Scission: Signal Characteristic-Based Sender Identification and Intrusion Detection in Automotive Networks

1st ITG Workshop on IT Security (ITSec)
University of Tübingen
April 2, 2020

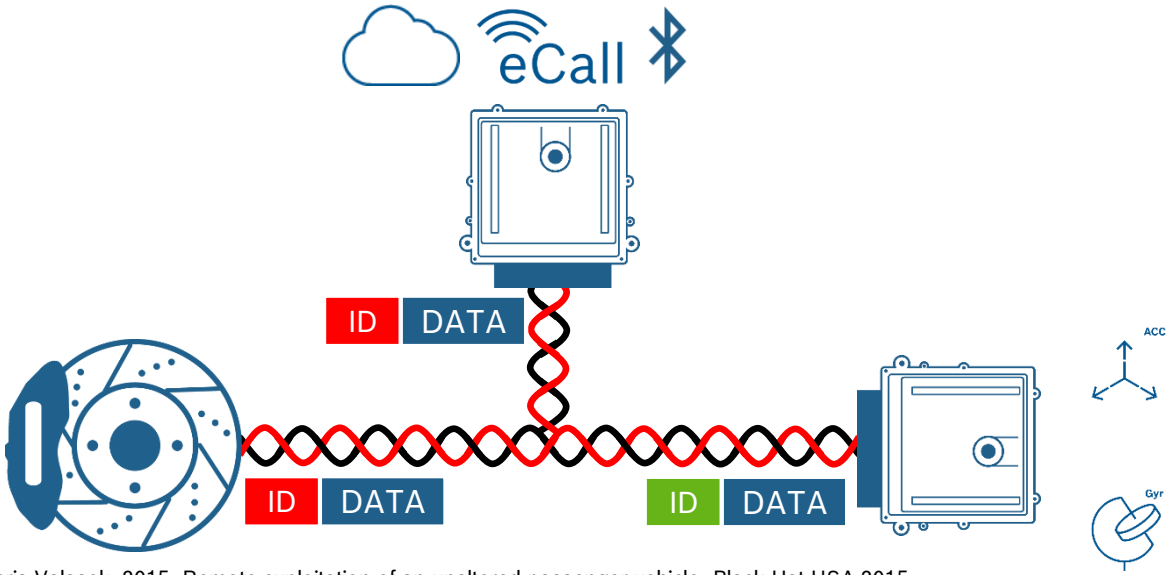
Marcel Kneib[1], Christopher Huth[2], Paul Duplys[2]

[1] Bosch Engineering GmbH,
[2] Robert Bosch GmbH

BOSCH

Introduction

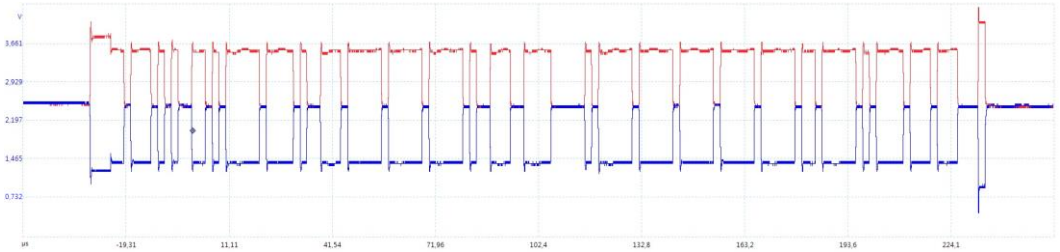
- Attacks on vehicles…
  - on the rise due to increased connectivity features
  - may be highly scalable
  - result in threats for humans and the environment
- Demonstrated by Miller and Valasek [31]



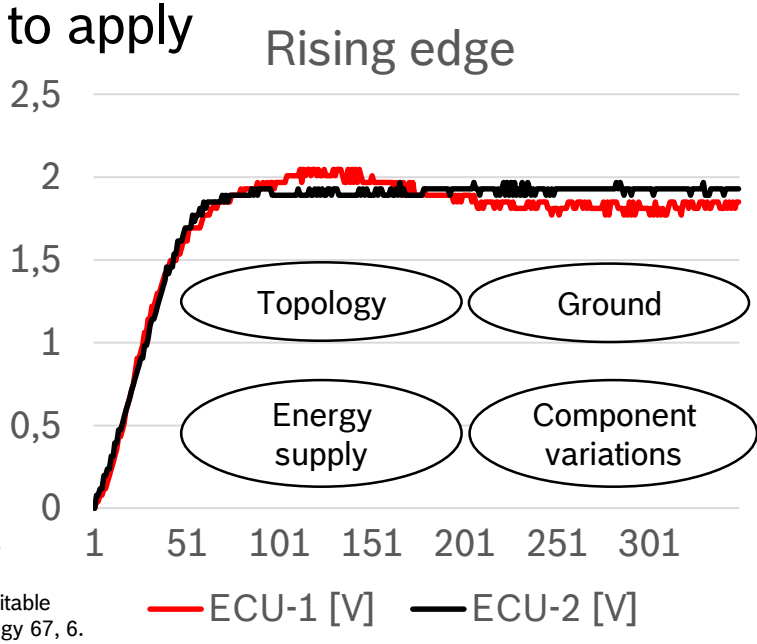
[31] Charlie Miller and Chris Valasek. 2015. Remote exploitation of an unaltered passenger vehicle. Black Hat USA 2015

Introduction

- Controller Area Network widely used for in-vehicle communication
  - 500 kb/s bandwidth
  - 64 bit payload
  - No sender authenticity



- Message Authentication Codes hard to apply
- Intrusion Detection Systems
  - Signatures
  - Anomalies
  - Physical properties
    - Clock drifts [4]
    - **Variations in the analog signal** [33, 6]



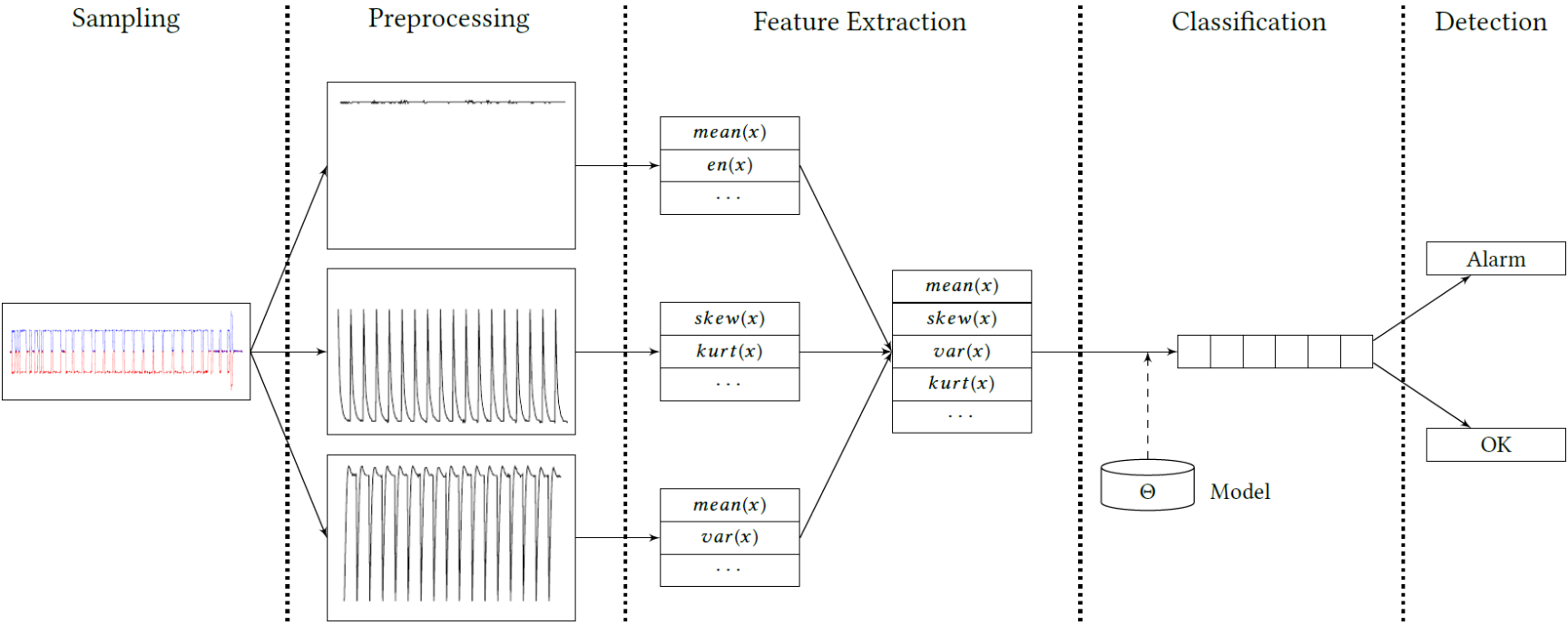
[4] Kyong-Tak Cho and Kang G. Shin. 2016. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. In 25th USENIX Security Symposium.

[33] P. S. Murvay and B. Groza. 2014. Source Identification Using Signal Characteristics in Controller Area Networks. IEEE Signal Processing Letters 21.

[6] W. Choi, H. J. Jo, S. Woo, J. Y. Chun, J. Park, and D. H. Lee. 2018. Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks. IEEE Transactions on Vehicular Technology 67, 6.

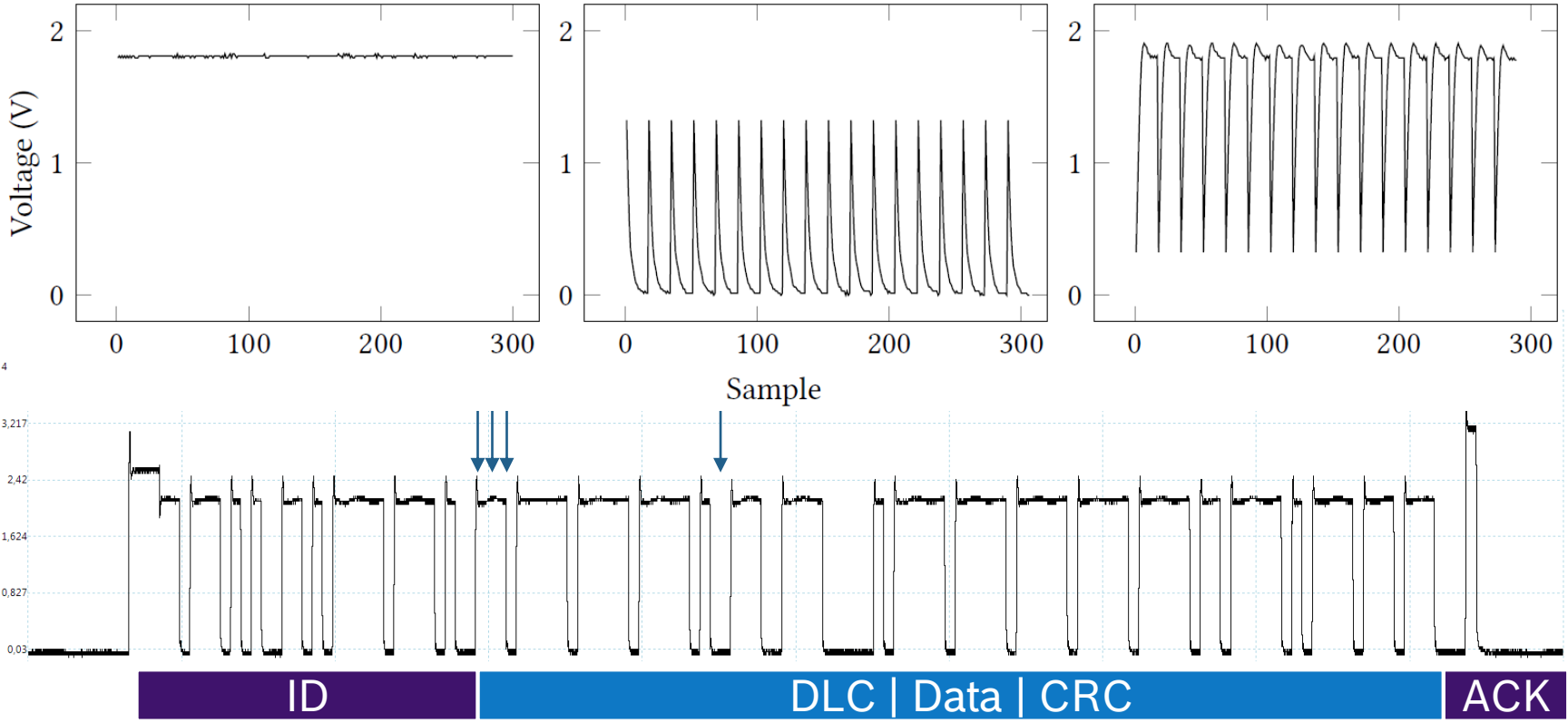
BOSCH

Scission Overview



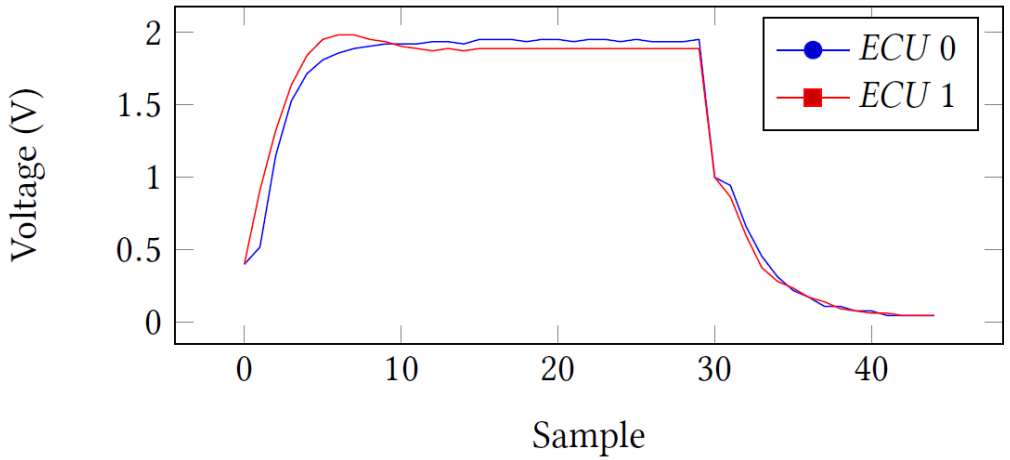
Sampling and Preprocessing

- Sampling differential signal (20 MS/s)
- Cluster symbols based on its signal shape



Feature Selection

- Statistical features (time, frequency) individual for each group
  - Mean, Standard Deviation, Variance, Skewness, ...



	Concatenated	Rising	Falling	High
ECU 0	1.286 V	1.623 V	0.289 V	1.947 V
ECU 1	1.285 V	1.691 V	0.275 V	1.890 V
Difference	0.001 V	0.068 V	0.014 V	0.057 V

Model Generation and Classification

- Logistic Regression

ECU 0	ECU 1	ECU2
95 %	3 %	2 %

- Supervised learning with 200 frames per ECU

- Initial training in safe environment
  - Initiated by secure diagnostic access
  - Key between ECUs and Scission assigned

- Performance Monitoring (aging, corrosion, ...)
  - Probabilities of each ECU
  - Online adaption of the classifiers
  - MAC supported adaption/learning
    - AUTOSAR Secure Onboard Communication (SecOC)

Intrusion Detection

- Sender identification based on the highest probability

ECU 0	ECU 1	ECU2
95 %	3 %	2 %
2 %	**98 %**	0 %
49.9 %	50.1 %	0 %

- In-vehicle communication is static
  - Each identifier is used by only one ECU
  - Alarm if an identifier is used by a invalid ECU

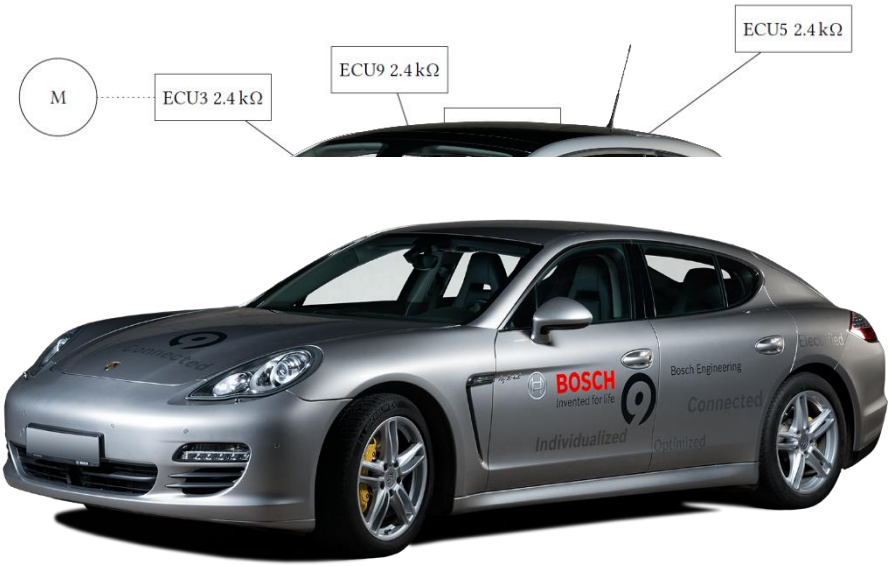
- False positives
  - Due to interferences (start of a strong consumer)
  - Alarm if probability of invalid ECU exceeds threshold t_{max} (e.g. 70 %)
  - Leads to a higher false negative rate

Evaluation

	ECUs	Frames	Avg. accuracy	Min. accuracy
Prototype	10	56,560	99.9 %	99.58 %
Fiat	6+2	25,979	99.6 %	98.56 %
Porsche	6+2	6,389	99.88 %	99.58 %

▶ 99.85% Identification rate → FP after 666 frames → threshold t_{max}

		Predicted	
		No attack	**Attack**
Prototype	**No attack**	100 %	**0 %**
	Attack	1.5 %	98.5 %
Fiat	**No attack**	100 %	**0 %**
	Attack	0 %	100 %
Porsche	**No attack**	100 %	**0 %**
	Attack	3.18 %	96.82 %



Conclusion

- Sender identification based on physical properties of CAN signals
- Reduction in the necessary hardware requirements
- Evaluated on series production vehicles
  - High identification rate
  - No false positives
- Scission can improve the security of modern vehicles
  - IDS extension
  - Additional security functionality for gateways
  - Standalone system
- Outlook
  - Further reduction of hardware/performance requirements
  - Implementation on an embedded platform

THANK YOU!

Marcel.Kneib@de.bosch.com

Christopher.huth@de.bosch.com

Stability

- Characteristics remain unchanged over several months [33]

- Fiat under changing conditions
  1. Measurement (includes training)
     - Engine off | 25°C (77°F) | 3369 frames | 100% identification
  2. Measurement
     - Driving 30 min. | 32°C (89.6°F) | 6672 frames | 100% identification
  3. Measurement (3 hours of cooling at 23°C (73.4°F))
     - Driving 20 min. | 36°C (96.6°F) | 4863 frames | 100% identification

- Biggest change in the voltage level between 0.012V and 0.026V

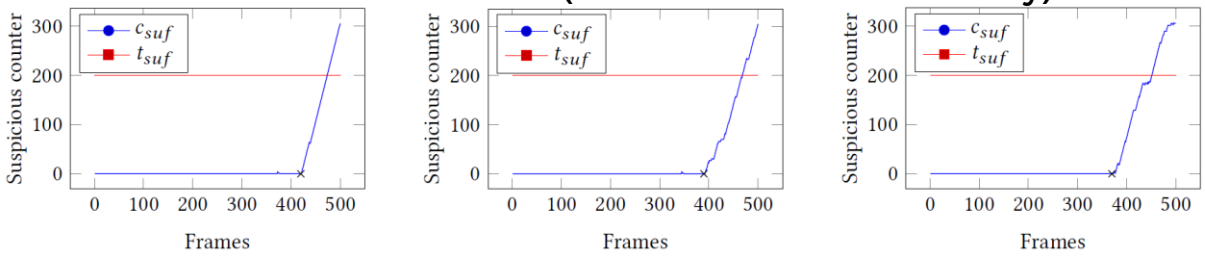
[33] P. S. Murvay and B. Groza. 2014. Source Identification Using Signal Characteristics in Controller Area Networks. IEEE Signal Processing Letters 21.

Reaction on intrusion

- Warn the driver
- Log the attack
- Prevent the attack
  - Invalidation of the CRC
  - Error Frame
- Send the detected attack to Cloud-IDS
  1. Analyze the attack
  2. Update the in-vehicle Signature-based IDS
  3. Find the vulnerability
  4. Update the vulnerable ECU

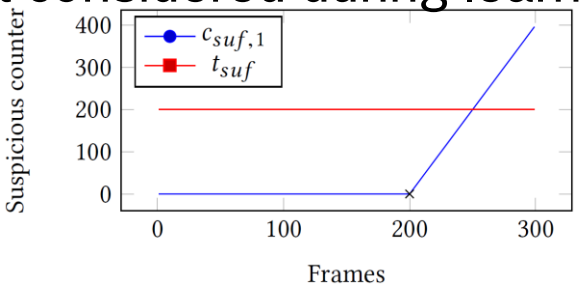
Additional / Unknown ECU

- Lower threshold t_{min} (e.g. 30 %)
- Counter for each ECU
  - Increment if an unexpected ECUs probability > 30% but < 70%
  - Decrement if expected ECU > 30%
- Additional ECU (connected to the bus after training)
  - Counter of several ECUs will rise (no frames are necessary)



(a) Prototype (b) Fiat 500 (c) Porsche Panamera

- Unknown ECU (connected but not considered during learning)
  - Detection like normal attack or
  - Counter of the faked ECU will rise



Scission-aware Attacker

- Influencing all ECUs (draining battery)
  - Quick and significantly → System maybe inactive during model adaption
  - Slow → System adapts model continuously

- Influencing its own signal (heating up / cooling down) to impersonate another ECU
  - No information about its own or the signal of the other ECU
  - Several signal characteristics must be similar
  - Precise adaption must be possible