Machine-Learning Methods for In-Vehicle Intrusion Detection

Roland Rieke

The 4th International Workshop on Safety, securiTy, and pRivacy In automotiVe systEms
6th of September, 2021 - Wien, Austria

Overview

- Evolution of Vehicles & Attack Surface
- Anomaly Detection
- Datasets
- Comparing Approaches
- Understanding Results
- Automotive Ethernet
- Machine Learning for Rule Engineering
- Evaluation Platform
- Collaborative Risk Perception
- Vision

Horse & Hardware Defined Vehicles

- Challenge 1898: Growing crisis posed by urban horses & their output
- London 1900: > 50.000 horses
- London Times 1894: in 50 years streets buried under 9 feet of manure

"If I had asked people what they wanted,

they would have said faster horses."

Henry Ford

- Attacks on HW:
  - Steal vehicle; Speedometer manipulation

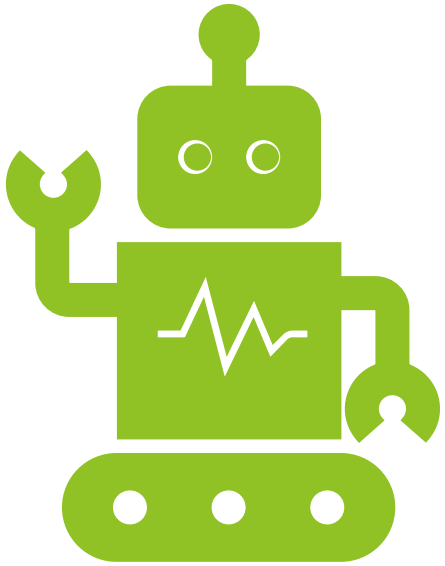
Software Defined Vehicles

- 100 Mio lines of code
- CAN replaced by Automotive Eth.
- Growing network dependency V2X
- Plug to Charge & Billing

“Once you add a Web browser to a car, It's over,”
Charlie Miller, Black Hat 2014

Transportation & Mobility as a Service

- AI decision making proesses
- Safety by V2X Collaboration
- System of Systems Infrastructure



“Data can be converted into information that fuels human and AI decision-making processes, which in turn enable self-driving cars, ...”

George Firican, 2019

Attacks on Networked Vehicles

- A whitepaper from Trend Micro derived a generic attack chain from four attacks: **Jeep hack** of 2015, **TESLA hacks** of 2016 and 2017, and **BMW hack** of 2018.
- Some steps also match other attacks such as a **hack on KIA Cee'd** head unit in 2020, and the **TBONE Tesla hack** 2021.
- **Step 9 could be detected and reported by a network-based IDS.**
- The NIDS can be part of cooperative in-vehicle IDS (cf. AUTOSAR) comprising IDS manager, IDS reporter as well as NIDS and HIDS instances.

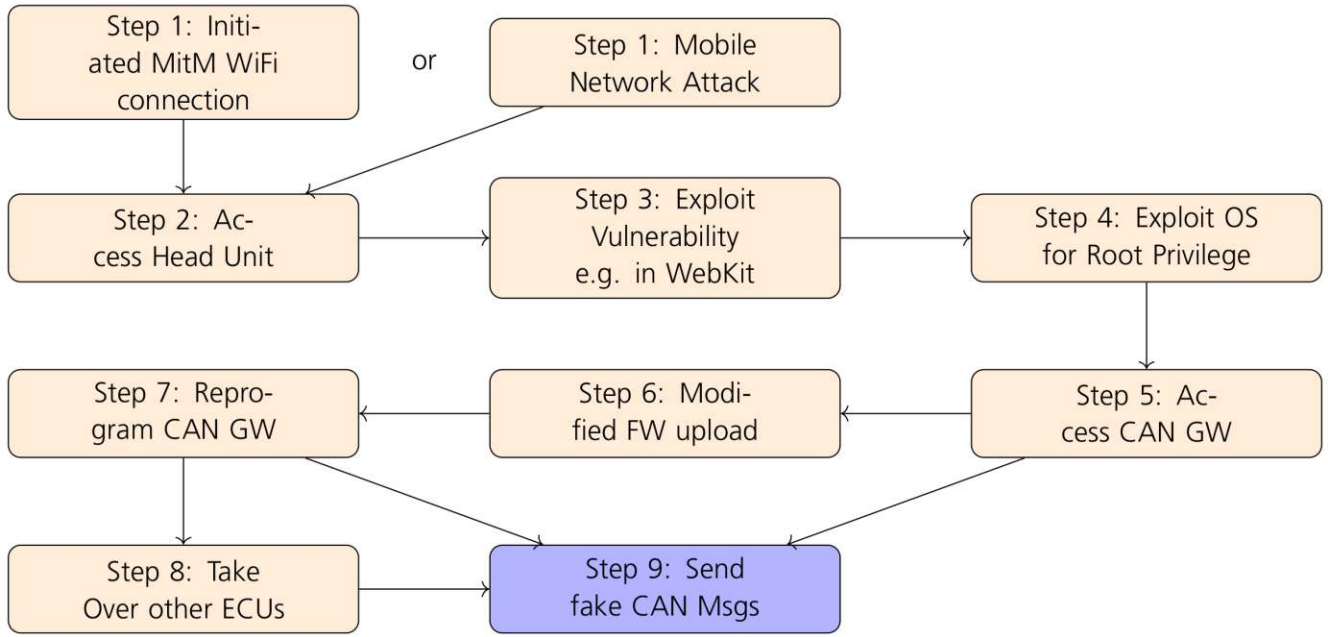


Figure based on: Numaan Huq, Craig Gibson, and Rainer Vosseler. Driving Security Into Connected Cars: Threat Model and Recommendations. Trend Micro Research, 2020.

UN Regulations

UN Regulation No. 155:

Uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system

- Demonstrate that supplier-related risks are identified and are managed.
- Document risks assessment, test results and mitigations applied to the vehicle type.
- Implement appropriate cyber security measures in the design of the vehicle type.
- ***Detect and respond to possible cyber security attacks.***
- Log data to support the detection of cyber-attacks and provide data forensic capability.

UN Regulation No. 156:

Uniform provisions concerning the approval of vehicles with regards to software update and software updates management system

Plappert, Zelle, Gadacz, Rieke, Scheuermann, Krauß:
Attack Surface Assessment for Cybersecurity Engineering in the Automotive Domain, PDP2021

Unsupervised Anomaly Detection

Identify instances that fit least to the remainder

- Automatic identification of unknown anomalies
- Adaptation to different systems
- No mapping of anomalies to attacks

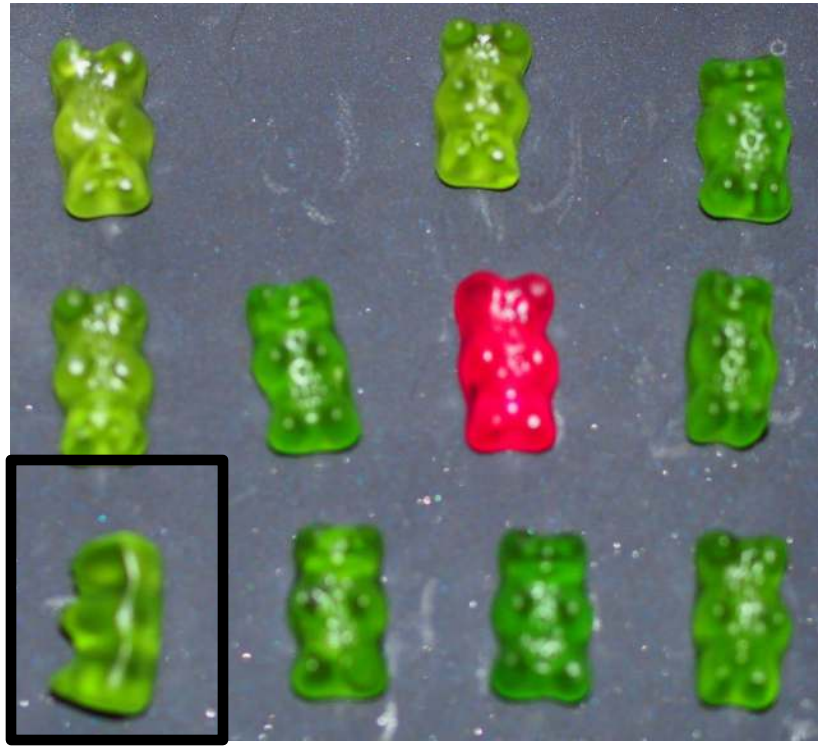
color

Supervised Anomaly/Attack Detection

Extract features that differentiate labelled data

- Learning set must be prepared
- Different types of anomalies/attacks
- Only works on systems represented by learning set

Normal: item lies on its back
Intrusion: color = red



Specification-based Detection

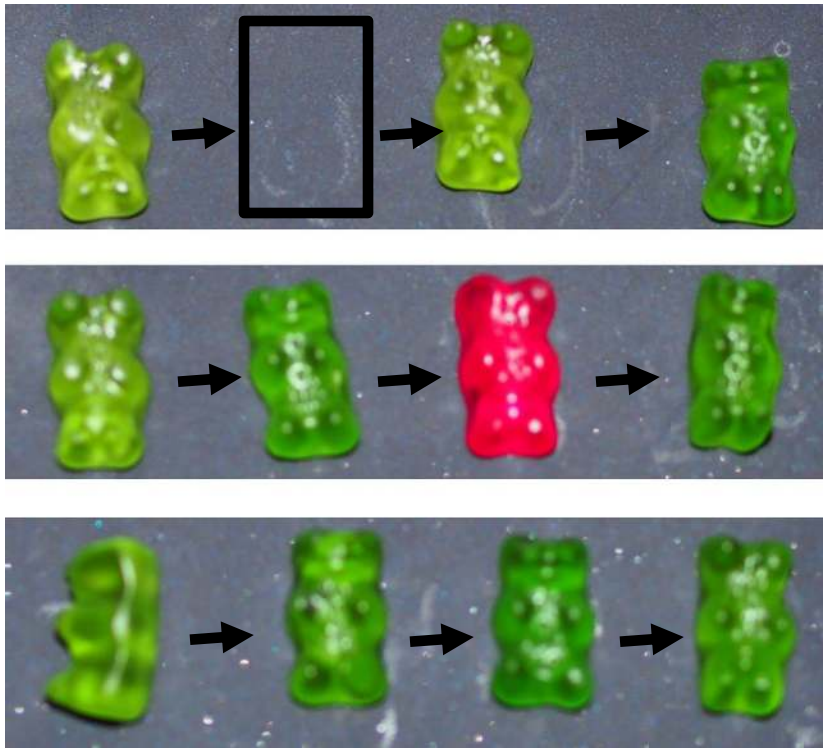
Construct a model for normal behavior

- Traceability of classification
- No mapping of anomalies to attacks

Specify model of abnormal behavior

- Mapping of anomalies to attacks, e.g. signature-based

sensor data is sent every 100ms



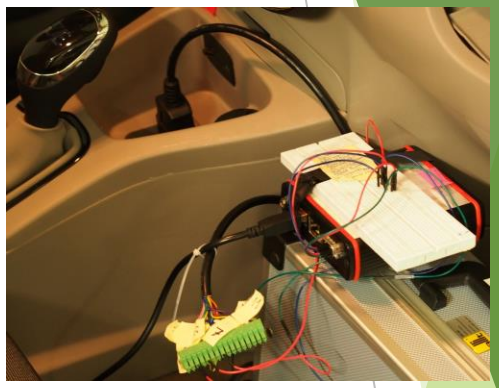
Behavior-based Anomaly Detection

Set of possible sequences of actions

- Identify missing events
- Identify attack patterns
- High cost and complexity

Application Scenario & Datasets

- **Renault ZOE**
  - Urban driving, >1 million messages
  - Artificially introduced intrusions
  - **Fuzzing** & **DoS** intrusions
  - Spoofing **Speedometer** & **RPM** values
- **Model X**
  - Urban driving, 2.5 million messages
  - Synthetic **fuzzing** attack
- **HCRL Car Hacking**
  - Open Access, ~4 million messages
  - Spoofing attacks on **driving gear** & **RPM**
  - https://ocslab.hksecurity.net/Datasets/CAN-intrusion-dataset
- **ORNL**
  - Open access, actively driven on dynamometer
  - 33 attack captures
  - https://0xsam.com/road/



Byte	8	8	8	8	8	8	8	8
FC	5	11	16		5	7	6	5	9
DBC	16		28				6*	5	9*

CAN field structure analysis

Intrusion Design

Denial of Service (*U/DoS*)

- Insertion of messages with all zero payload

Fuzzing (*U/Fuzzy*)

- Insertion of messages with randomized payload

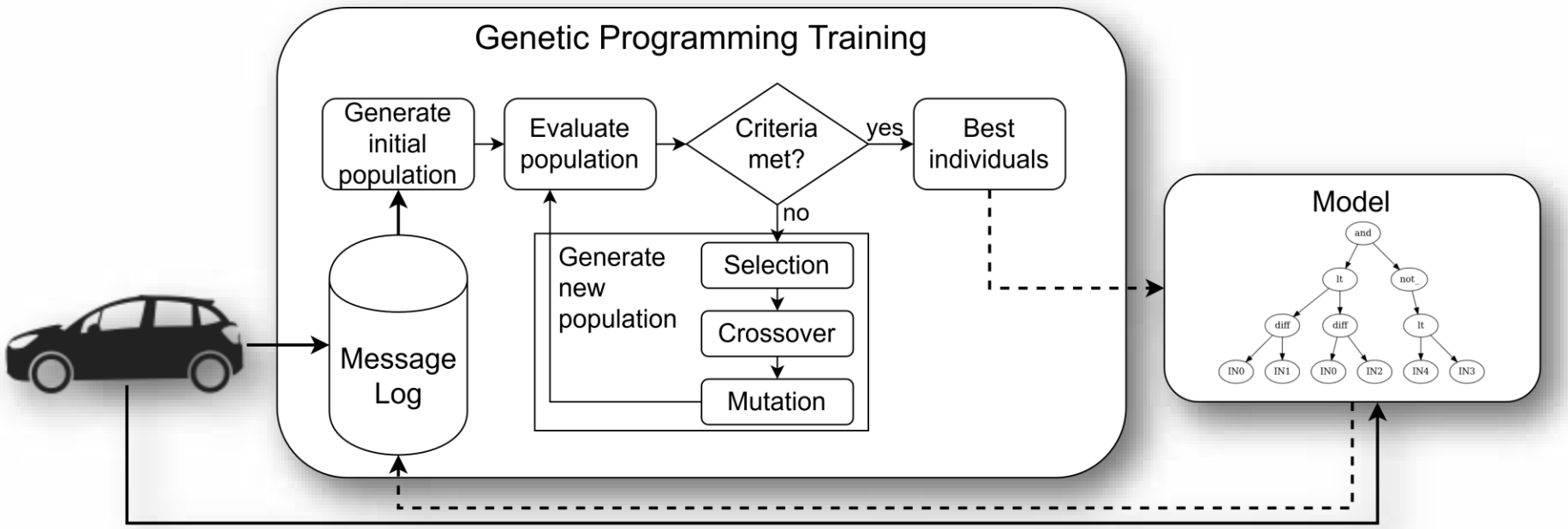
Spoofing of Revolutions per Minute (*U/RPM_LEFT*)

- Set values for the revolutions per minute to zero for only the left frontal wheel
- Can be detected by finding correlation to right frontal wheel

Spoofing of Speedometer (*U/SPEED*)

- Set values for speedometer to zero
- Can be detected by observing changes in vehicles travelled distance value

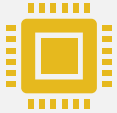
Genetic Programming Workflow



Genetic Programming and other Approaches

Artificial neural networks (ANN)

Implementation with Tensorflow
Binary classification
Designed to be small and fast in embedded environment
Limited insight in decision



Characteristic Functions (CF)

Rule-based Intrusion Detection System
Designed for embedded systems
Fast
Explainable

Genetic Programming (GP)

GP models may prove to be …
- … dynamically adaptable to new situations
- … more comprehensive for humans
- … able to find complex relations within data

Results from Selected Approaches

Genetic Programming (GP)

- Fast, but inferior at DoS Intrusions
- *U/Speed shows capability of detecting complex relations*

Characteristic Functions (CF)

- Fast, excels at DoS intrusions

Artificial Neural Networks (ANN)

- Solid results for DoS, but complex relations are often disregarded
- *High performance* requirements

	GP-FC			GP-BA			ANN-BA			CF-BA		
Log file	ACC	PPV	TPR	ACC	PPV	TPR	ACC	PPV	TPR	ACC	PPV	TPR
U/Fuzzy'	.952	.769	.994	.990	.982	.958	.999	.999	**1**	**1**	**1**	**1**
U/Dos'	.921	.946	.528	.905	.625	**1**	.941	.986	.634	.999	.997	.997
U/RPM_LEFT'	.914	.800	.115	.998	.980	**1**	.984	.998	.826	.839	.366	**1**
U/Fuzzy"	.981	.963	.999	.995	.997	.992	.999	**1**	.999	**1**	**1**	**1**
U/DoS"	.499	.201	.012	.904	.834	**1**	.942	.986	**1**	**1**	**1**	**1**
U/SPEED"	.957	.716	.894	.906	**0**	**0**	.906	–	**0**	.186	**0**	**0**
Model_X	**1**	**1**	**1**	.998	.998	.994	Not measured			Not measured		
HCRL/RPM	.901	.892	**1**	.910	.891	**1**						
HCRL/Gear	.912	.901	**1**	.914	.897	**1**						

Denial of Service (*U/DoS*): Insertion of messages with all zero payload

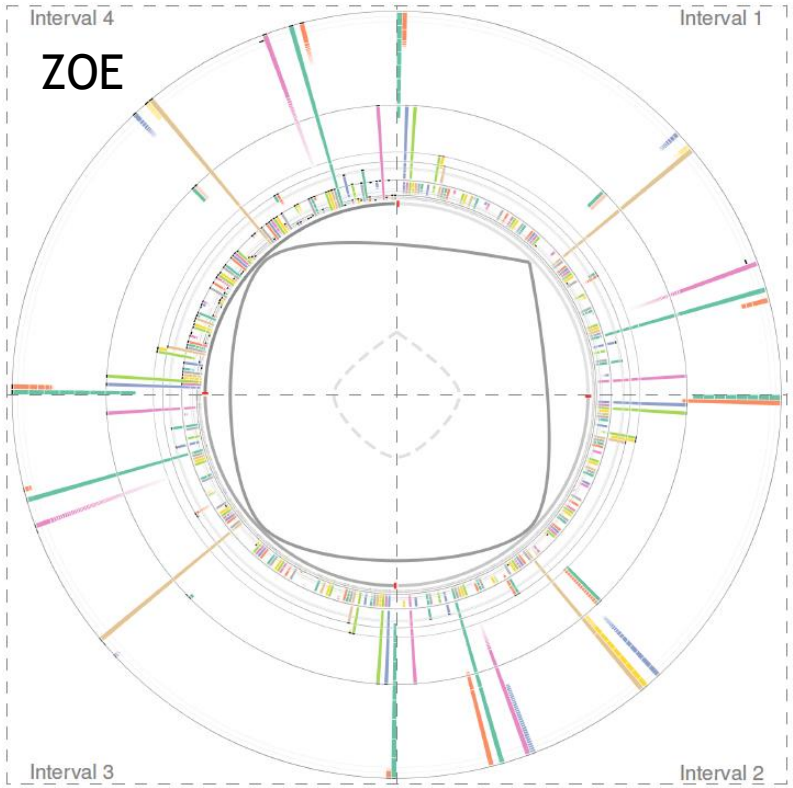
Fuzzing (*U/Fuzzy*): Insertion of messages with randomized payload

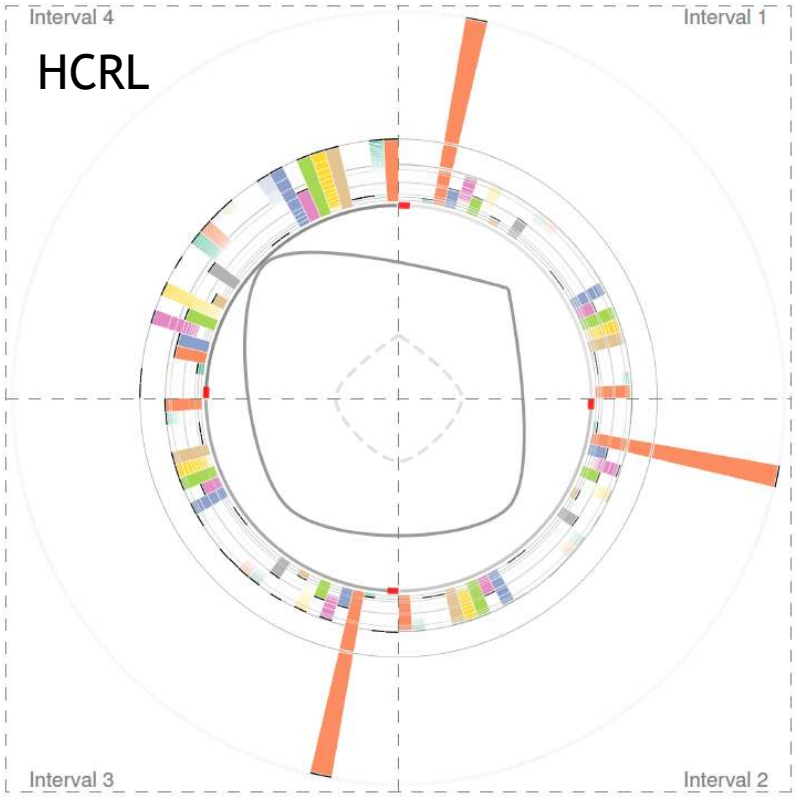
Spoofing of Revolutions per Minute (*U/RPM_LEFT*): Set revolutions to 0 for left front wheel; detect by correlation to right front wheel

Spoofing of Speedometer (*U/SPEED*): Set speedometer to 0; detect by observing changes in vehicles travelled distance

Florian Fenzl, Roland Rieke, Andreas Dominik: *In-vehicle detection of targeted CAN bus attacks*, ARES2021.

Understanding Data and Results





Y. Chavalier, F. Fenzl, M. Kolomeets, R. Rieke, A. Chechulin, C. Krauß: *Cyberattack detection in vehicles using characteristic functions, artificial neural networks and visual analysis*, Journal of Informatics and Automation (SPIIRAS Proceedings), 2021

Automotive Ethernet

```
time,     ID,  len, p1,  p2,  p3,  p4,  p5,  p6,  p7,  p8,  type
...
0.045838, 382, 8,   255, 255, 255, 0,   255, 64,  0,   255, 1
0.046024, 951, 5,   255, 255, 90,  15,  254, 108, 117, 118, 1
0.04625,  390, 7,   0,   0,   50,  3,   32,  0,   32,  118, 1
0.047303, 697, 3,   68,  135, 0,   109, 112, 108, 117, 118, 1
0.048409, 302, 8,   199, 127, 255, 127, 224, 255, 255, 0,   1
0.048653, 666, 8,   0,   0,   0,   0,   0,   0,   10,  245, 1
```

CAN

Time	Chn	Dir	Protocol	Source IP	Destination IP	Name	Protocol Info
3.465829	Eth 2	Tx	someip	192.168.2.3	239.192.255.251		
3.465829	Eth 2	Tx	someip	192.168.2.3	239.192.255.251	Special::ServiceDiscovery	SOME/IP-SD: Offer Service
Offer Service				Service 000A		Version 1.0	Instance 1 192.168.2.3:C352 UDP
3.477780	Eth 2	Rx	someip	192.168.2.4	239.192.255.251		
3.477780	Eth 2	Rx	someip	192.168.2.4	239.192.255.251	Special::ServiceDiscovery	SOME/IP-SD: Stop Offer Service
Stop Offer Service				Service 000A		Version 1.0	Instance 1 192.168.2.3:C352 UDP
3.489366	Eth 2	Rx	someip	192.168.2.4	239.192.255.251		
3.489366	Eth 2	Rx	someip	192.168.2.4	239.192.255.251	Special::ServiceDiscovery	SOME/IP-SD: Offer Service
Offer Service				Service 000A		Version 1.0	Instance 1 192.168.2.4:C352 UDP
3.507624	Eth 2	Tx	someip	192.168.2.2	192.168.2.4		
3.507624	Eth 2	Tx	someip	192.168.2.2	192.168.2.4	Special::ServiceDiscovery	SOME/IP-SD: Subscribe Eventgroup
Subscribe Eventgroup				Service 000A	Eventgroup 0001	Version 1	Instance 1 192.168.2.2:C352 UDP
3.521534	Eth 2	Rx	someip	192.168.2.4	192.168.2.3		
3.521534	Eth 2	Rx	someip	192.168.2.4	192.168.2.3	Special::ServiceDiscovery	SOME/IP-SD: Stop Subscribe Eventgroup
Stop Subscribe Eventgroup				Service 000A	Eventgroup 0001	Version 1	Instance 1 192.168.2.2:C352 UDP
3.534297	Eth 2	Rx	someip	192.168.2.4	192.168.2.3		
3.534297	Eth 2	Rx	someip	192.168.2.4	192.168.2.3	Special::ServiceDiscovery	SOME/IP-SD: Subscribe Eventgroup
Subscribe Eventgroup				Service 000A	Eventgroup 0001	Version 1	Instance 1 192.168.2.4:C352 UDP
3.535240	Eth 2	Tx	someip	192.168.2.3	192.168.2.4		
3.535240	Eth 2	Tx	someip	192.168.2.3	192.168.2.4	Special::ServiceDiscovery	SOME/IP-SD: Subscribe Eventgroup Acknowledgment
Subscribe Eventgroup Acknowledgment				Service 000A	Eventgroup 0001	Version 1	Instance 1
3.551468	Eth 2	Rx	someip	192.168.2.4	192.168.2.2		
3.551468	Eth 2	Rx	someip	192.168.2.4	192.168.2.2	Special::ServiceDiscovery	SOME/IP-SD: Subscribe Eventgroup Acknowledgment
Subscribe Eventgroup Acknowledgment				Service 000A	Eventgroup 0001	Version 1	Instance 1
4.000354	Eth 2	Tx	udp	192.168.2.3	192.168.2.2		C352 -> C352
4.000362	Eth 2	Tx	udp	192.168.2.3	192.168.2.4		C352 -> C352
4.009039	Eth 2	Rx	udp	192.168.2.4	192.168.2.2		C352 -> C352
4.465838	Eth 2	Tx	someip	192.168.2.3	239.192.255.251		

DoIP: Diagnostics over Internet Protocol

SOME/IP: Scalable Service-Oriented Middleware over IP

D. Zelle, T. Lauser, D. Kern, C. Krauß: Analyzing and Securing SOME/IP Automotive Services with Formal and Practical Methods, ARES 2021 best paper.

Hybrid ML for Rule Generation

Rule-based *Detector*

- *main component active in detecting **attacks***

Rule Generator

- reates reliable and traceable rules for the rule-based detector based on shallow ML techniques

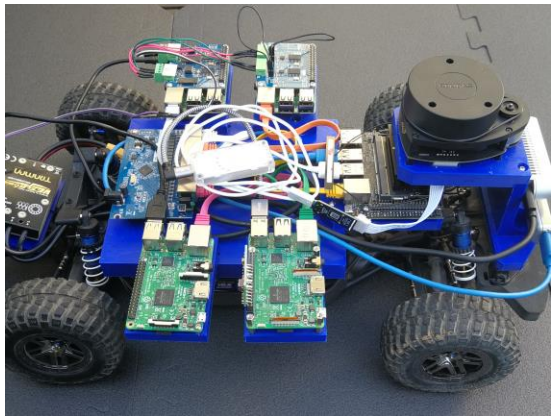
Anomaly Detector

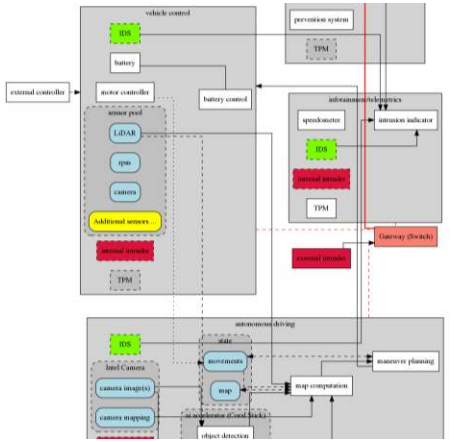
- extends the data set available to the rule generator

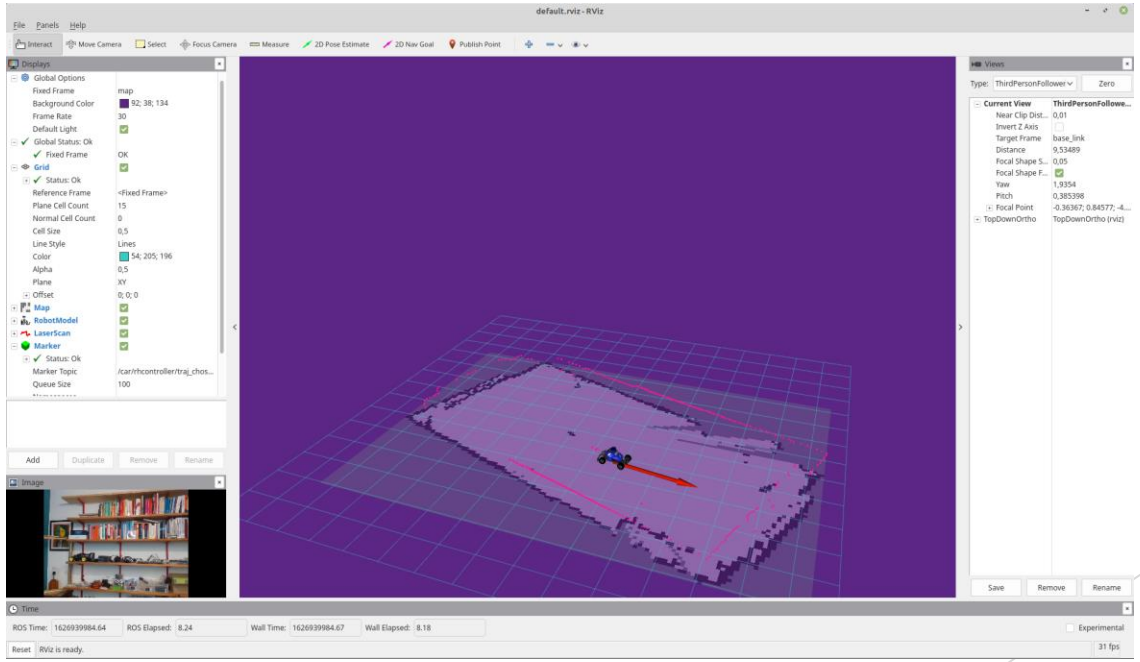
Traffic Logger

- records all traffic within the operating environment

Security Evaluation Platform



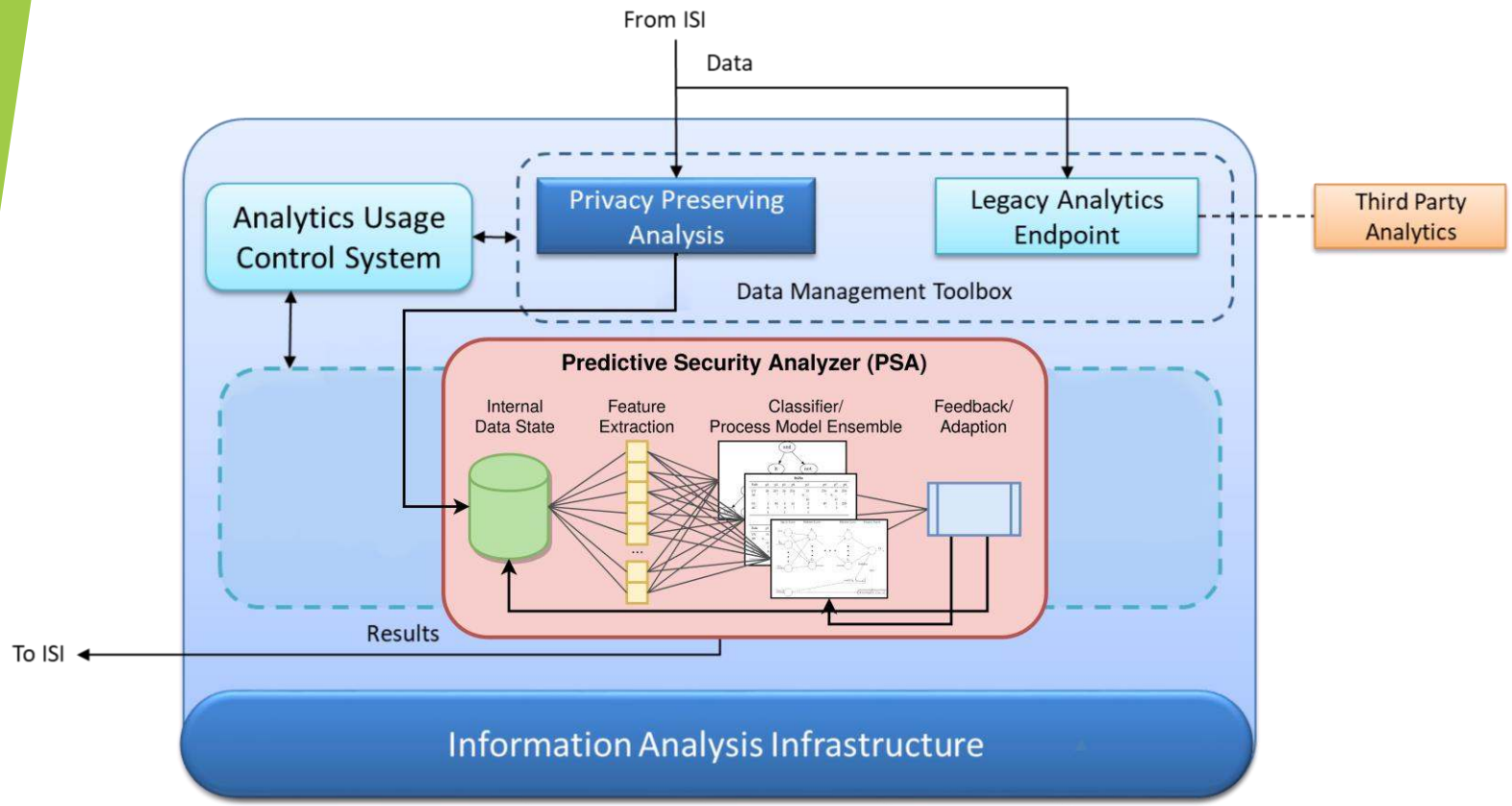


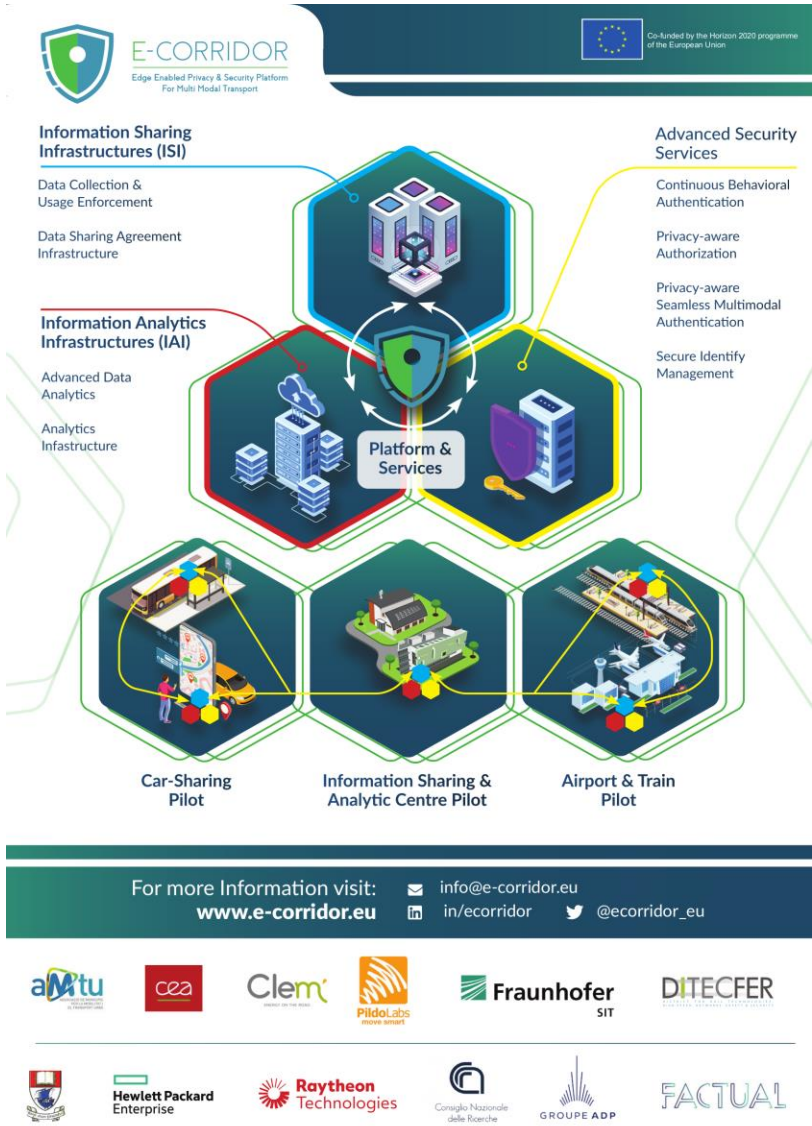


- Mostly harmless
- Distributed collaborative IDPS
- Test security by design (TPM)
- Evaluate new Automotive Ethernet protocols
- Forensic

https://www.athene-center.de/en/research/research-areas/sad

Integration into Edge-enabled Information Sharing, Analysis and Protection Framework

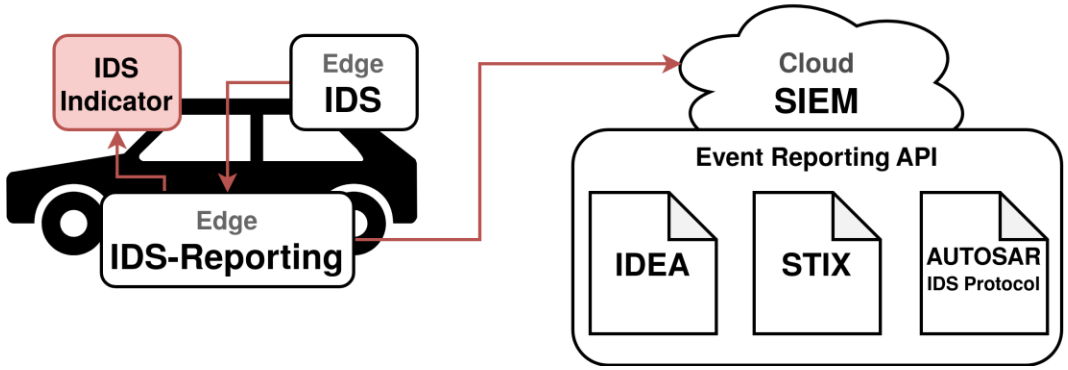




Roland Rieke, STRIVE2021

Actionable Reporting

Challenge: Transfer results into actionable reports




```
{
    "Format": "IDEA0",
    "ID": "3ad275e3-559a-45c0-8299-6807148ce157",
    "DetectTime": "2021-01-08T11:00:00Z",
    "Category": "Anomaly.Behaviour",
    "Description": "VAL_TOO_HIGH",
    "Confidence": 0.86,
    "Target": [
        {
            "Proto": ["can"],
            "Spoofed": true,
            "ASN": 768
        }
    ],
    "Attach": [
        {
            "Type": "MessageLog",
            "ContentType": "text/plain",
            "Content": "binary_blob (last seen messages)"
        }
    ]
}
```

IDEA (Intrusion Detection Extensible Alert)
https://idea.cesnet.cz/en/definition
STIX (Structured Threat Information eXpression)
https://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html
AUTOSAR IDS Protocol
https://www.autosar.org/fileadmin/user_upload/standards/foundation/20-11/AUTOSAR_PRS_IntrusionDetectionSystem.pdf

Future Work

Genetic Programming for IDS

- Good detection of relationships between fields
- *Denial of Service* results dependent on data
- Only slight improvment over ANN results
- Computationally performant during classification

Random Forest approach

- Train multiple smaller decision trees with GP
- Majority voting
- Potentially using different payload alignments

Hybrid approach

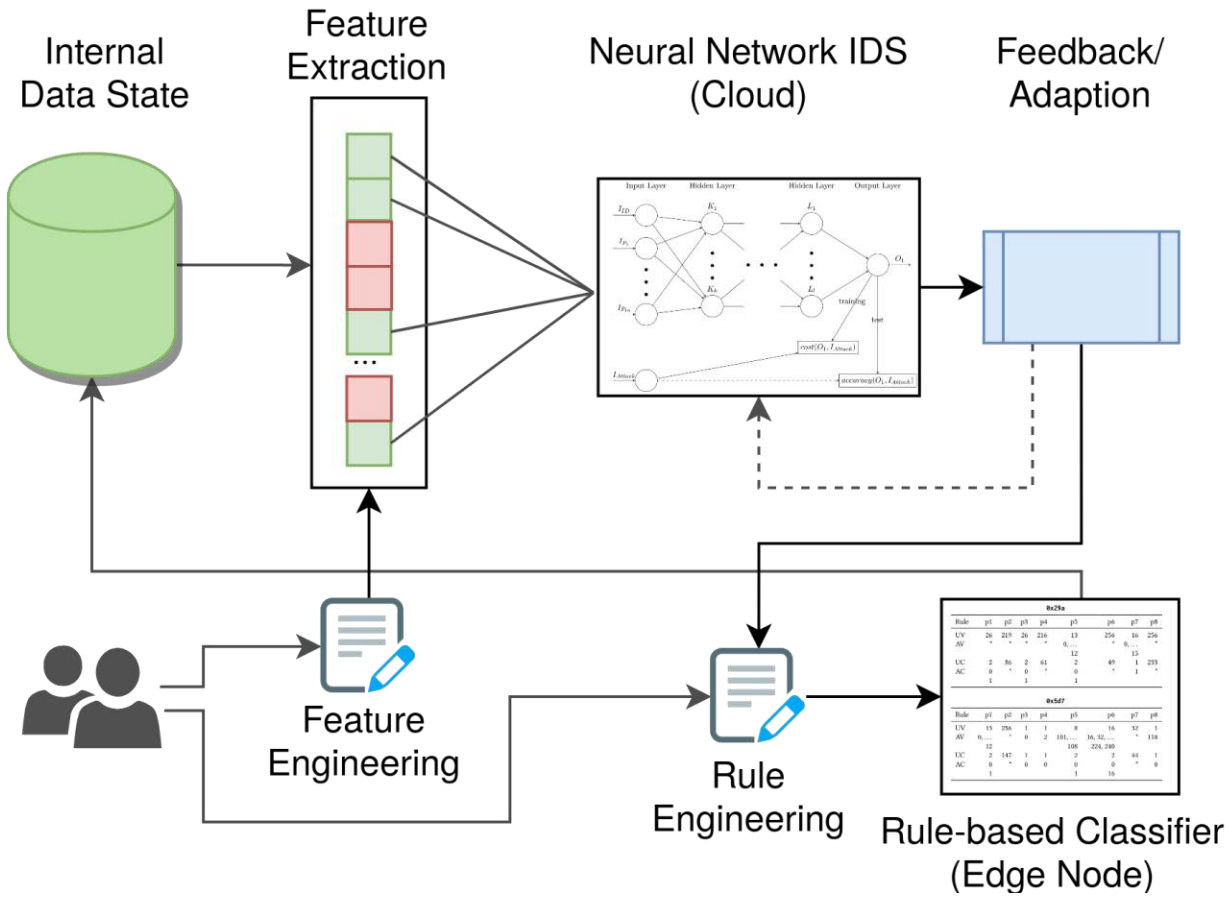
- *Characteristic functions* for boundary detection
- *Genetic Programming* for detecting relationships
- Either in sequence or with majority voting

	Genetic Programming	Deep Neural Networks	Characteristic Functions
Detect DoS	0	0	+
Detect Manipulation	+	+	-
Detect Field Correlation	+	0	-
Time: Training Classification (msg/s)	- + (735)	0 - (140)	+ ++ (1674)
Explainability & actionable reports	+	-	+

VISION

"One employs it (ML) not to ultimately detect malicious activity, but rather to understand the significance of the different features of benign and malicious activity, which then eventually serve as the basis for a non-machine-learning detector." *Robin Sommer; Vern Paxson*

- Feature engineering (abstract view)
- Feature configuration (optimization)
- Privacy preserving edge monitoring
- ML training (ANN / LSTM)
- ML-based classification (SoS level)
- Feedback adaptation
- ML supported rule engineering (decision tree / genetic programming)
- Rule/Model transfer to edge
- Rule-based classification
- Semantic interpretation and reporting



Publications

https://rieke.link

Florian Fenzl, Roland Rieke, and Andreas Dominik,
In-vehicle detection of targeted CAN bus attacks, ARES2021

Yannick Chevalier, Florian Fenzl, Maxim Kolomeets, Roland Rieke, Andrey Chechulin, and Christoph Krauß,
Cyberattack detection in vehicles using characteristic functions, artificial neural networks and visual analysis,
Journal of Informatics and Automation (SPIIRAS Proceedings), 2021

Christian Plappert, Daniel Zelle, Henry Gadacz, Roland Rieke, Dirk Scheuermann, and Christoph Krauß,
Attack Surface Assessment for Cybersecurity Engineering in the Automotive Domain, PDP2021.

Florian Fenzl, Roland Rieke, Yannick Chevalier, Andreas Dominik, and Igor Kotenko,
Continuous Fields: Enhanced In-Vehicle Anomaly Detection using Machine Learning Models, Elsevier Journal, 2020.

Roland Rieke, Florian Fenzl, Daniel Zelle, Wei Zhuo, Rehana Yasmin,
ATICME - Adaptive Time Interval Classification MEthod for optimization of machine learning based anomaly detection and intrusion detection.
Patent application number: PCT/CN2020/087711

Daniel Zelle, Roland Rieke, Christian Plappert, Christoph Krauß, Dmitry Levshun, and Andrey Chechulin (2020),
SEPAD - Security Evaluation Platform for Autonomous Driving, PDP2020.

Yannick Chevalier, Roland Rieke, Florian Fenzl, Andrey Chechulin, and Igor Kotenko,
ECU-Secure: Characteristic Functions for In-Vehicle Intrusion Detection,IDC2019, Springer SCI, volume 868.

Ivo Berger, Roland Rieke, Maxim Kolomeets, Andrey Chechulin, and Igor Kotenko,
Comparative study of machine learning methods for in-vehicle intrusion detection, ESORICS 2018 WS, Springer LNCS 11387

Roland Rieke, Marc Seidemann, Elise Kengni Talla, Daniel Zelle, and Bernhard Seeger,
Behavior Analysis for Safety and Security in Automotive Systems, PDP 2017.