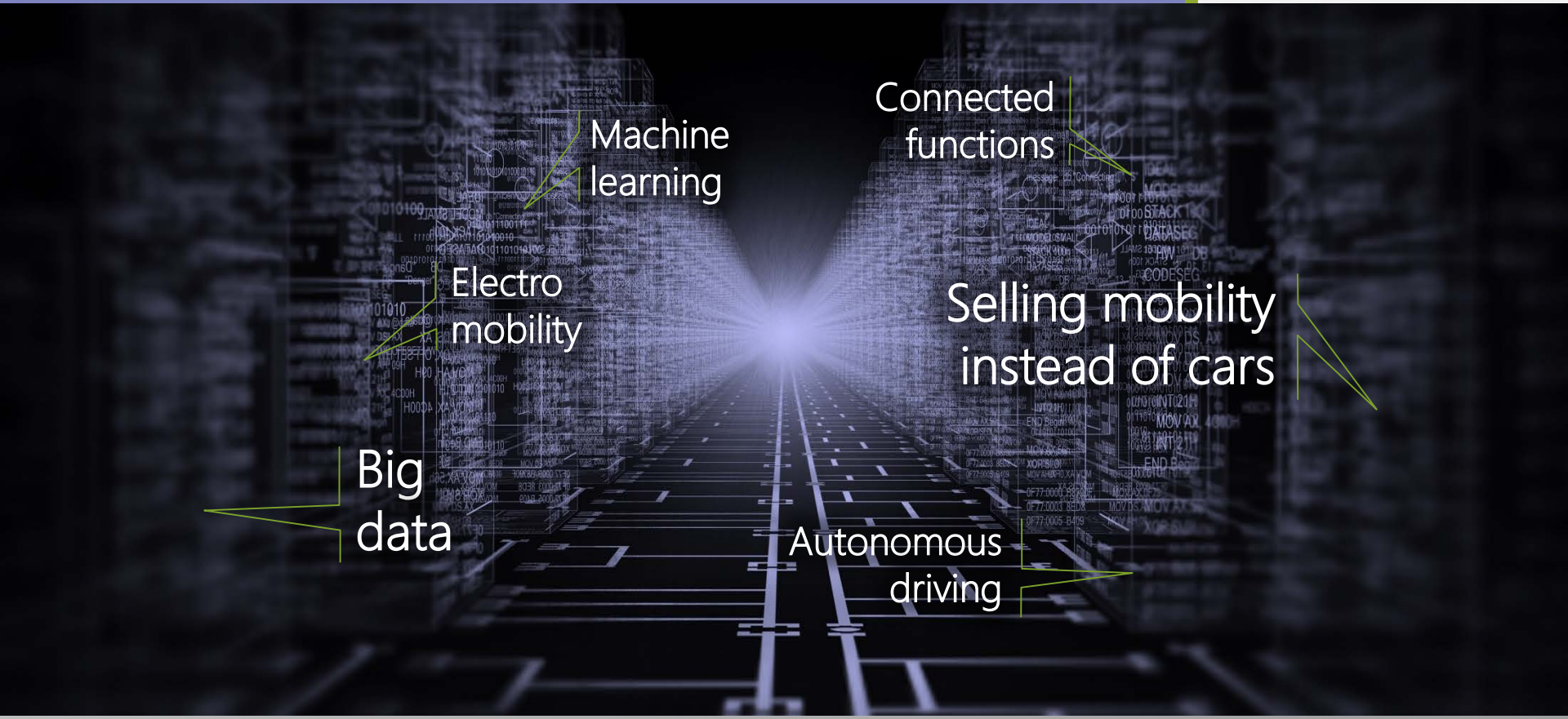
escrypt
SECURITY. TRUST. SUCCESS.

Real life experience from implementation of Firewall, Router and IDS Ethernet switch and uC

Siddharth Shukla, Jan Holle

IEEE-SA Ethernet & IP @ Automotive Technology Day, Detroit USA, 25.09.2019

escrypt
SECURITY. TRUST. SUCCESS.



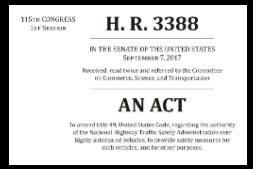
escrypt
SECURITY. TRUST. SUCCESS.

Recent remote attack examples

- 2019 – Tesla Model 3, JIT (Just In Time)
- 2018 – Volkswagen (Infotainment), BMW
- 2017 – Tesla Model X, HMC (Bluelink)
- 2016 – Tesla Model S, Mitsubishi Outlander
- 2016 – Key relay attack on 19 OEM, 24 Cars
- 2015 – Jeep Cherokee

Consequences

- Economic and reputation damage
  - First security-related recall campaign on 23th July 2015, 1.4 Mio potentially affected vehicles
- Mendatory legal requirements


115TH CONGRESS
1ST SESSION

H. R. 3388

IN THE SENATE OF THE UNITED STATES
SEPTEMBER 7, 2017

Received; read twice and referred to the Committee on Commerce, Science, and Transportation

AN ACT

To amend title 49, United States Code, regarding the authority of the National Highway Traffic Safety Administration over highly automated vehicles, to provide safety measures for such vehicles, and for other purposes.


Over a dozen vulnerabilities uncovered in BMW vehicles

There Will Be Glitches: Extracting and Analyzing Automotive Firmware Efficiently

Part 573 Safety Recall Report

Manufacturer Name:
Submission Date: JUL 23, 2015
NHTSA Recall No.: 15V-461
Manufacturer Recall No.: R40

114TH CONGRESS
1ST SESSION

S.1806

To protect consumers from security and privacy threats to their motor vehicles, and for other purposes.


Securing Self-Driving Cars (one company at a time)

Dr. Charlie Miller (charlie.miller@getcruise.com)

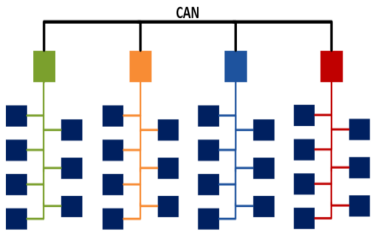
Chris Valasek (chris.valasek@getcruise.com)

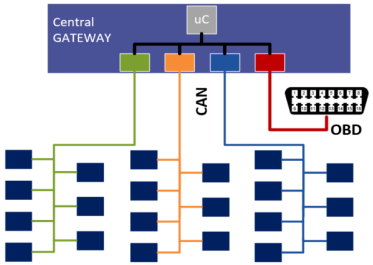
August 2018

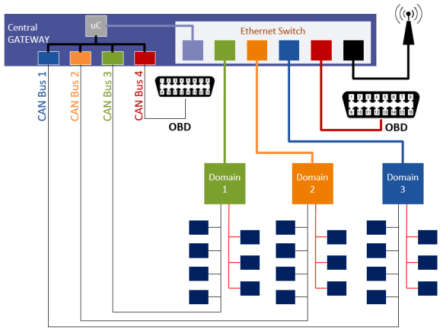
"As much as possible, we use network segregation…"

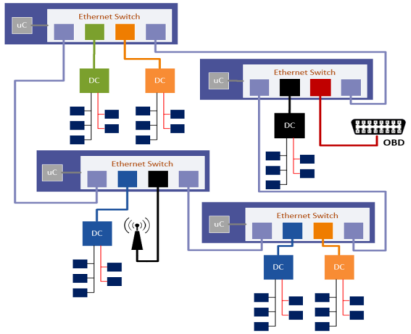
"More importantly, there needs to be real time detection and reaction on vehicle"

escrypt
SECURITY. TRUST. SUCCESS.









Yesterday

- Many small ECU's performing a specific function
- Signal based communication

Today

- Use of a central Gateway for cross-domain communication
- Security introduction with CAN firewall and SecOC etc.

Tomorrow

- E/E Architecture with support of security features
- Application of service oriented communication and high performance ECUs
- Still cyclic messages being used

Future

- Using ring based network to achieve redundancy
- Introduction of vehicle computers (using security enhanced high performance microprocessors)

escrypt
SECURITY. TRUST. SUCCESS.

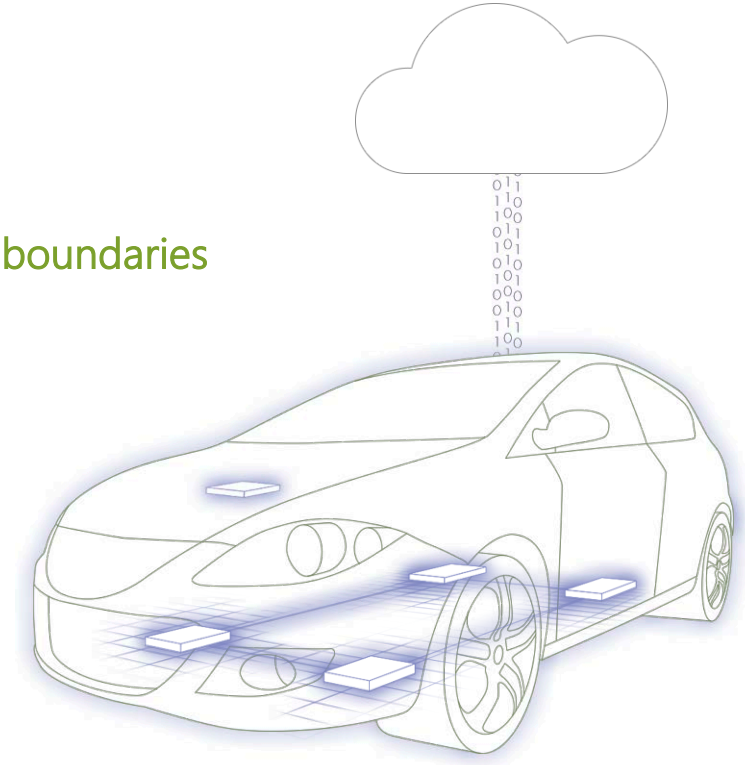
Often, implicitly assumed attack

Secure connected vehicle
- Secure Channel (TLS/IPSec),
- Secure Endpoint Authentication
- Firewall

Secure E/E architecture – establish trust boundaries
- Use separation and securely configured gateways to protect functional domains of E/E architecture

Secure in-vehicle communication
- Protect integrity of critical in-vehicle signals
- SecOC standardized in AUTOSAR

Secure individual ECU
- Hardware security module
- Protect integrity of ECU software and data
- Secure Diagnostic/Flashing/Boot



Spoiler: A good defense in depth concept is more than the number of barriers/layers to stop an remote attacker

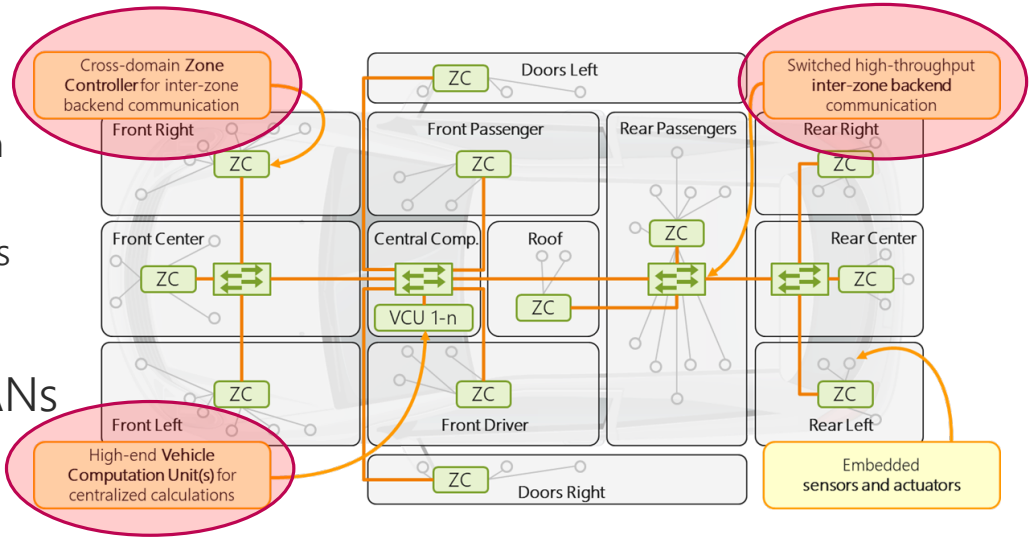
escrypt
SECURITY. TRUST. SUCCESS.

Infrastructure of Next Gen. EE-Architectures will be shared

Mixed (domain/criticality/trustworthiness/…) applications on zone and vehicle computers and also mixed traffic on backbone and trunk communication links

Selected security challenges

- Zone separation
  - **Domain based** separation or
  - **Trusted/Not-trusted model** based separation
- Virtualization to isolate applications
  - Access control to sensitive (shared) resources
  - Side-Channel attacks on sensitive data, e.g., on caches to extract cryptographic keys
- Isolation of Communication, e.g. VLANs
  - Mixed trustworthiness of network nodes
  - Central and local enforcement of communication policy and access control



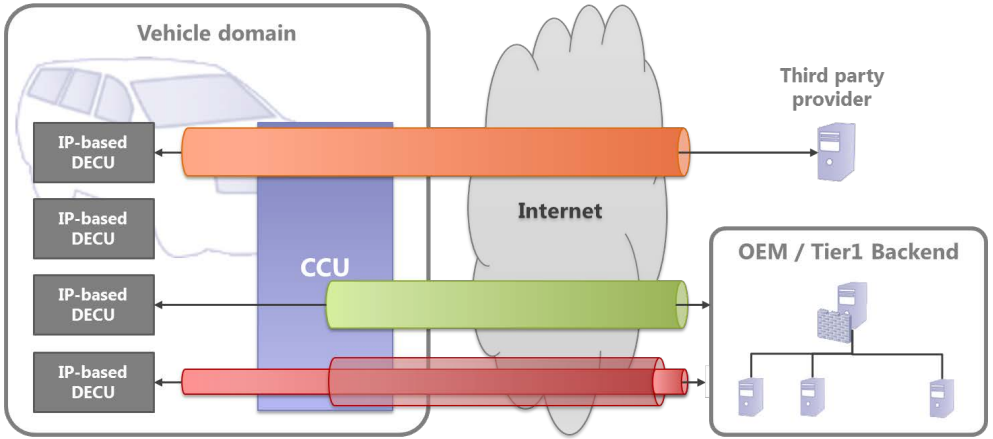
info@escrypt.com

escrypt
SECURITY. TRUST. SUCCESS.

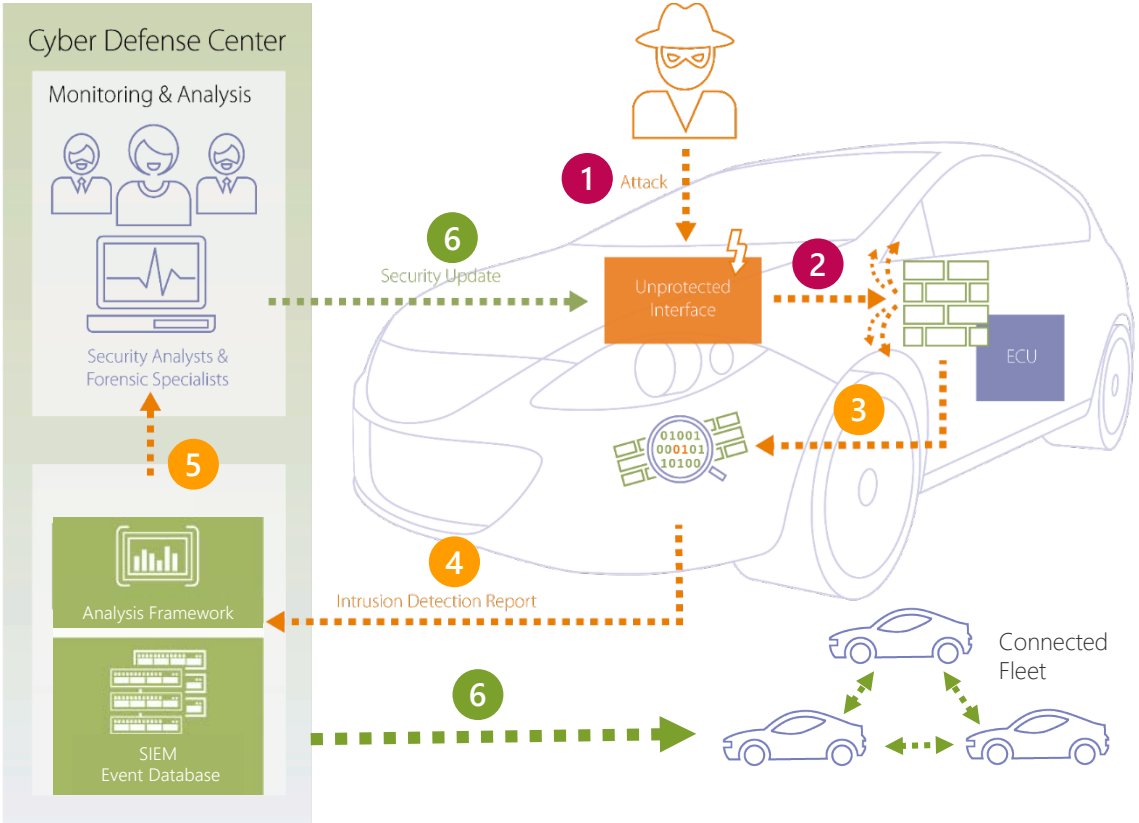
Ambiguous border – Where is the (secured) in-vehicle domain?

The former, natural separation (caused by the application of different network technologies within and beyond the car) will be less strict in nG EE-Architectures. While separation is still a meaningful and recommended concept, implementation becomes very challenging for upcoming use-cases.

- End2End protection vs. Filtering/IDS
  - Many novel use-cases require end2end protected communication (e.g., privacy or IP)
  - Firewalls and IDS may not be able to inspect
  - An exploit of a potential vulnerability become effective deeply inside the EE-Architecture
- Local interfaces (e.g., Bluetooth, WiFi)
  - Are another (while known) attack avenue



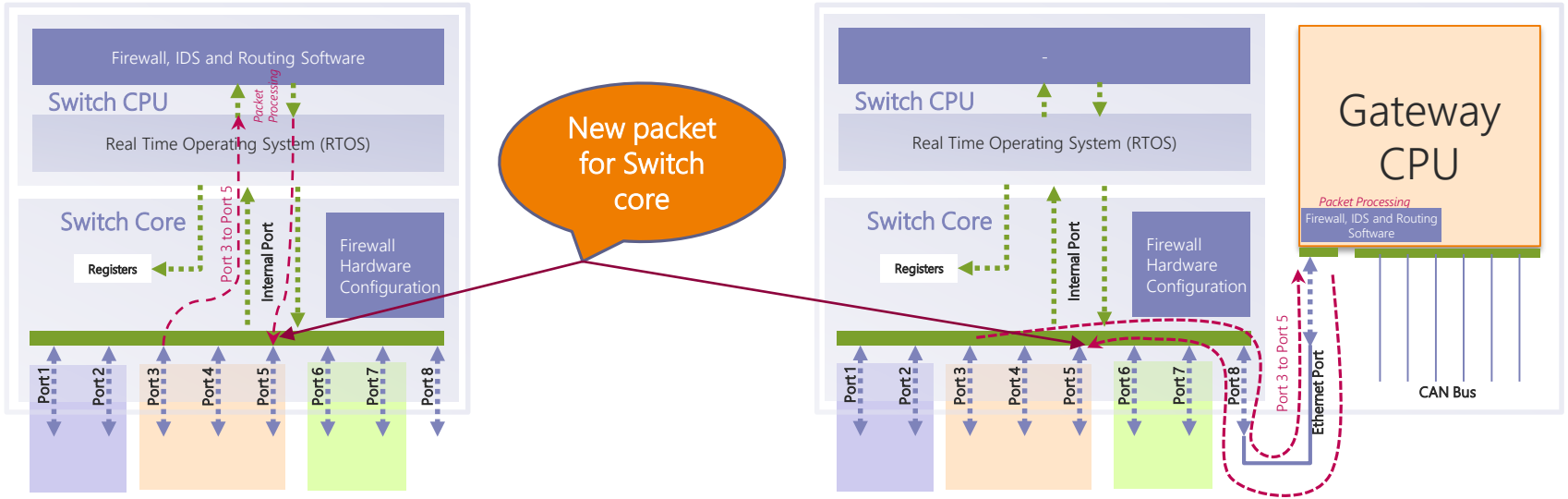
escrypt
SECURITY. TRUST. SUCCESS.



1. **Attack:** Misuse of 0-day exploit in web browser
2. **Security is not absolute:** The OEM's secure flashing implementation was vulnerable and the attacker was able to flash and run arbitrary code, e.g., in order to send malicious signals.
3. **Firewall:** The filtering mechanisms blocks illegitimate signals, e.g, from an invalid source, and informs the IDS. The attacker is not able to control other ECUs.
4. **Intrusion Detection:** The in-vehicle IDPS solution detects the anomaly (i.e., potential attack) on the in-vehicle network, it creates and sends an Intrusion Detection Report
5. **Monitoring & Analysis:** The IDPS backend collects all anomaly reports from the vehicle fleet and enables security analysts and forensic specialist to analyze the attack and identify the vulnerability
6. **Intrusion Prevention:** A security update to remedy the vulnerability will be deployed to the entire vehicle fleet

Real Life experience : Challenges/Solution

Switch thinks it's a new packet!



- Switch handles this processed packet as new packet
- Floods to all vlan members

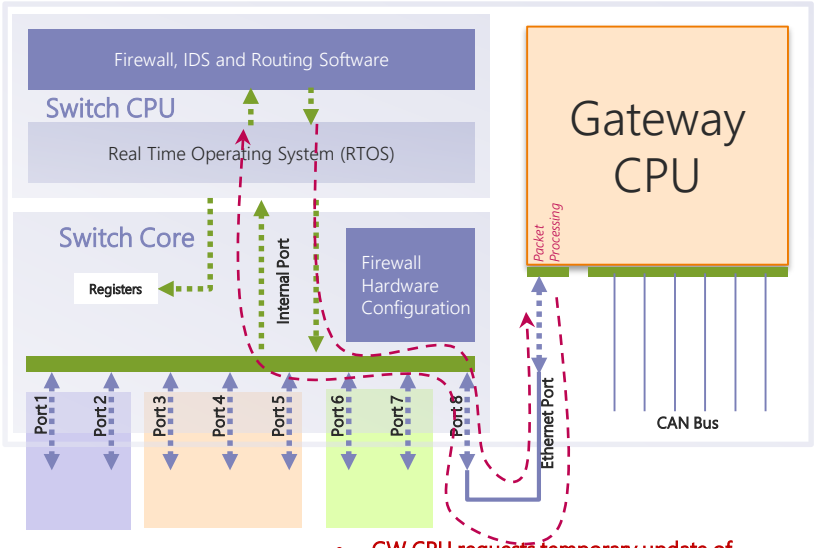
escrypt
SECURITY. TRUST. SUCCESS.

Secure/Safe update of policy during runtime

- Host uC requests Firewall policy update during runtime e.g. activate a rule during diagnostic session
- Policy needs to be linked to one or multiple vehicle states
- Is the message requesting policy update authentic and integrity protected?

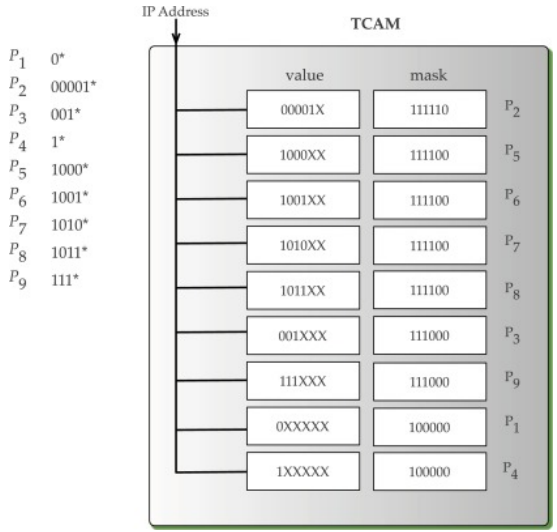
New requirements?

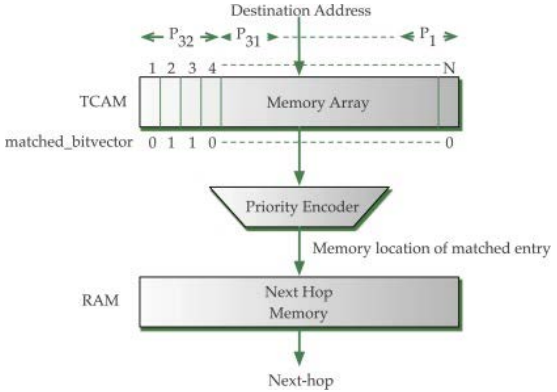
- HSM inside switch
- Encryption/Decryption module in Switch hardware or CPU



escrypt
SECURITY. TRUST. SUCCESS.

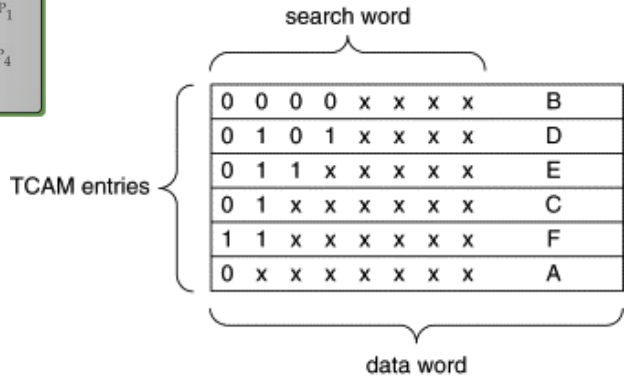
- TCAM is just a memory
- A whitelist/blacklist entry can match multiple TCAM rules but it will hit the first rule from top
- More complexity when TCAM hardware rules are linked to firewall software
- Unexpected network behavior if the TCAM policy is updated dynamically during runtime





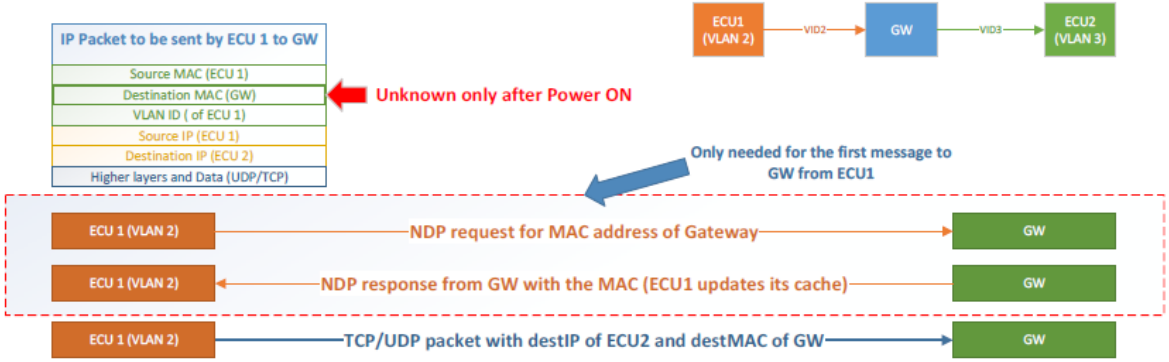
Best practice

- Sorting of data before configuration
- Automatic rule generation
- Sanity check of configuration if rules updated dynamically



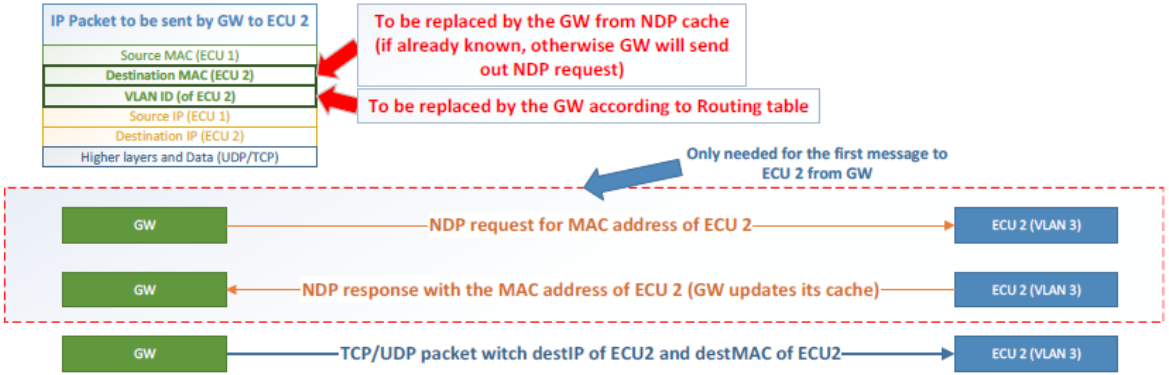
escrypt
SECURITY. TRUST. SUCCESS.

- End to End NDP request is not allowed by ECU's
- MAC address translation for every message adds latency



Solution

- Hardware assisted translation
- Add security to allow end to end NDP

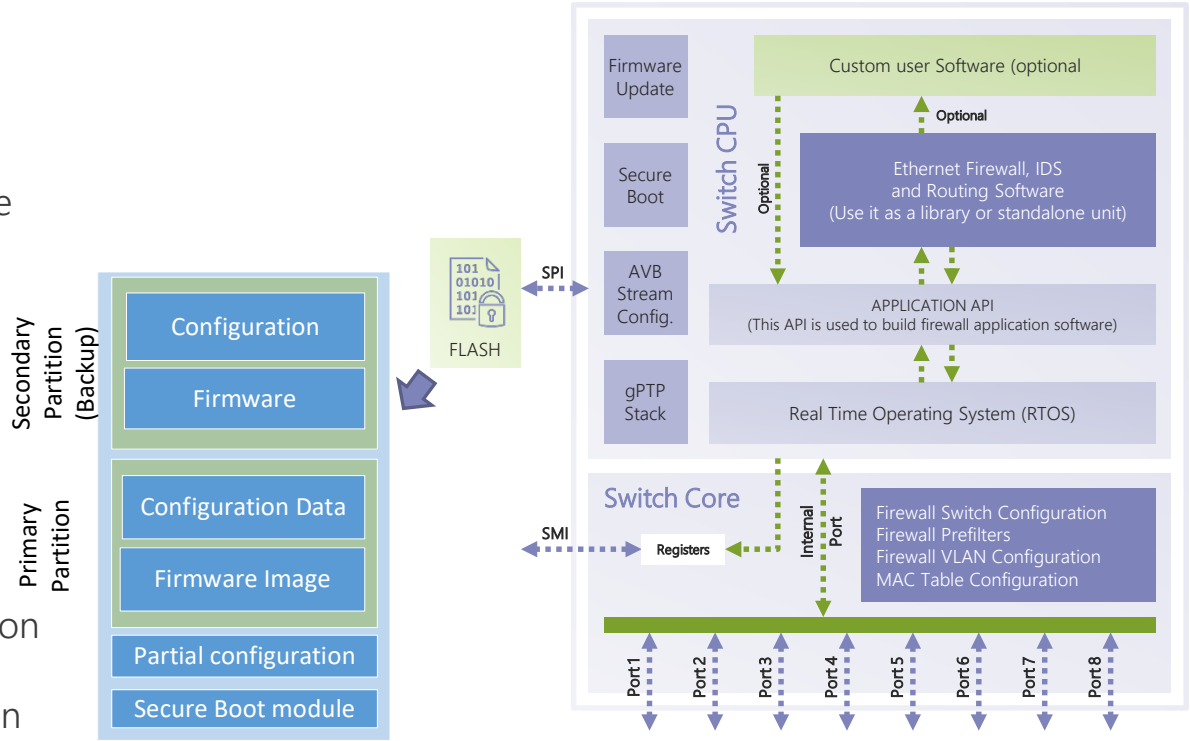


* NDP:Neighbour Discovery Protocol

- Switch needs to store secure configuration
- Boot over SPIO flash could be slow
- Boot over Ethernet requires the host CPU to boot first
- Challenging start-up time requirements

Possible solutions

- Secure boot
- Encrypted boot
- Secure key storage
- Hardware encryption/decryption engine
- Loading of partial configuration followed by full configuration

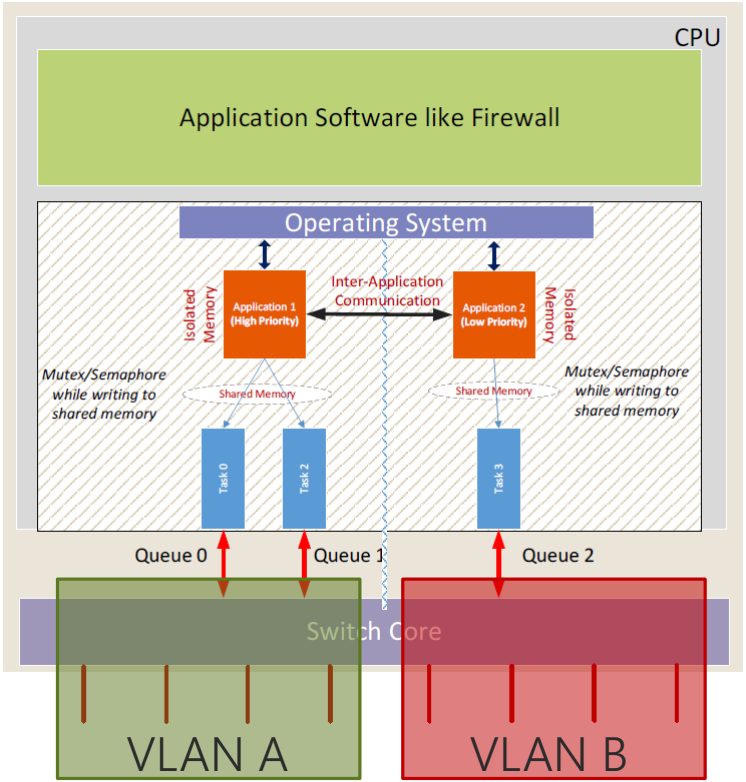


escrypt
SECURITY. TRUST. SUCCESS.

- Zone separation can be implemented using VLANs
- Software memory separation easily possible in host CPU

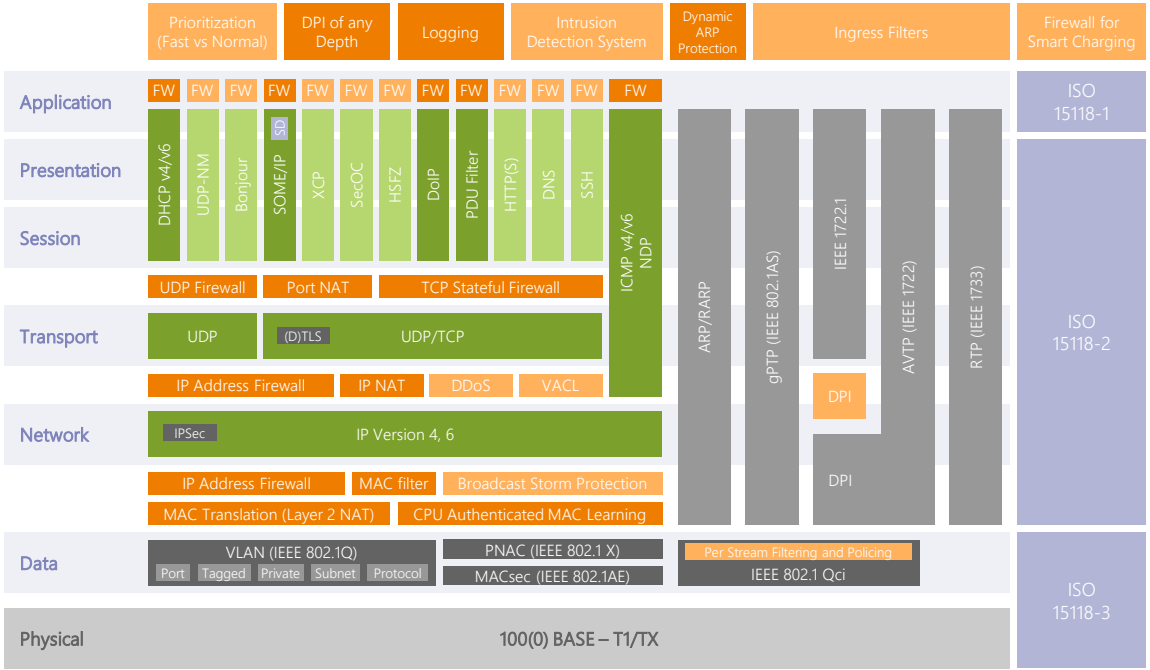
Best practice

- Try to have software traffic separation also in switch CPU
- Helpful typically for traffic from Untrusted port like DoIP
- No interference on normal communication if traffic flooding on untrusted port



escrypt
SECURITY. TRUST. SUCCESS.

- Ethernet has too many protocols
- Has bigger header size compared to CAN therefore needs more time to inspect header
- Latency/Bandwidth is a problem when inspecting headers at higher layer
- What should be the boundary between IDS and Firewall?



escrypt
SECURITY. TRUST. SUCCESS.

FIREWALL

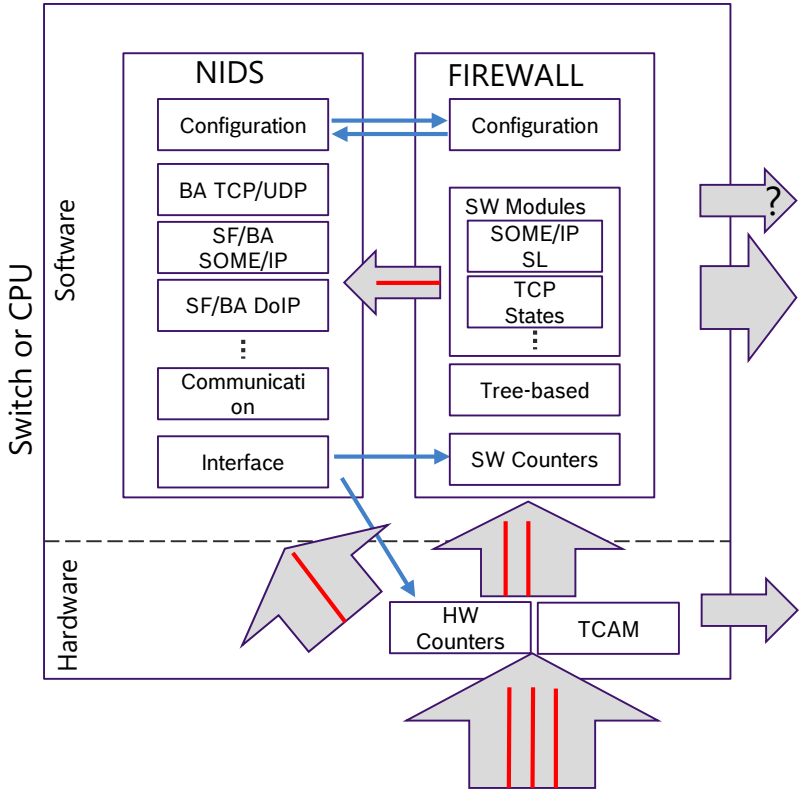
- "Fast Lane" very little delay in processing packets
- Stateless SOME/IP can be part of the fast lane, because we can drop packets

IDS

- "Slow Lane"
- Behavioral Analysis (BA) on TCP/UDP
- Detailed logging
- Application layer inspection (SOME/IP, DoIP etc.)

Where to implement

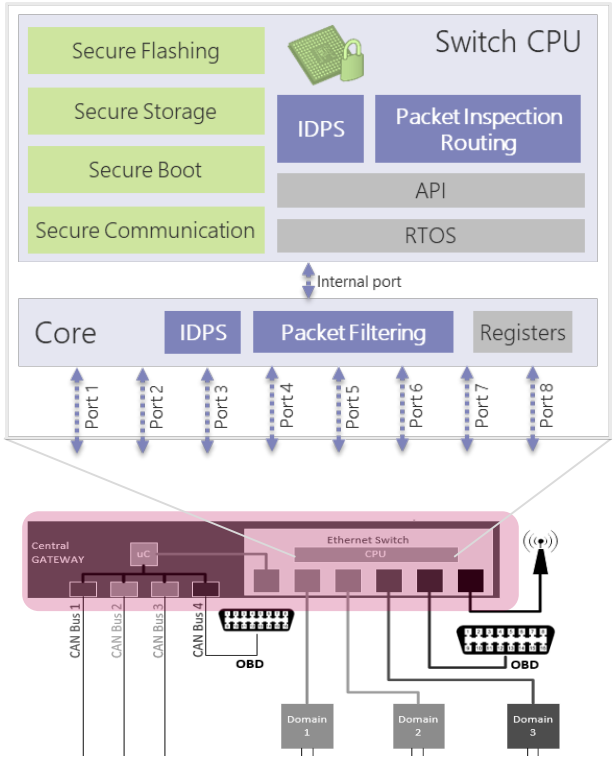
- Implement load balancing and distribution
- Do as much as possible in the switch, rest in external microcontroller



escrypt
SECURITY. TRUST. SUCCESS.

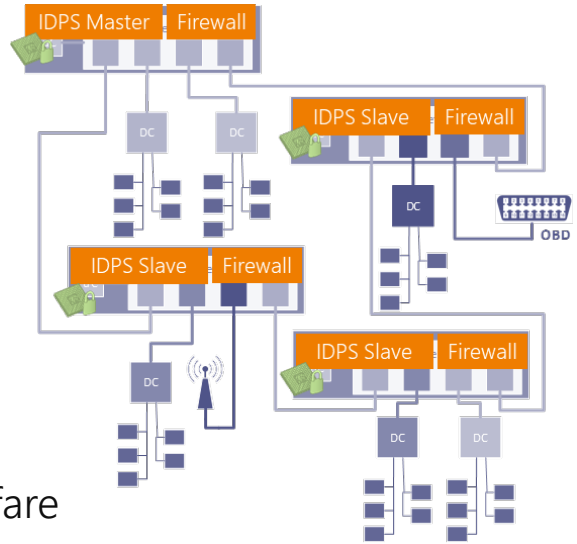
Implementation on Ethernet Switch Processor

- No interference with host microcontroller or embedded ECU
- High performance can be achieved with a good hardware/software co-design
- Application of security measures on switch controller using the integrated hardware security features
  - E.g., secure boot, secure key storage
- Secure update configuration of update
- Secure and central management of firewall, routing, and TSN/AVB configuration
  - Complete packet flow can be maintained from one place



escrypt
SECURITY. TRUST. SUCCESS.

- Distribution: Development of a (fully) distributed in-vehicle IDPS and Firewall solution
- Scalability: Load-balancing on arbitrary E/E-Architectures
- Dynamic: Adaptable configuration considering use-cases as, e.g., MAC address learning and IEEE 802.1X
- Actuality: Integration of new standardizations (e.g., TSN) or additional protocols possible
- Machine Learning: Sophisticated anomaly detection
- Fleet Monitoring: Maintain an overview about the fleet's welfare
- Protection: Real-time protection and reaction considering safety concerns
- Flexibility: secure updates of Firewall/IDPS rulesets able to support use-cases as, e.g., variant management and feature activation

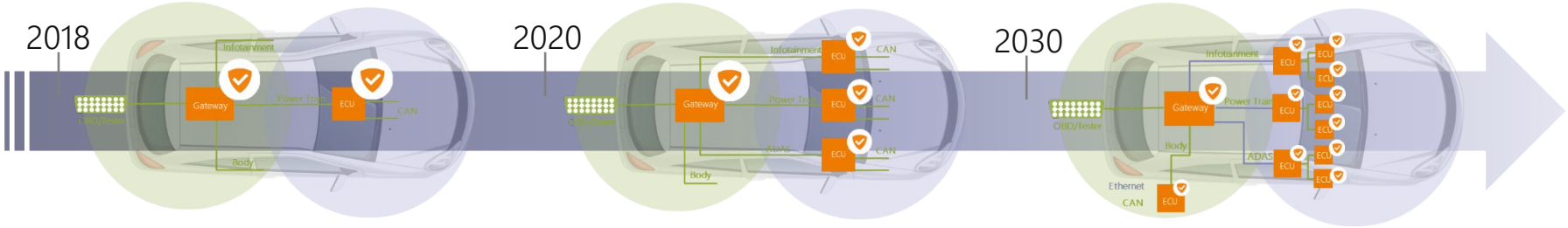


escrypt
SECURITY. TRUST. SUCCESS.

Development of a (fully) distributed in-vehicle IDPS

Self-learning intrusion detection mechanisms for Automotive Ethernet

Support for non µC based platforms, e.g. POSIX RTEs (Linux or QNX, cf. Adaptive Autosar)



- Central rule-based IDS (for single ECU instance)
- Most likely on gateways or other µC based ECUs

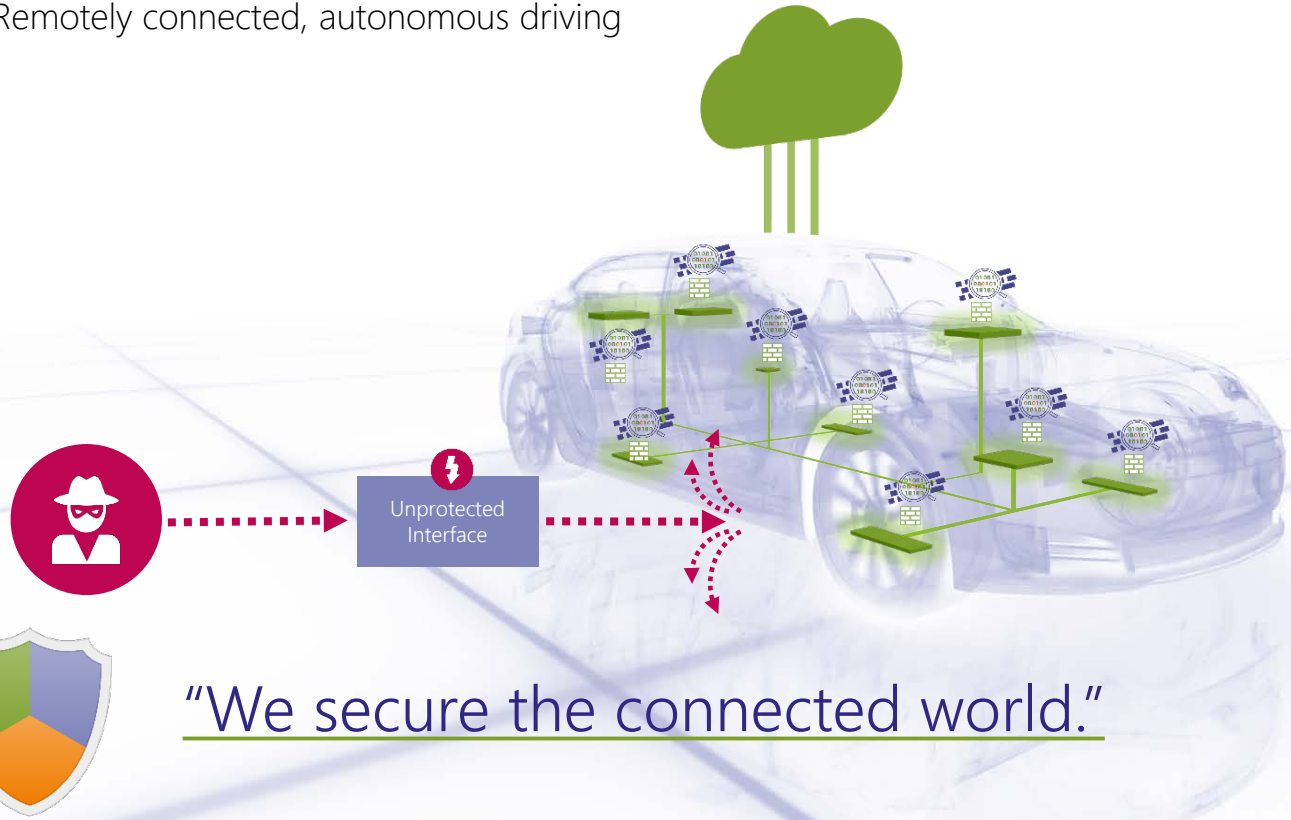
- Distributed rule-based IDS
- Collaboration and load-balancing between multiple IDS instances in the vehicle

- Distributed self-learning IDS
- Multi-Network and Multi-Platform distribution among heterogen ECU architectures

Future IDPS will be a fully distributed (virtually installed on every ECU) multi-platform solution

escrypt
SECURITY. TRUST. SUCCESS.

Remotely connected, autonomous driving



QUESTIONS?

"We secure the connected world."

ESCRYPT GmbH
Headquarters
Wittener Straße 45
44879 Bochum
Germany

Phone: +49 234 43870-200
Fax: +49 234 43870-211

info@escrypt.com
www.escrypt.com