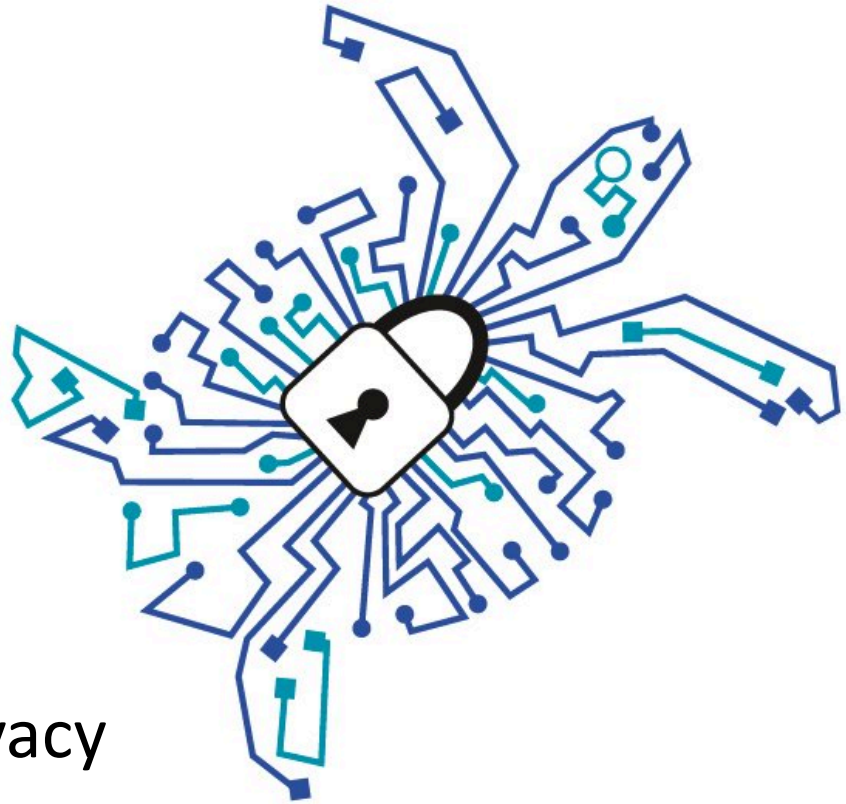
Current State in Car Security

Martin Schmiedecker

$whoami

- Security Engineer at Bosch Engineering
- Court certified expert witness
- Lecturer at TU Wien
- Member of C3Wien
- Co-founder of the Foundation for Applied Privacy



Disclaimers

- Opinions and views in this presentation are my own, and not necessarily the views of my employer.
- This is me, not Bosch
- Screenshots from YouTube are not my original work (linked)

However: Paper at ACM CSCS 2018

Cybersecurity Evaluation of Automotive E/E Architectures

Martin Ring
Bosch Engineering
Abstatt, Germany
martin.ring@de.bosch.com

Davor Frkat
Bosch Engineering
Vienna, Austria
davor.frkat@at.bosch.com

Martin Schmiedecker
Bosch Engineering
Vienna, Austria
martin.schmiedecker@at.bosch.com

ABSTRACT

The number of connectivity features of a modern car have expanded tremendously in recent times, including convenience applications over local wireless networks and back-end-connections over mobile networks. Additionally, the amount of exploited vulnerabilities in recent years has increased [16], and as such it is a paramount requirement to keep cybersecurity on pace with the additional demands. This is critical for new and upcoming features to prevent software vulnerabilities and later possibly incidents.

1 INTRODUCTION

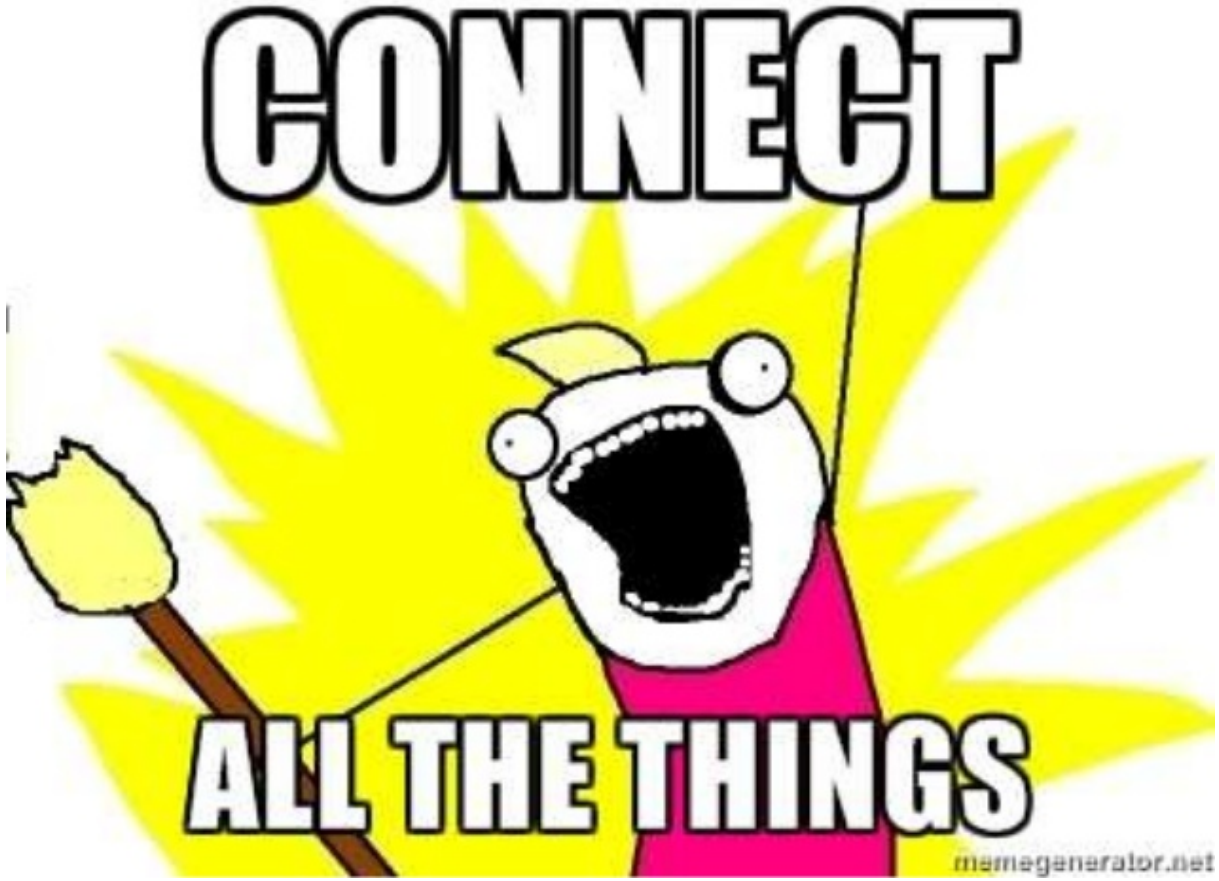
Based on recent attacks on vehicles that have received large coverage in media, in particular Charlie Miller's and Chris Valasek's attacks on a Jeep [12, 13], the need for additional security mechanisms is now clearly visible. As cars are further connected, the security requirements rise in the same way as their connectivity features. Possible pitfalls have been shown to, e. g., the BMW AG with an attack on their connected services [19], which was only possible because they had not activated encryption for the commu-

Problem Description

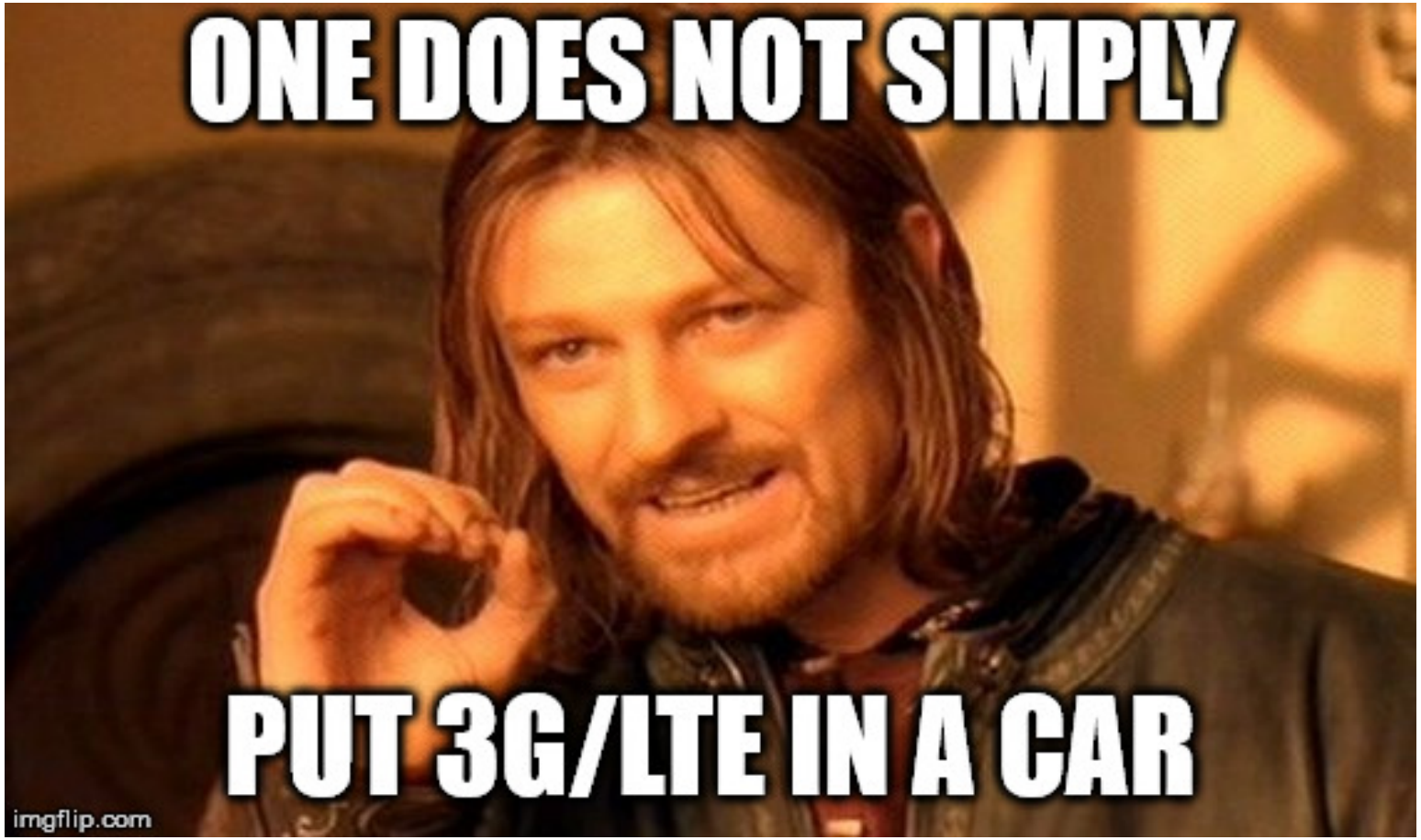
- Cars have become rolling computers …
- With wireless interfaces …
- And Internet connectivity …
- And software updates …

- And all this (possibly) while driving 130 km/h, or more

Problem Description



Problem Description



© Andy Greenberg, wired.com

Other examples

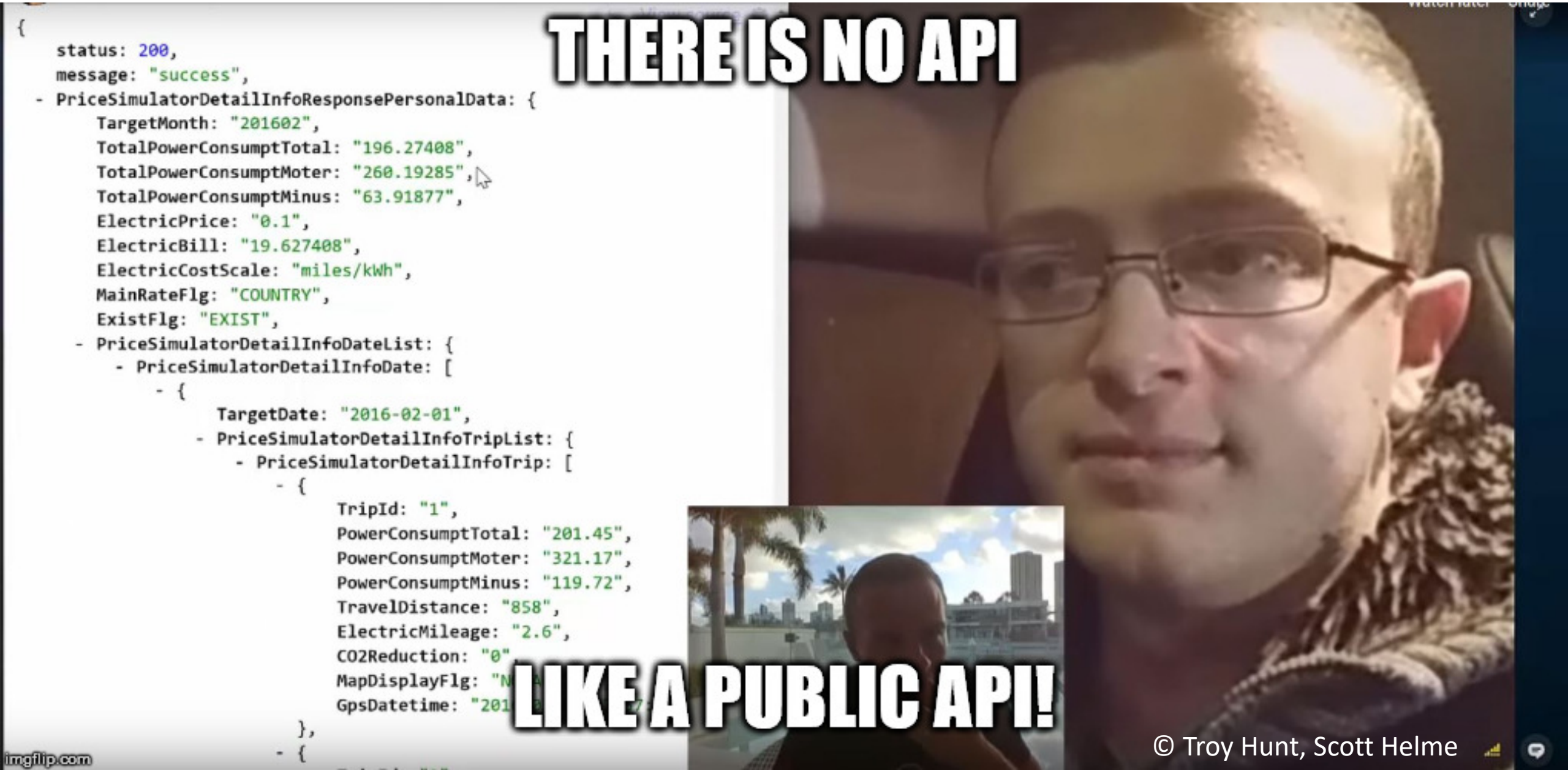
- Miller/Valasek via OBD-II (2010)
- Rouf et. al via wireless tire pressure sensors (2010)
- Checkoway et. al via MP3 & audio channel (2011)
- Verdult et. Al on Megamos immobilizer (2013)
- ADAC via IMSI catcher (2015)
- Garcia et. Al on weak crypto in keys (2016)
- KU Leuven via 40bit keys FOBs (2018)
- …

09-25-2017 Mon 01:01:55
WEST MIDLANDS POLICE
Camera 01
0:29 / 1:26

Attack Surface

Currently, mostly:

- Keys and keyless systems
- Immobilizers
- Odometer fraud
- Wireless interfaces



© Troy Hunt, Scott Helme

Current Environment

- Locked == safe
- Physical access wins
- CAN bus (and others) everywhere
- Patching is hard, mostly

Diagnostic access:

- OBD-II interface
- UDS with challenge-response

Mitigation Overview

- Currently very, very active field
- Entire industry is shifting

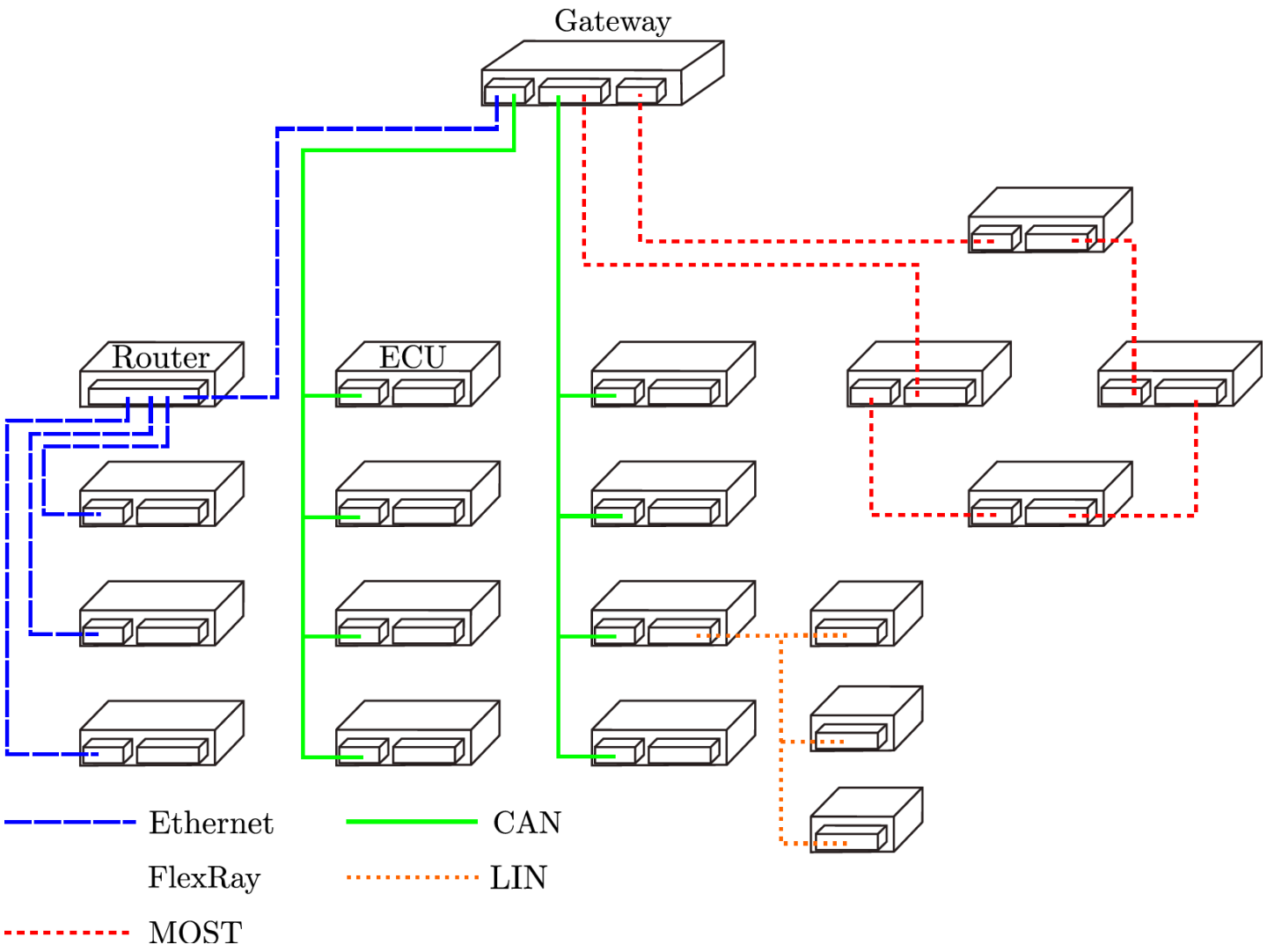
Challenges:

- Long development cycles
- Long product lifetime

Mitigation Overview

Feature	2018	2023+
Domain Separation	Seldom	Common
Public Key Infrastructure (PKI)	Seldom	Many
Hardware Trust Anchor (e. g., HSM)	Seldom	Many
AUTOSAR Modules	Seldom	Many
Signed Software Updates	Seldom	Many – Common
Secure Diagnostic Services	Seldom (with weaknesses)	Many
Secure Boot	Seldom	Many
Authenticated Boot	Seldom	Many
Secure Communication with Backend	Many	Common
Secure Onboard Communication	None	Many
Firewall	Many	Common
Intrusion DetectionSystem	None	Seldom-Many
Wi-Fi/Bluetooth Security	Common (with weaknesses)	Common

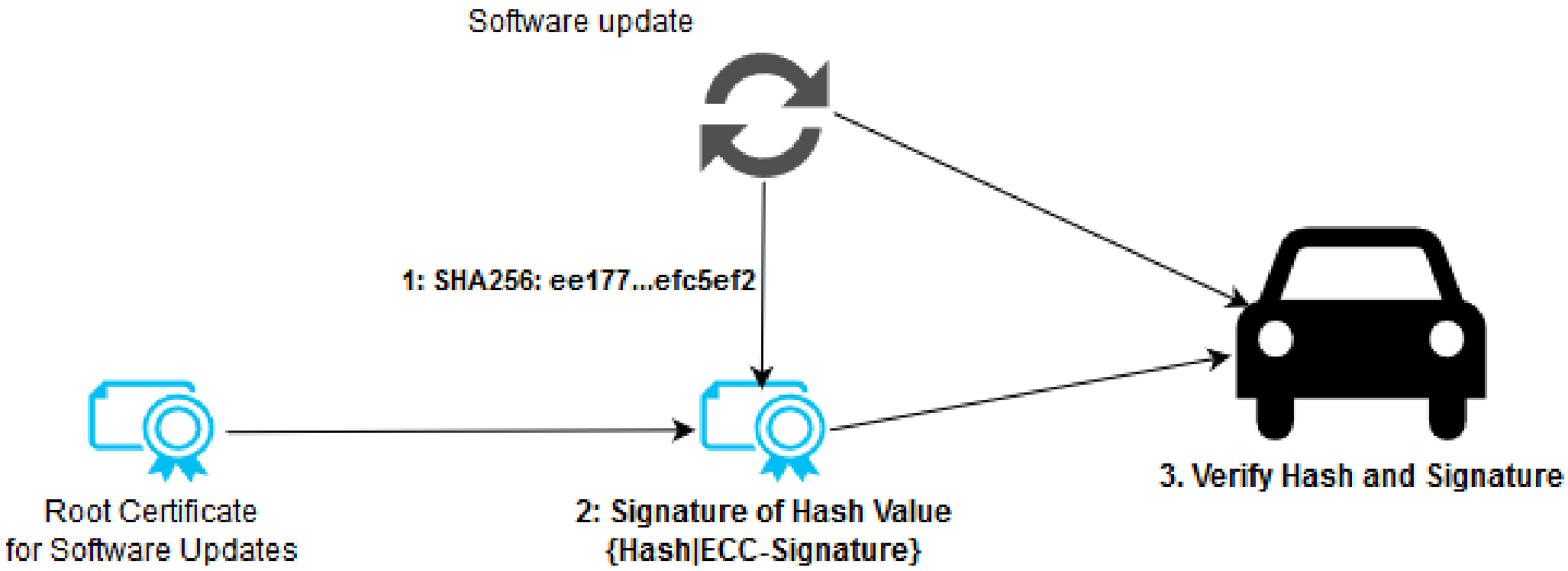
Domain Separation



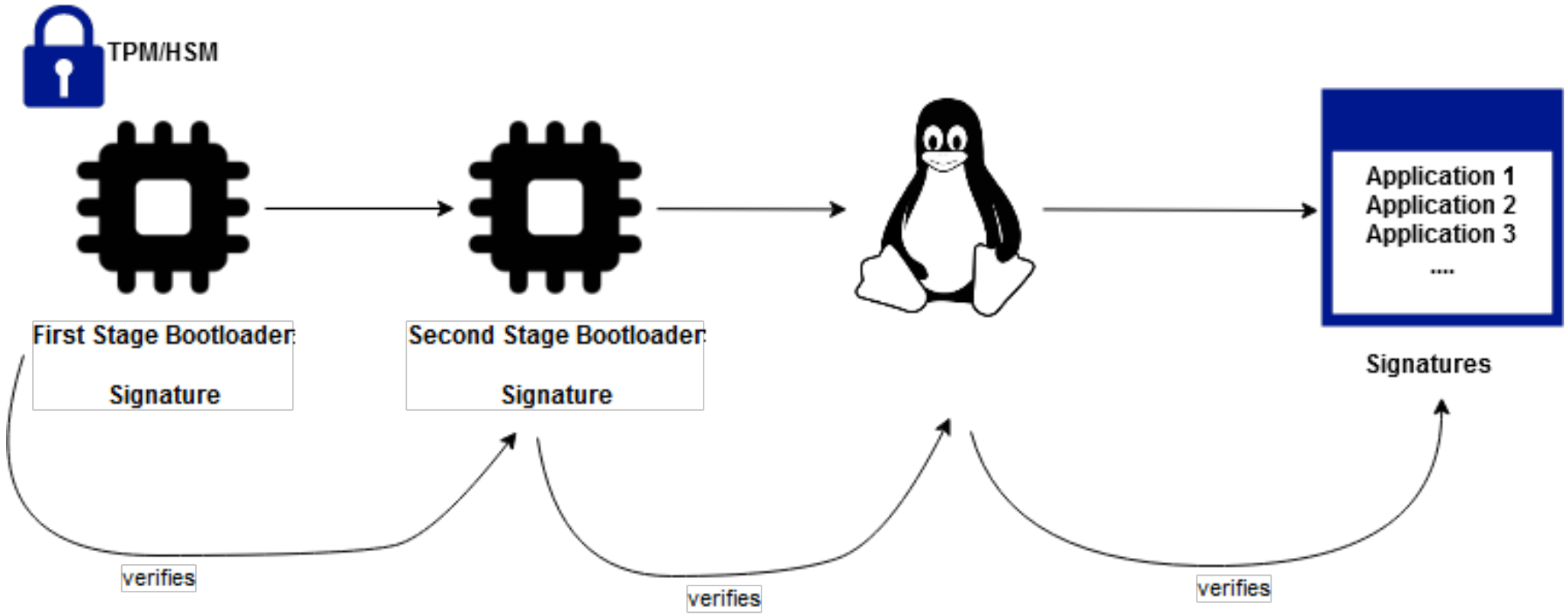
Hardware Trust Anchors

- HSMs or TEEs
- Store keys securely
- Verify signatures securely
- Ed25519, ECC, SHA256 …

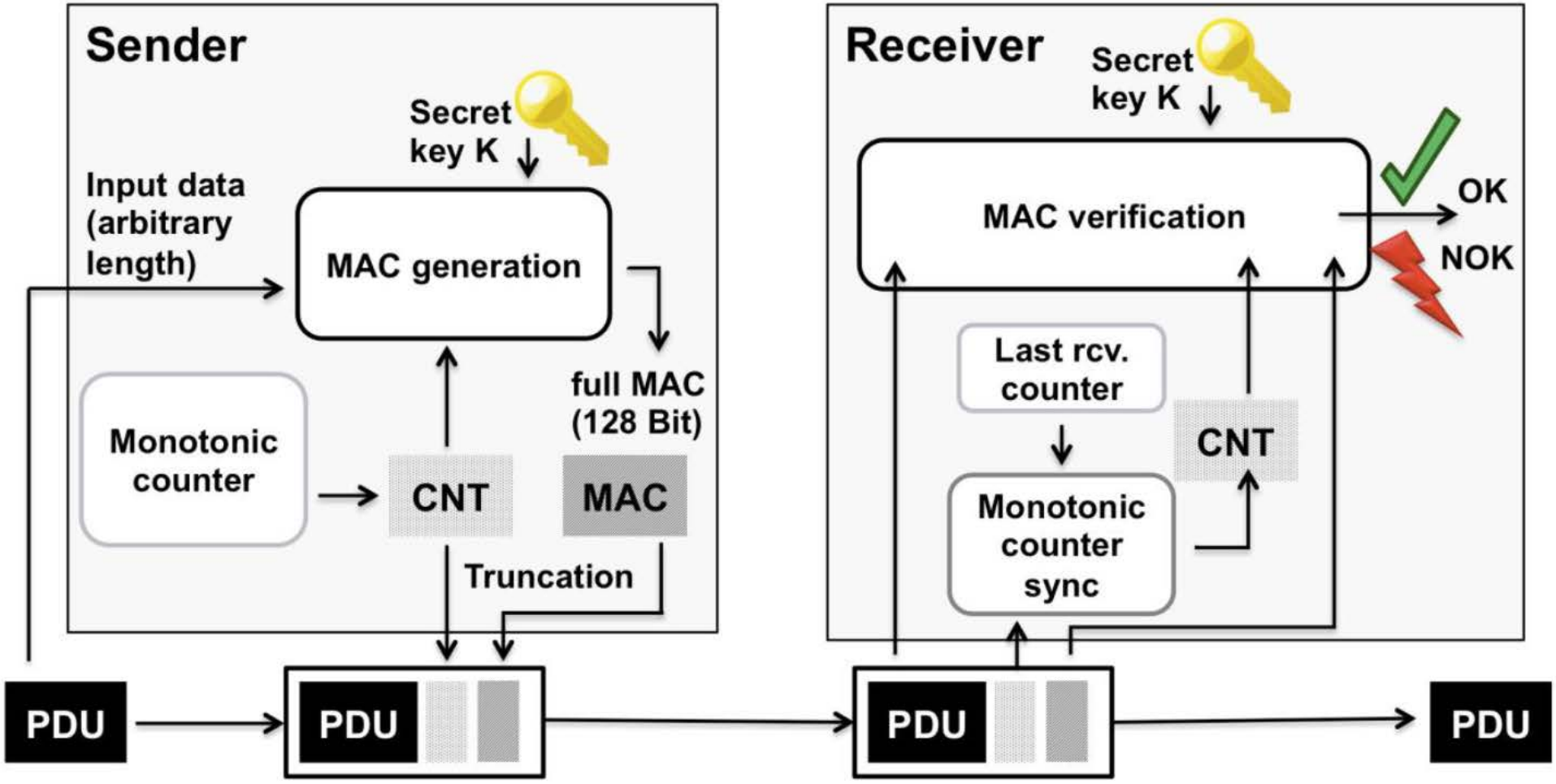
Signed Software Updates



Secure Boot


TPM/HSM
First Stage Bootloader
Signature
Second Stage Bootloader
Signature
Application 1
Application 2
Application 3
....
Signatures
verifies
verifies
verifies

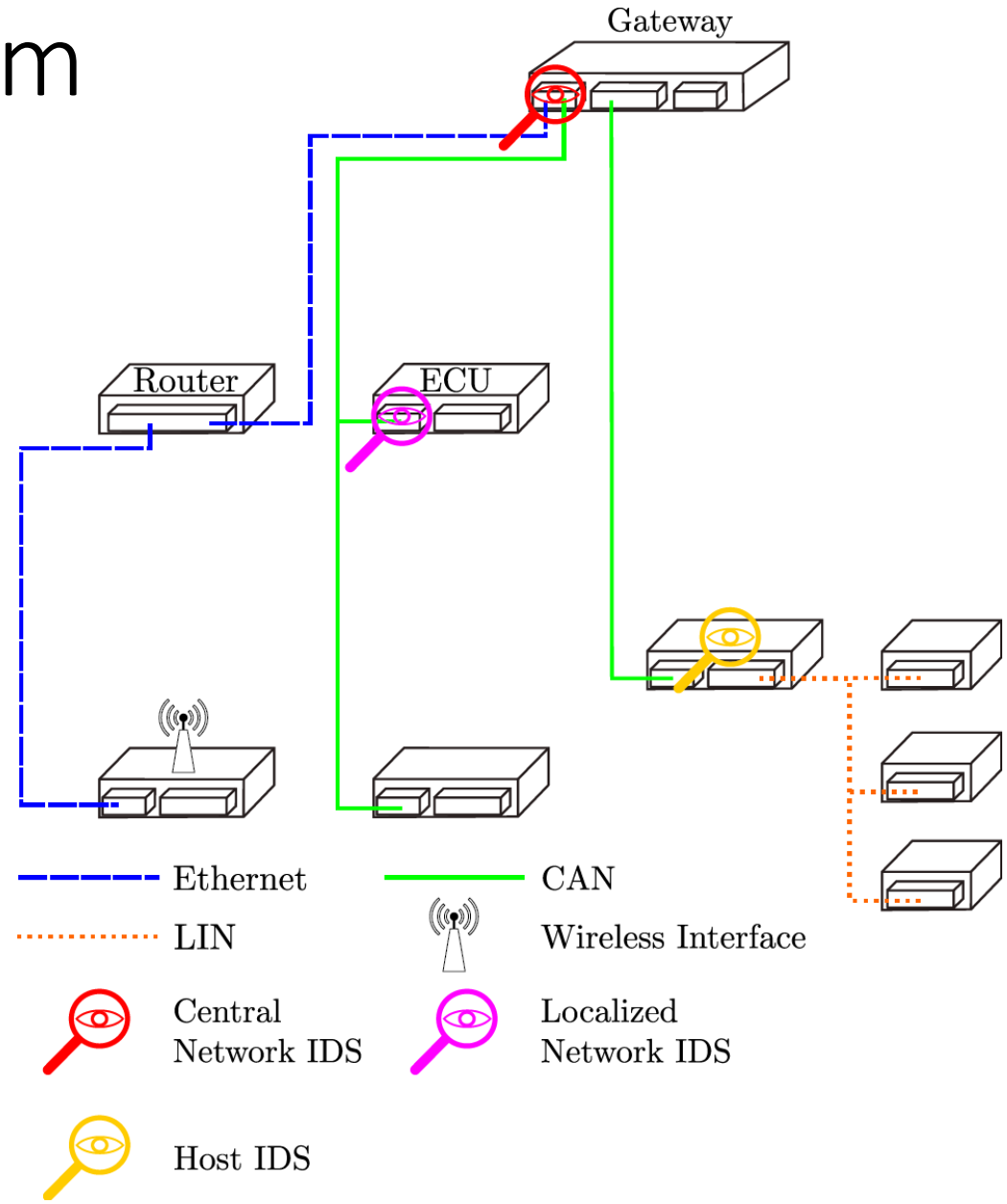
Secure Onboard Communication



Source: AUTOSAR – SecOC Requirements, v4.3

Intrusion Detection System

- Analyse traffic pattern
- Detect outliers
- Part of the NHTSA recommendations



Near Future

- Autonomous driving
- AI i.e., convolutional neuronal networks
- Automotive Ethernet
- Modern sensors (radar, LiDAR, …)
- Cloud services
- Wireless: LoRa, Narrowband-IoT as part of LTE, 5G, meshing, …
- Vehicle-to-vehicle, vehicle-to-X
- …
- Also, legislation!

To summarize …

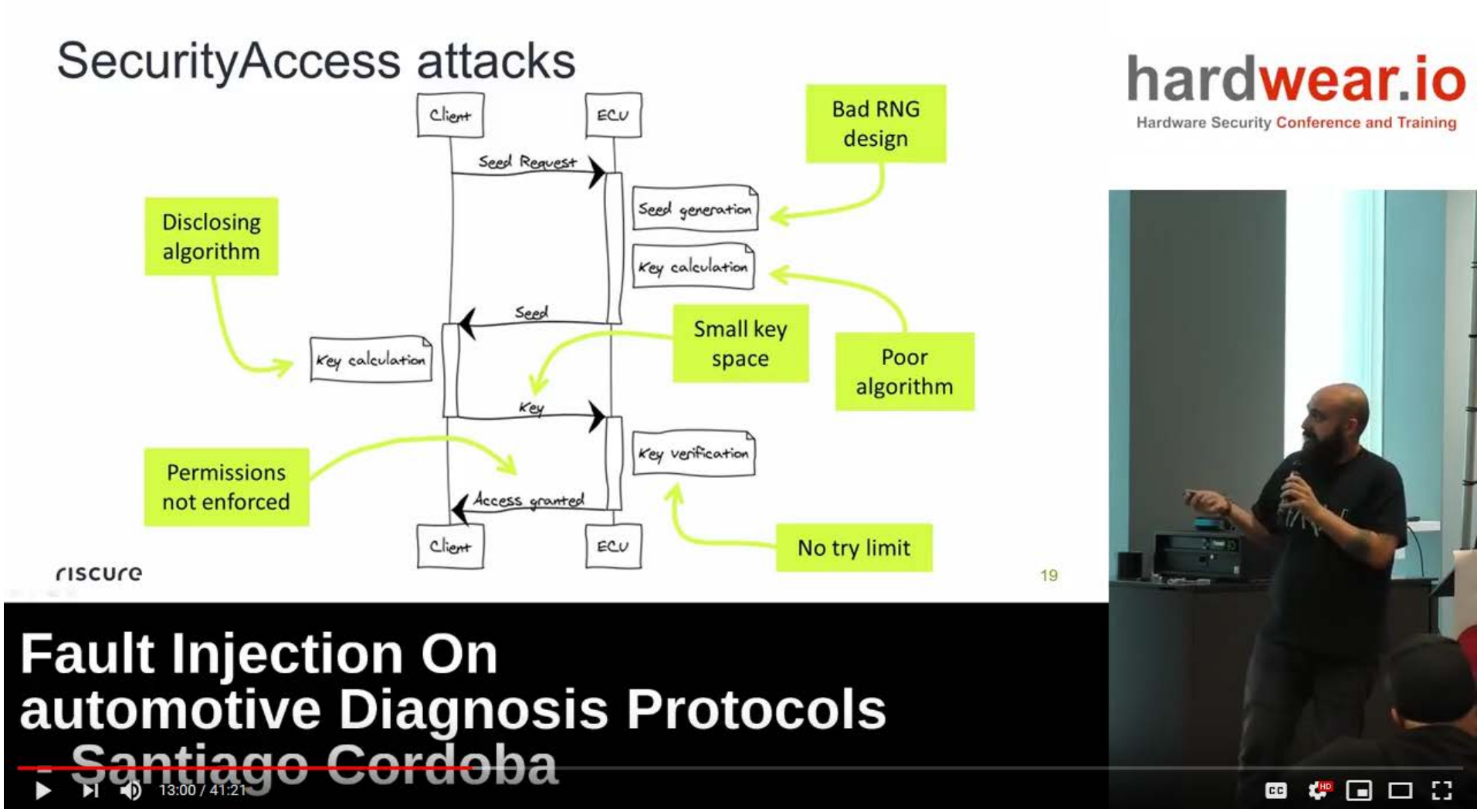
- Security improves rapidly
- En-detail and en-gros
- “May you live in interesting times”

- $$$ is still a powerful deterrent
- Read the paper for all details

Thank you for your attention!

Bosch is hiring!

- Goto https://www.bosch-career.at/

pi@raspberrypi:~/tesla $ python poc.py pocdemo
---------- PHASE 0: retrieve car identifier ----------
TESLA
Max. 40 min
0:53 / 2:01

Glitching (Power)