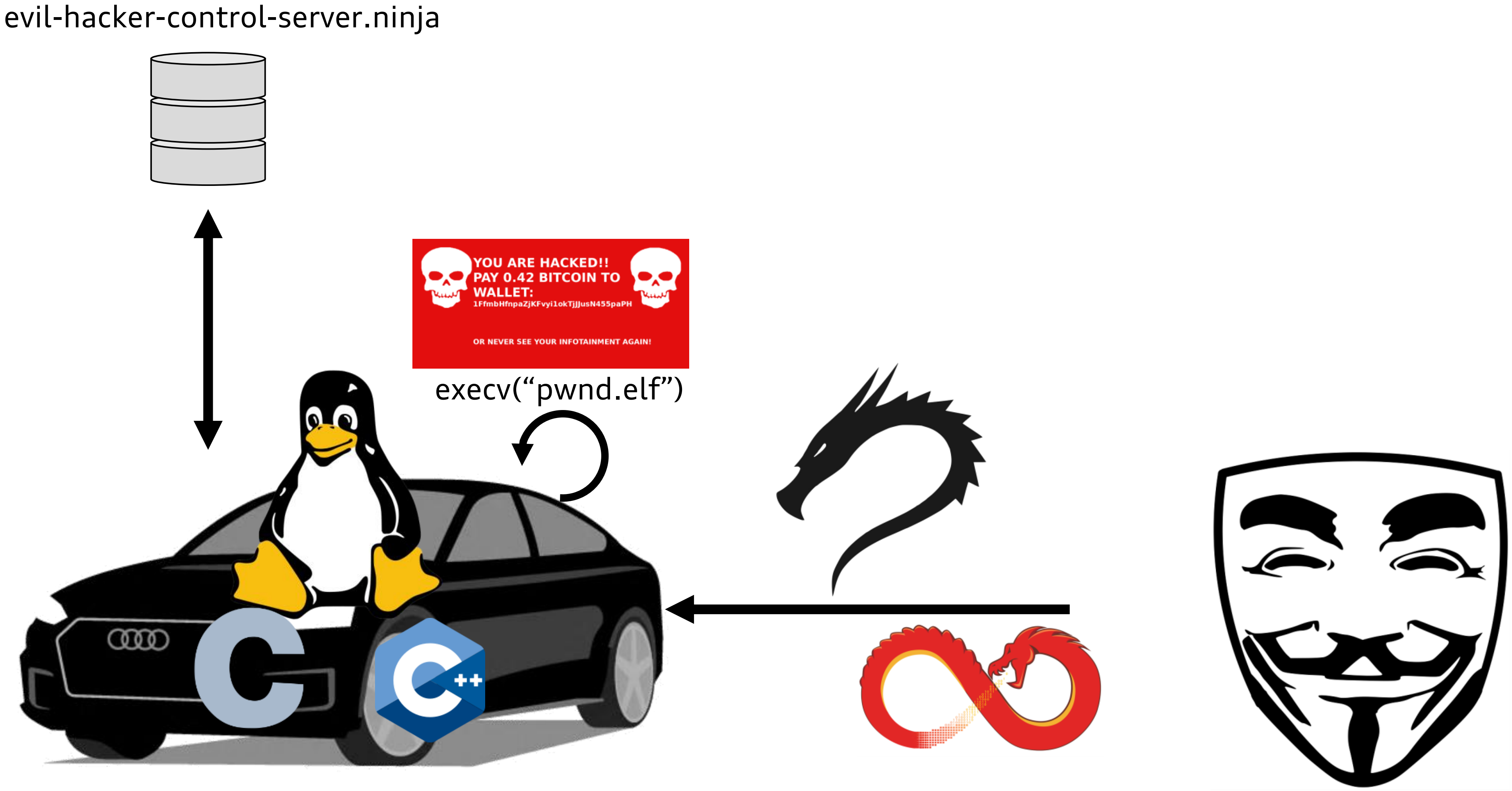
Embedded Intrusion Detection based on AI

Dr.-Ing. Andreas Weichslgartner, Bonn, 17.10.2019

Audi Electronics Venture



evil-hacker-control-server.ninja

YOU ARE HACKED!!
PAY 0.42 BITCOIN TO
WALLET:
1FfmbHfnpaZjKFvyi1okTjJJusN455paPH

OR NEVER SEE YOUR INFOTAINMENT AGAIN!

execv(“pwnd.elf”)

Why Should we Use an IDS?

The Ethernet network should ***be analyzed for anomalies****. While, in general, the problem of generic intrusion detection is difficult and often leads to false positives,* ***in this case it works well****. That is because this is a network devoid of human users like we are used to in an enterprise environment. All the traffic is periodically generated from* ***machine to machine****. […] Like Ethernet,* ***the CAN network*** *traffic should be observed in real time to identify anomalies. All the attacks outlined in the historical section could have been detected (and prevented) with even the most trivial CAN network intrusion detection software.*

Miller, Valasek: Securing Self-Driving Cars (one company at a time), 2018

UNECE WP 29 is coming

Draft Recommendation on Cyber Security of the Task Force on Cyber Security and Over-the-air issues **of UNECE WP.29** GRVA:

- *The use of combinations of gateways, firewalls, **intrusion prevention or detection mechanisms, and monitoring** are employed to defend systems*
- System **monitoring** (mentioned in various places)
- Limit and **monitor message content** and protocol
- Measures to protect systems **against embedded viruses/malware** should be considered
- System monitoring for **unexpected messages/behaviour**
- …

- See also ISO/SAE CD 21434 Road Vehicles — Cybersecurity engineering

Agenda

Motivation

Intrusion Detection

Anomaly Detection & Machine Learning

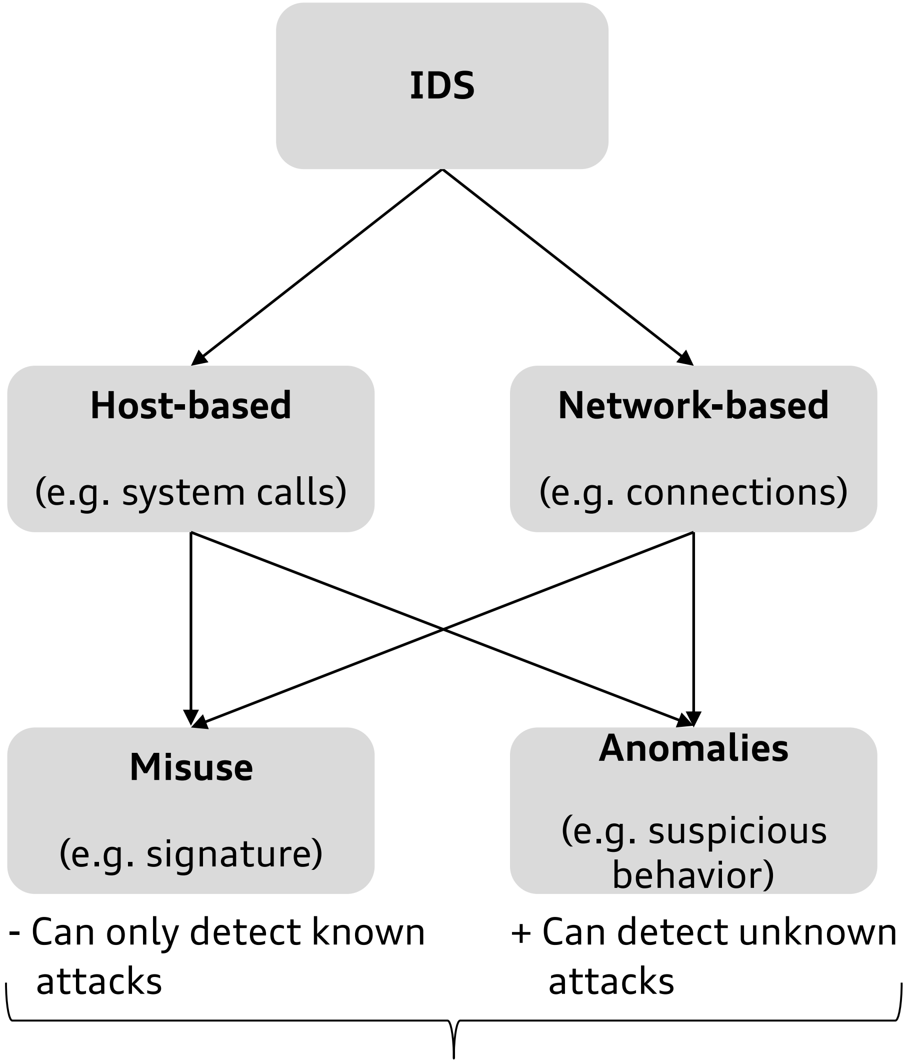
Results

Summary

Intrusion Detection Systems

A Taxonomy

Intrusion Detection Systems (IDS) Classification



- Can only detect known attacks

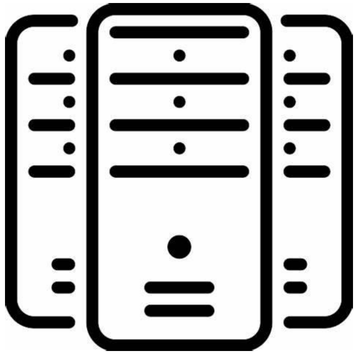
+ Can detect unknown attacks

Can be combined to detect reliably known attacks and also flag suspicious traffic of unknown attacks

Differences of IDS

Enterprise Domain

- Vast availability of computing and memory resources
- Special hardware (GPUs, FPGAs, Many-Core-Chips) available
- Databases with vulnerabilities, malware, IDS rules
- Unstructured/unpredictable communication & computation
- Human to machine communication



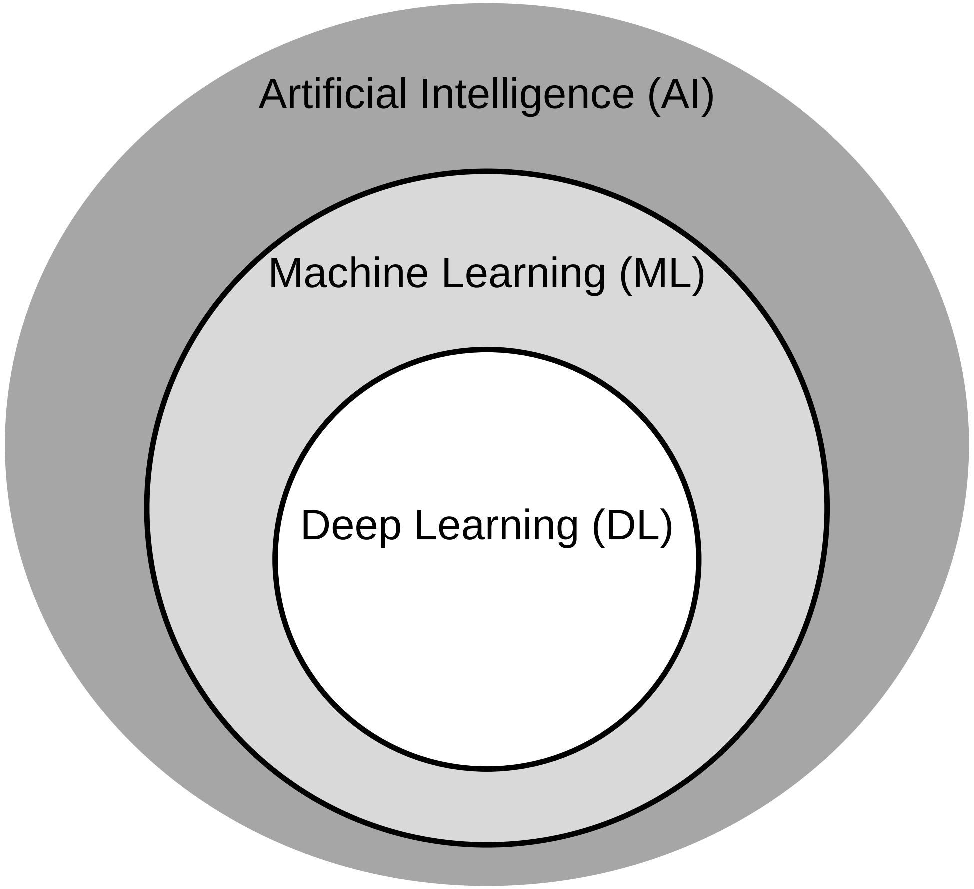
Embedded Automotive Domain

- Limited computing and memory resources
- No special hardware such as GPUs available
- No database with known attacks
- Structured/predictable communication & computation
- Machine to machine communication

Anomaly Detection

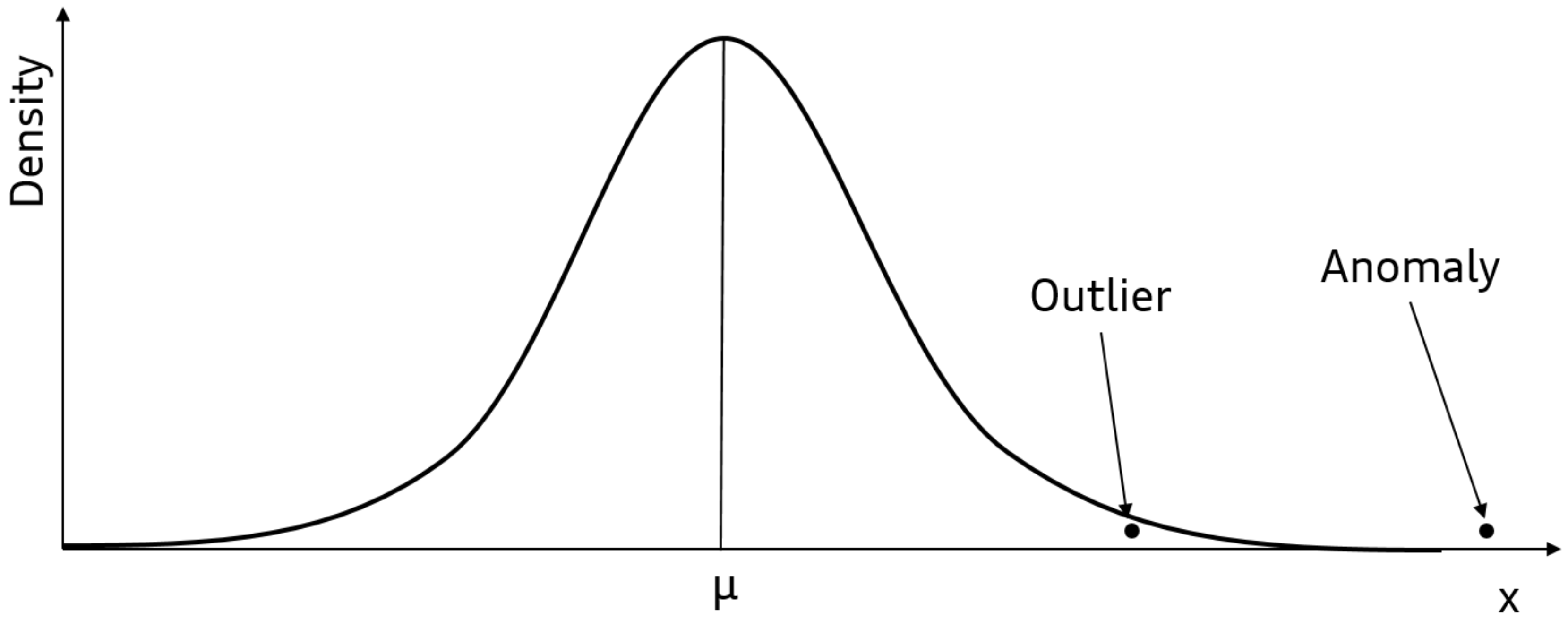
What is Normal and What Abnormal?

What is AI?

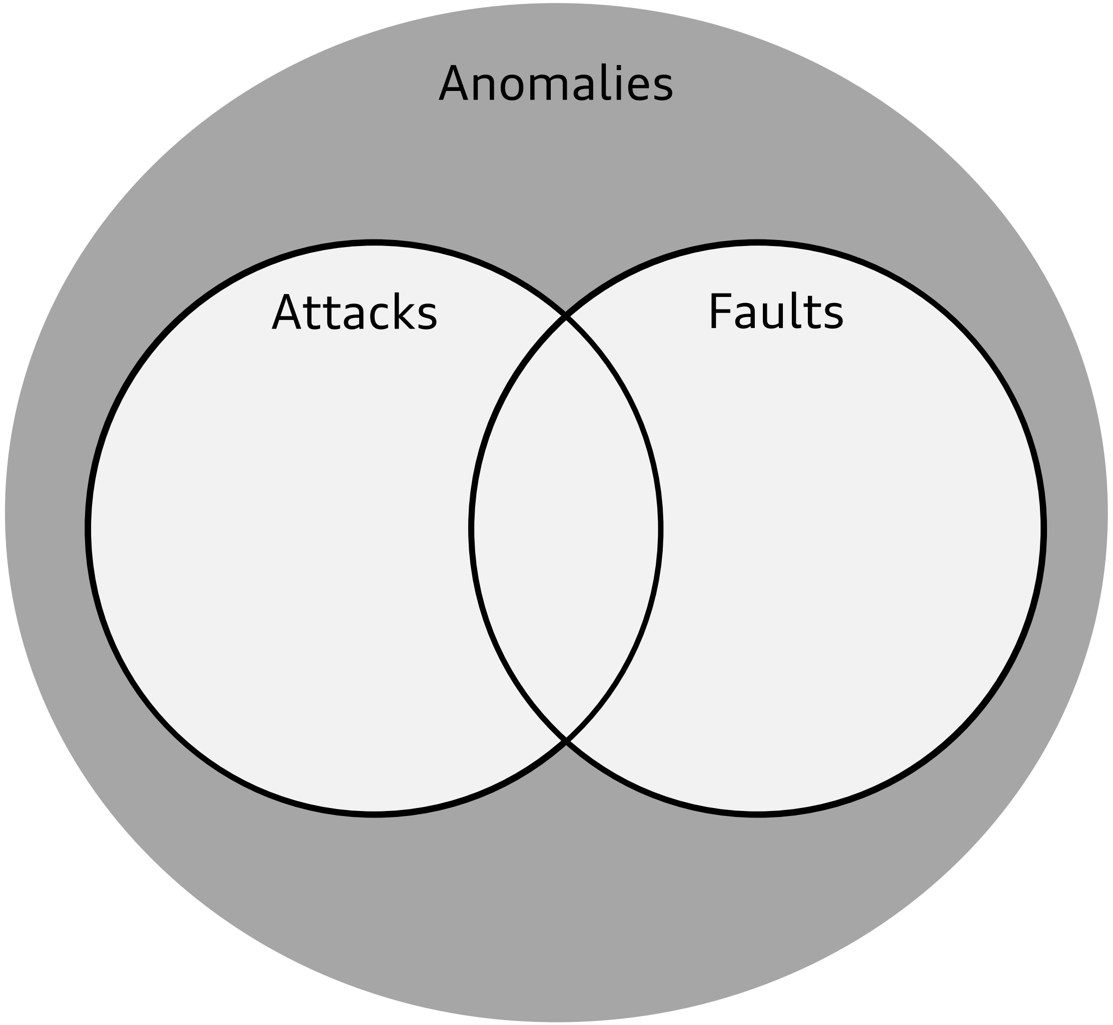

Artificial Intelligence (AI)
Machine Learning (ML)
Deep Learning (DL)

What is an Anomaly?

Example of an Anomaly and an Outlier

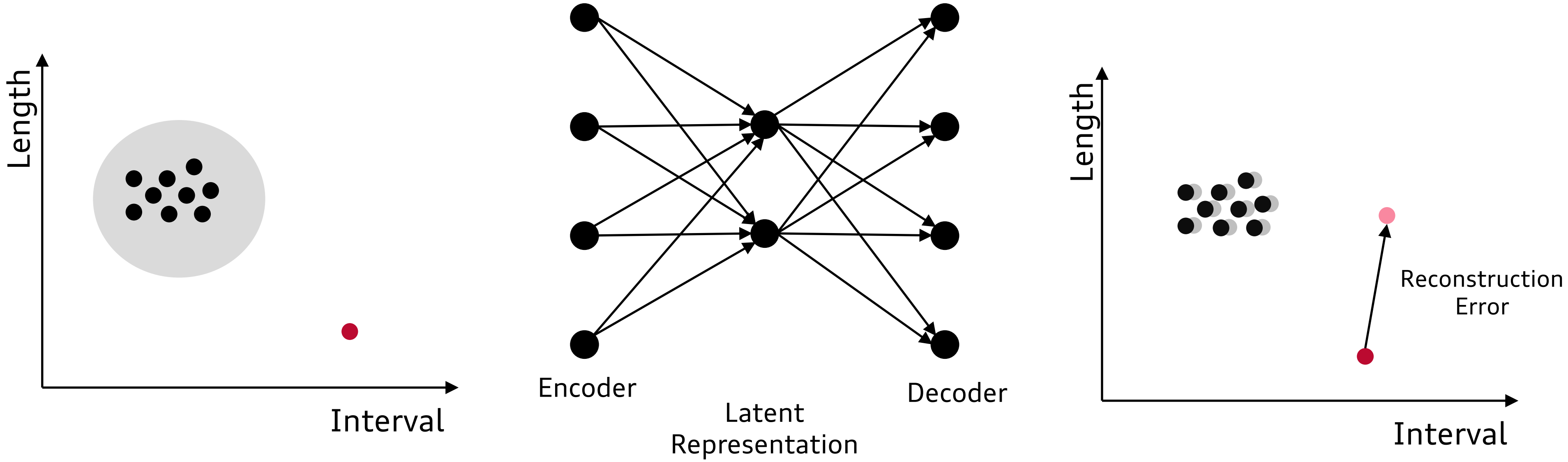


What to do with Anomalies?



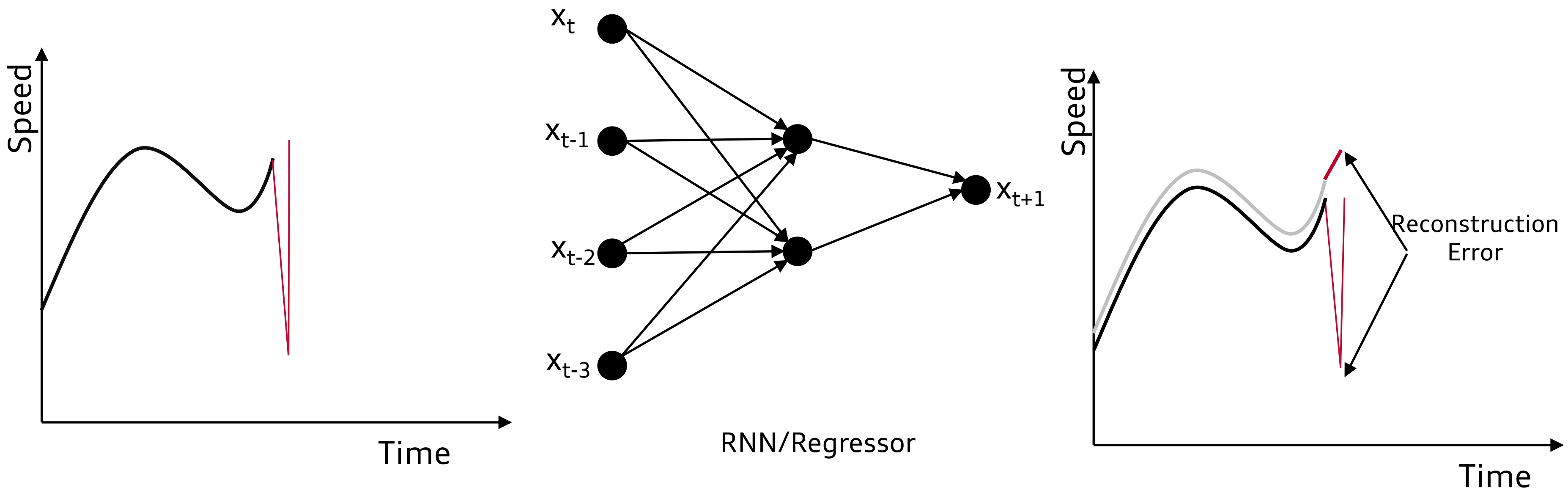
Anomaly Detection

- Point Anomaly



Anomaly Detection

- Context-based Anomaly



Implementation

Bringing AI to the ECU

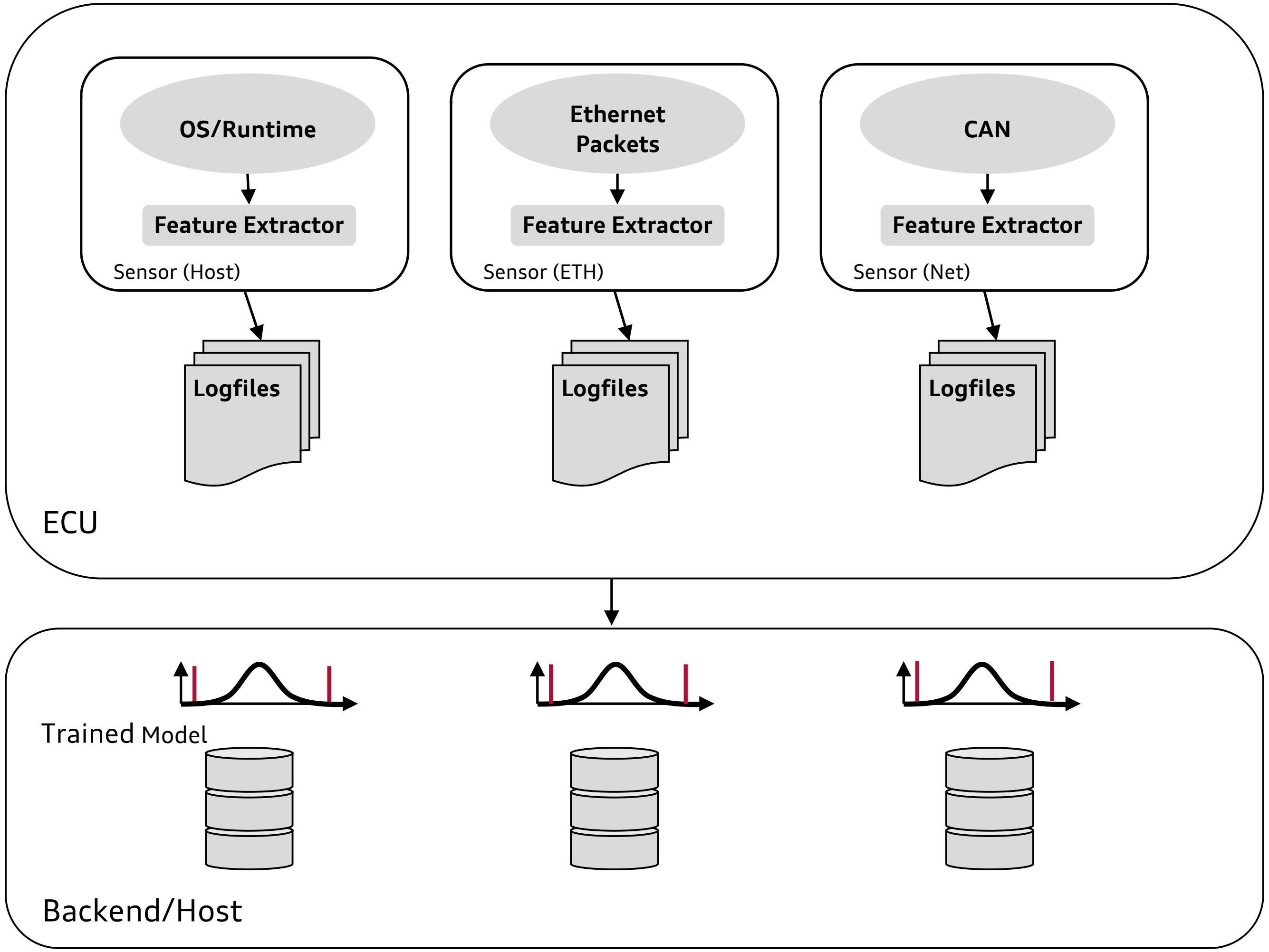
Challenges of an Embedded Implementation

- No GPUs, FPGAs, or accelerators for linear algebra are available for security

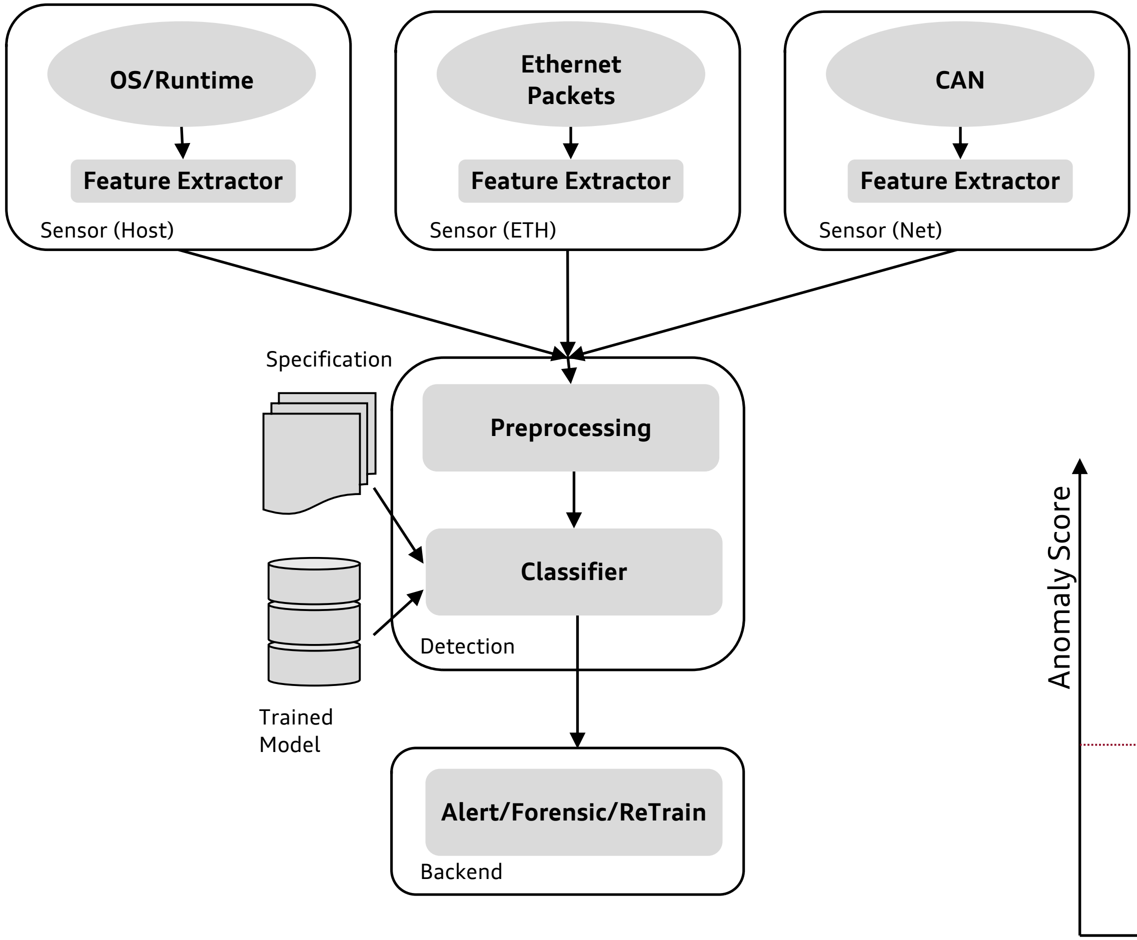
- Memory limitations on ECU prevent large models:
  - Algorithms like k-NN are not suitable
  - Pruning, quantization, precision reduction

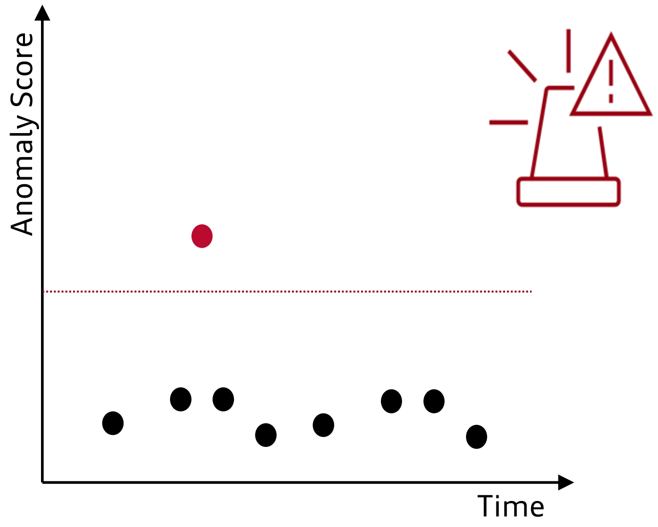
- Real-Time requirements:
  - Each packet should be classified within a fixed time window

Logging and Training



Inference Pipeline (Embedded)



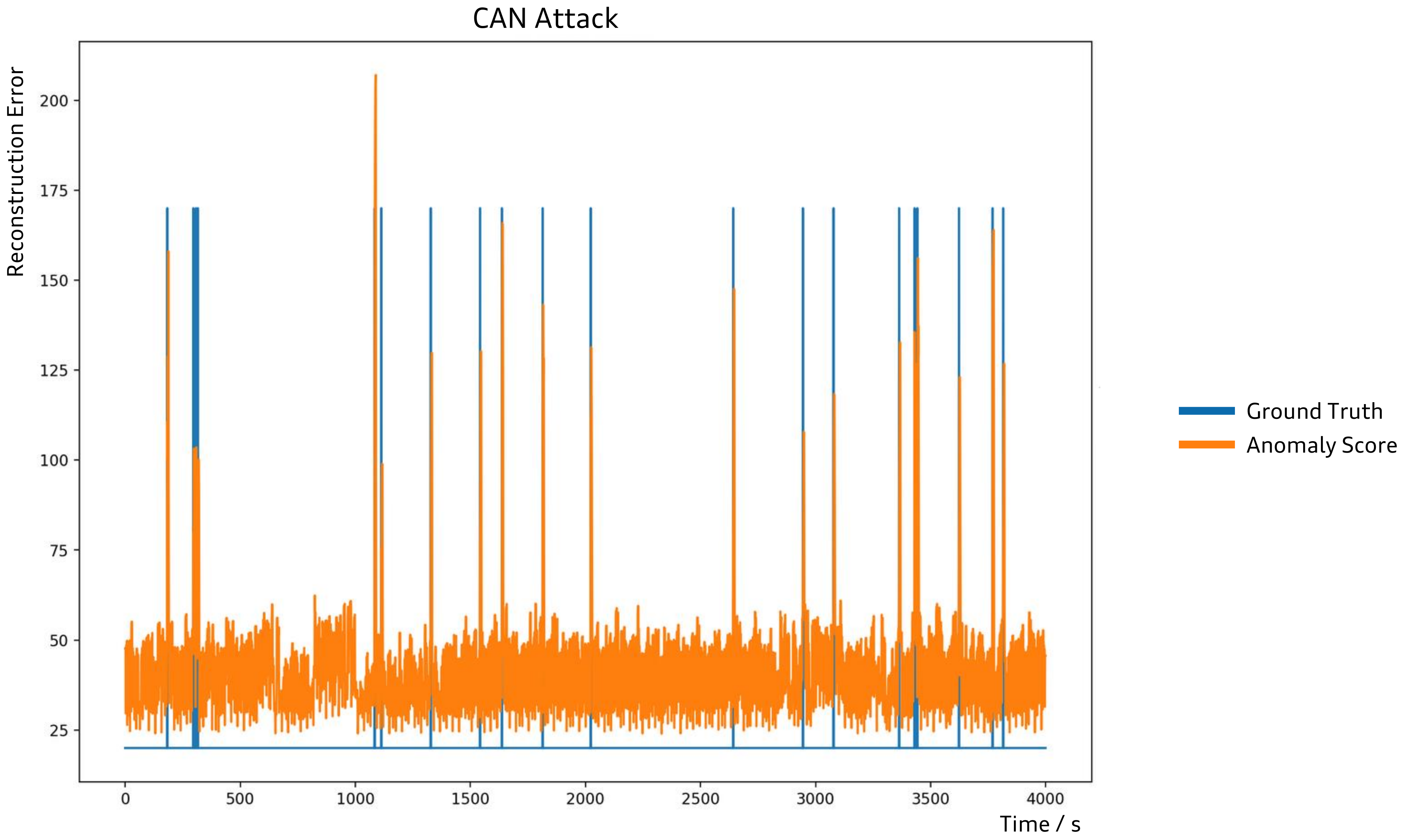


Results

CAN Anomaly

Results

Payload Fuzzing



Summary

Wrapping Up

Summary

- Intrusion Detection Systems are necessary in future automotive systems:
  - To detect unknown malicious attacks
  - Norms and regulations (UNECE WP 29)
- For the automotive domain no databases with malware (binaries and communication) exists
- A data-driven approach based on Machine Learning (ML) can detect unknown attacks
- Anomaly detection is a ML technique which requires only data/traffic from the normal case (no labeling needed)
- Embedded implementation requires thoughtful algorithm selection

- Contact:

Dr.-Ing. Andreas Weichslgartner
Audi Electronics Venture GmbH
andreas.weichslgartner@audi.de

Audi Electronics Venture