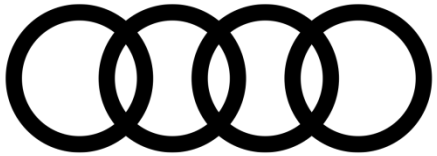


ulm university universität ulm

TECHNISCHE UNIVERSITÄT DARMSTADT

A Testing Framework Architecture Concept for Automotive Intrusion Detection Systems

30.05.2017 - Automotive 2017

Agenda

- **Introduction**
- **Intrusion detection systems scope**
- **Problem statement**
- **Our approach**
- **Conceptional architecture**
- **Conclusion**
- **Outlook**

Introduction
Speakers

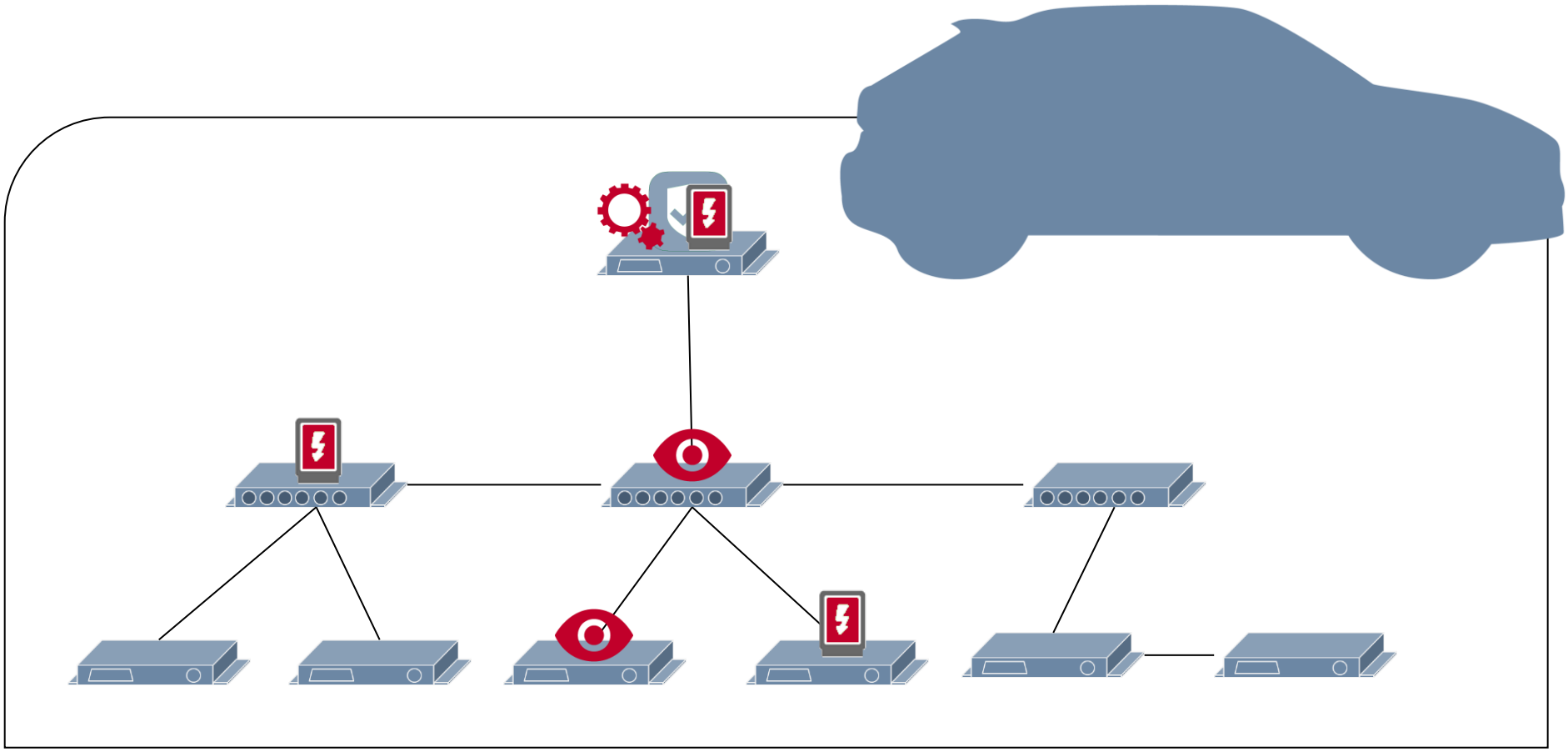
Corbett Christopher

- Phd Student at the University of Ulm
- Automotive security engineer at Audi AG
- ~ 15 years of experience in the automotive industry
- christopher.corbett@audi.de

Basic Tobias

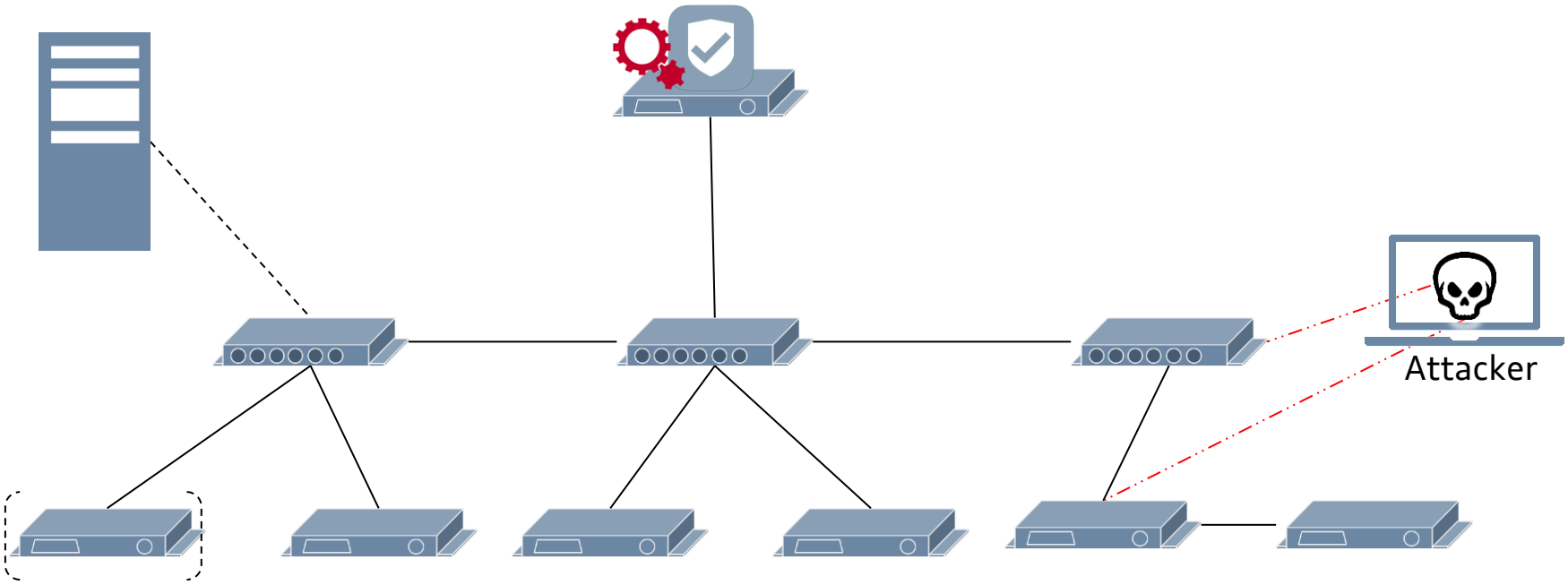
- Completed double masters degree on IT security and computer science at the university of Darmstadt
- Automotive specialist security and privacy at Continental AG
- fi59eged@rbg.informatik.tu-darmstadt.de

Intrusion Detection Systems in In-Vehicle Networks
Scope



Mainly focusing on Network Intrusion Detection Systems (NIDS) and anomaly detection

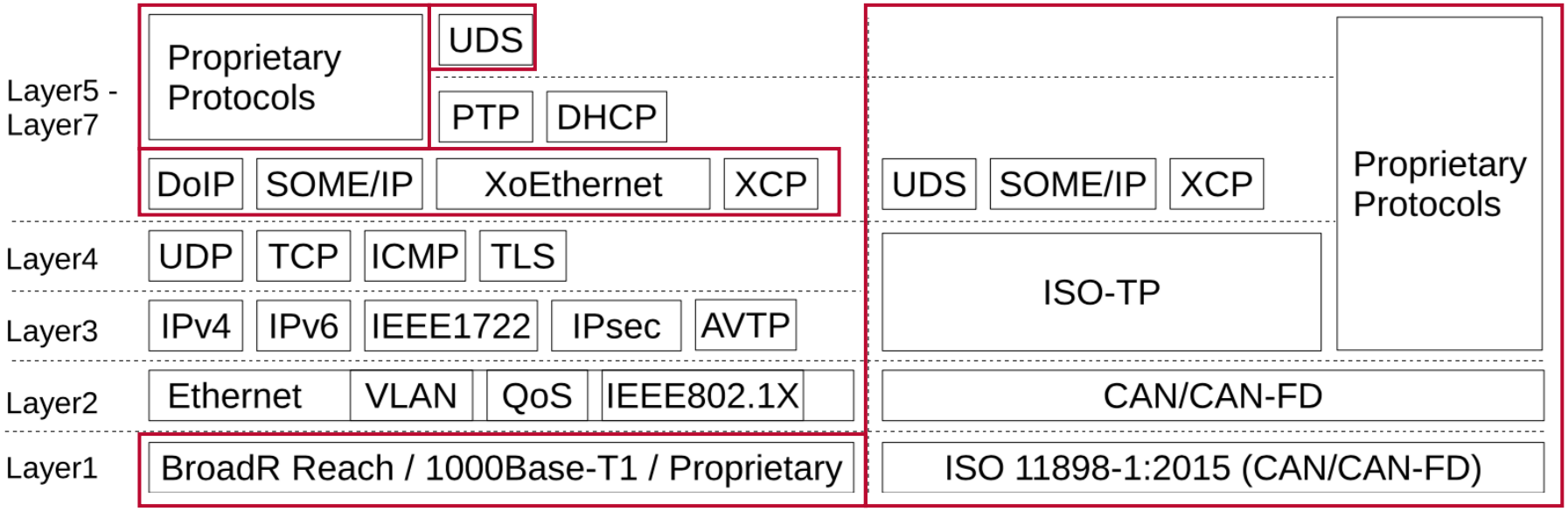
Intrusion Detection Systems in In-Vehicle Networks
Evaluation



Evaluation during development phase is very difficult as real data and attacks do not exist!

Intrusion Detection Systems in In-Vehicle Networks

Automotive protocols



- **There is a large variety of protocols to consider !**
- **Some protocols are automotive only !**

Problem Statement

- In-vehicle network traffic not publicly available for use
- Automotive network topologies differ from OEM to OEM
- Sharing of information, especially during development phase, is prohibited and often part of intellectual property (IP)
- New technologies (e.g. Ethernet, CAN-FD) and protocols (e.g. SOME-IP) can‘t easily be evaluated
- Malicious traffic barely exists
- Complexity of in-vehicle attacks is different to existing attacks

Dependencies for an NIDS evaluation are not fulfilled !

Our approach
Preparation

- Malicious traffic
- Valid traffic
- Evaluation metrics

NIDS Evaluation Requirements

- Automotive attack scenarios
- Applicable in real vehicles

Attack Requirements

- Support for required protocols
- Support for required technologies
- Use case coverage
- Realism

Network Traffic Requirements

- Available tools
- Supported platforms
- Available libraries
- User perspective

Miscellaneous

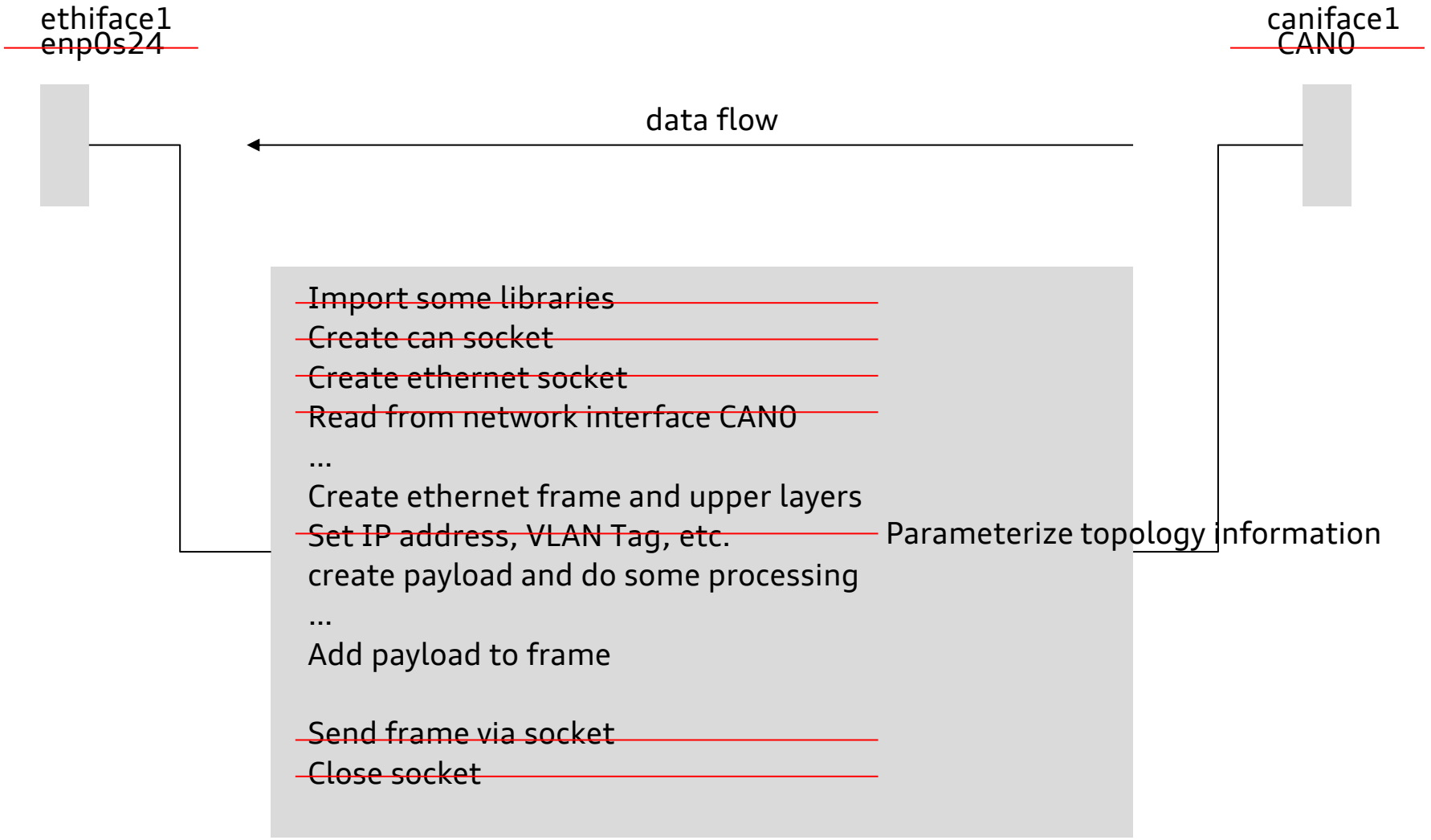
Our approach

Evaluation of existing Tools

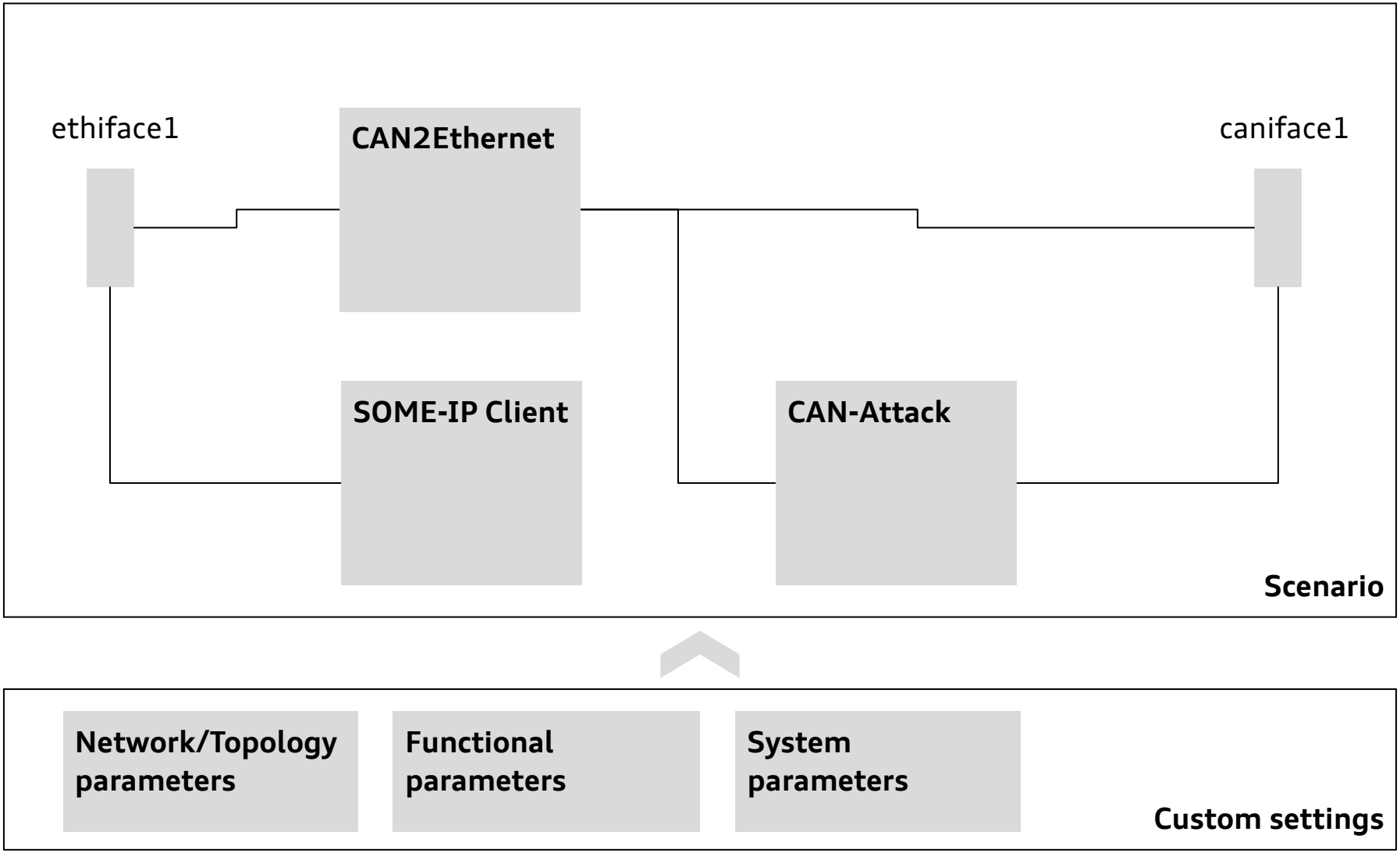
	PCAP Replay	Multiple Interface Handling	Scripting	Layer 2 Support	IPv6 Support	Automotive Protocols	Generate Mixed Traffic	Priority Handling	Capture Traffic	Packet modification	Packet sending interval	Automation
Tomahawk	✓						✓					✓
Bit-Twist	✓			✓			✓		✓			✓
Hping2							✓					✓
Hping3			✓				✓		✓			✓
Nemesis				✓	✓		✓					✓
Ostinato	✓	(✓)	✓	✓	✓		✓		✓		(✓)	
packETH	✓			✓	✓		✓				✓	
Yersinia				✓			(✓)		✓			
netsniff-ng	✓			✓	✓		✓		✓			
pktgen	✓	(✓)	✓	✓	✓		✓		✓			✓

Existing tools don’t cover the necessary requirements!

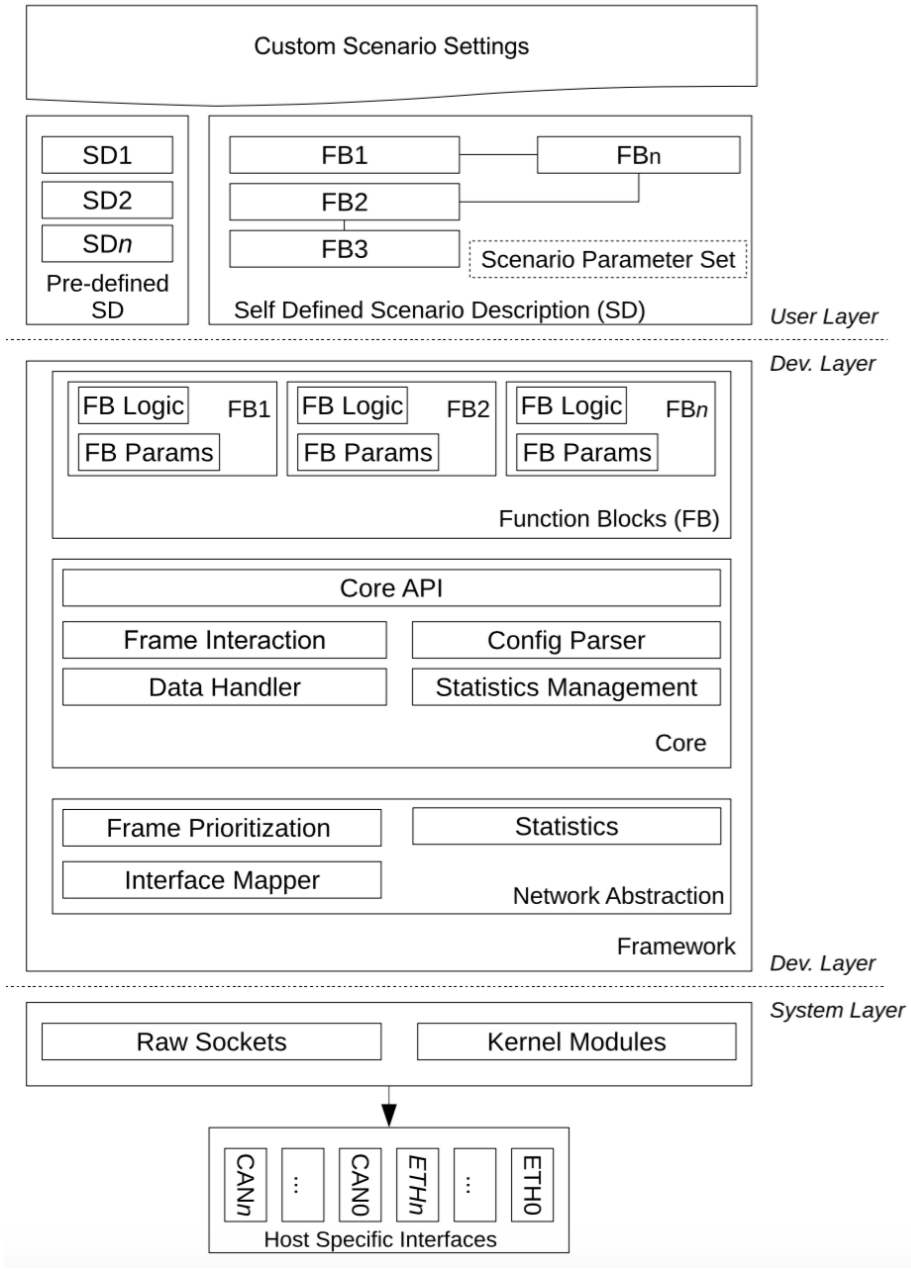
Our approach
Practical example



Our approach
Practical example



Architecture Concept



Our approach
Summary

- **Architecture only based on open source components**
- **Support of several network interfaces (Ethernet, CAN, WiFi, USB, ...)**
- **Separation of use case logic, operating system dependancies and network stacks**
- **Create realistic automotive traffic for Network Intrusion Detection Systems (NIDS)**
- **Providing If-Than-Else Functionality**
- **Separation of network topology information and use case description**
- **Encapsulate logic in function blocks**
- **Enable simple fuzzing functionality**
- **Sharing implementations, setups and (if possible) datasets with the community**

Conclusion

Feasible:

- If-than-else functionality
- Scene description
- Capsulating functionality
- Using open source software only
- Concept architecture implementation

Challenging:

- Parallelism
- Message/Interface priorities
- Timing
- Library support of protocols

Outlook

First prototype called (anxiety) using python3
Publication of the source code on a collaboration plattform (pending)

Final master thesis available soon on the university of Darmstadt website containing:

- **Detailed descriptions**
- **Performance measurement**

Publication of a follow up document about the implementation and evaluation of the prototype (currently working on it)

Thank you