# Exploring the processing of personal data in modern vehicles - A Proposal of a testbed for explorative research to achieve transparency for privacy and security

Alexandra Koch[1], Robert Altschaffel[2,3], Stefan Kiltz[2], Mario Hildebrandt[2], Jana Dittmann[2]

[1]Otto-von-Guericke University of Magdeburg
PO Box 4120, 39016 Magdeburg, Germany

[2]Otto-von-Guericke University of Magdeburg
Dept. of Computer Science, Research Group Multimedia and Security
PO Box 4120, 39016 Magdeburg, Germany

[3] The work from Robert Altschaffel was supported by research projects in the field of automotive security

## Introduction

- Modern vehicles as example for cyber-physical systems

- Cyber physical systems: deeply intertwined software and physical components perform an overall task [NSF18]

- Vehicles: highly complex and interconnected heterogenic systems with ressource-limited processing nodes

[NSF18] National Science Foundation: Cyber-Physical Systems (CPS); https://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm, accessed: 09/02/18

## Introduction

- IT-security in Automotive often (if at all) an afterthought, e.g. with field bus systems such as CAN used
- IT-security violations have the potential to impact safety [MiV15], but not only that! What about privacy/data protection?
- Data produced and stored inside the car during normal usage is on the increase (esp. with driver assistance systems)
- Planned and realized interconnection between cars, infrastructure and manufacturers add to the problem

[MiV15] C. Miller andC. Valesek,"Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, 2015.

## General Background

### Legal requirementsfor storing additional data

- US American SELF Drive act [USC18] requires "a process for taking preventive and corrective action to mitigate against vulnerabilities [...] including incident response plans, intrusion detection and prevention systems" is established (SEC. 5).

- German road traffic regulation [StVG18] establishes: a set of required data to be stored for highly automated or fully autonomous driving functions, the vehicle is required to record position and time during handovers, transmission of these recorded data sets to legal authorities if they are required to investigate questions of liability

- Car data is personal data [FIA17] regarding the European General Data Protection Regulation (GDPR)

- GDPR lists transparency as a fundamental requirement for privacy protection [Pri17]

[USC18] US Congress: H.R.3388 - SELF DRIVE Act; https://www.congress.gov/bill/115th-congress/house-bill/3388/text, accessed: 09/02/18
[StVG18] Straßenverkehrsgesetz. https://www.gesetze-im-internet.de/stvg/BJNR004370909.html#BJNR004370909BJNG000800116, accessed: 12/12/2017
[FIA17] FIA: What EU legislation says about car data - Legal Memorandum on connected vehicles and data. http://mycarmydata.eu/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf, accessed: 12/12/2017
[Pri17] Privacycompany: Overview of the EU General Data Protection Regulation(GDPR). https://www.privacycompany.eu/files/factsheet_GDPR.pdf, accessed: 12/12/2017 ref

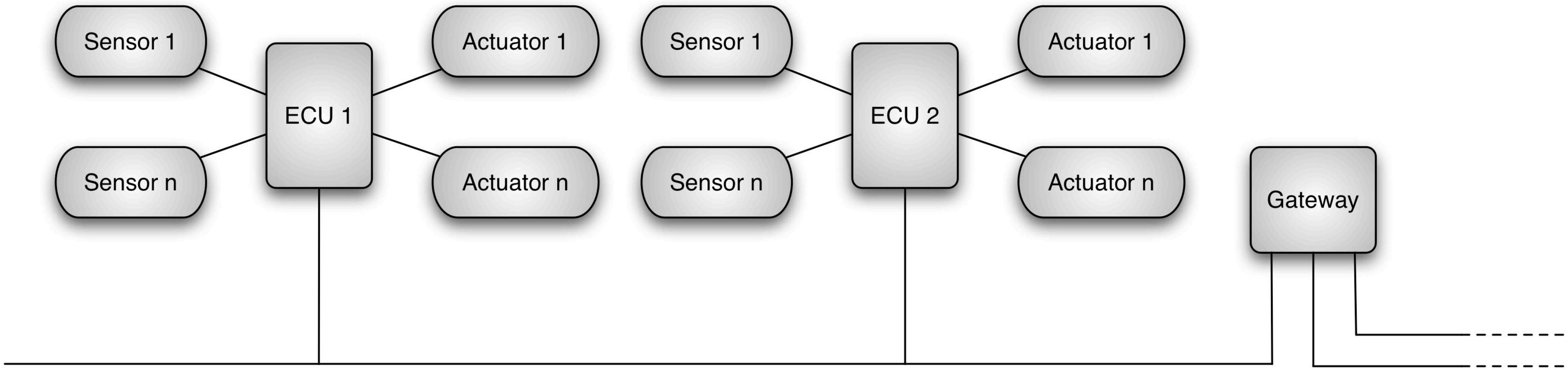
## General Background

- Examples for intransparent data collection [ADAC17]:
  - regular upload of vehicle position (as acquired by GPS), odometer, fuel consumption to the manufacturer's backend system
  - direct remote maintenance access to the vehicle communication bus
- Examples for transparent data collection by EDR [NHT+17]:
  - Speed difference (Delta-V), longitudinal; 0 to 250 ms or 0 to End of Event time plus 30 ms, whichever is shorter
  - Maximum Delta-V, longitudinal; 0 to 300 ms or 0 to End of Event time plus 30 ms, whichever is shorter
  - Time, Maximum Delta-V; 0 to 300 ms or 0 to End of Event time plus 30 ms, whichever is shorter

[ADAC17] ADAC: Welche Daten erzeugt ein modernes Auto?. https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx?ComponentId=260789&SourcePageId=8749&quer=daten, accessed: 12/12/2017
[NHT+17] NHTSA EDR Working Group: Event Data Recorders. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/nhtsa_edrtruckbusfinal.pdf, accessed: 12/12/2017

# Understanding (privacy-related) data in modern automotive systems

- Automotive infrastructure: Data processing facilities in Electronic Control Units (ECU) implementing measurement processes and open/closed control loops
- Sensors digitizing aspects of the automotive environment, actuators manipulating aspects of the physical world as instructed by the software code in the ECU
- ECU contains one or more Micro Controller Units (MCU)



# Understanding (privacy-related) data in modern automotive systems

- Mass storage contains programme data, configuration data in internal and/or external non-volatile memory, internal version often difficult to access

- Main memory often on-chip in the MCU, sometimes contained in an extra PCB, notoriously difficult to access from outside the MCU

- Network data typically easy accessible using the field bus system

# Understanding (privacy-related) data in modern automotive systems

- Forensic models e.g. [KDV15] and tools necessary to comprehensively access all data,
- Ideally as raw data but with semantics to extract other data types (nowadays only achieved in field bus communication)
- Neither the automotive infrastructure nor data extraction using garage tools is even close to forensically sound (e.g. integrity, authenticity, non-repudiation)
- Automotive forensics must make do with what is available, often only access to pre-processed data using self-monitoring diagnosis routines builtin the MCU, producing Diagnostic Trouble Codes (DTC)

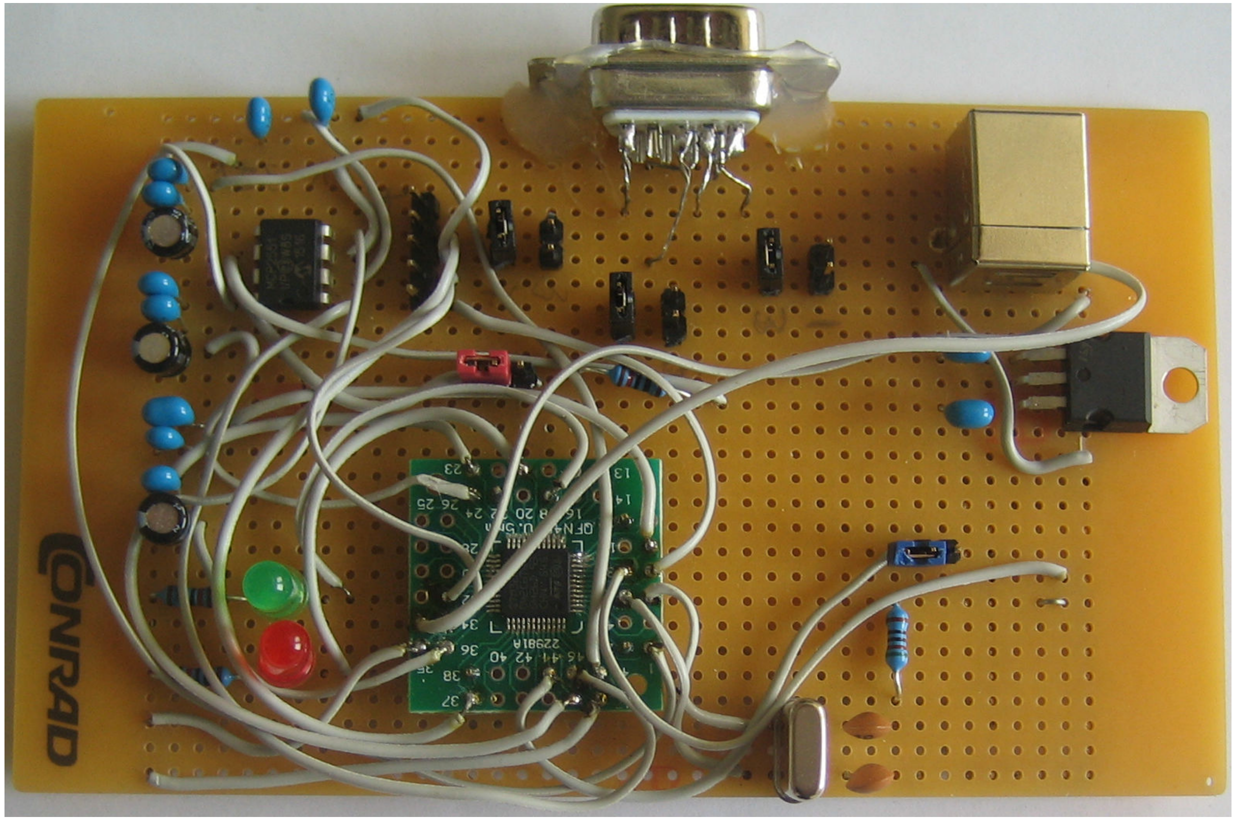
[KDV15] Kiltz, S.; Dittmann, J.; Vielhauer, C.: Supporting Forensic Design - a Course Profile to Teach Forensics, IMF 2015, 2015

# A concept for a demonstrator to identify hidden data in vehicles

- General idea: The „vehicle“, aka the demonstrator needs to be in a realistic state of operation
- Main principles:
  - Completeness (Availability of all relevant hardware/software of a vehicle, but removal of hazardous elements for safety, e.g. explosive SRS actuators, fuel system, coolant system)
  - Realisitic input for the sensors (replacement strategies for unavailabe sensors based on their physical, electrical or electronic characteristics, research into signal shapes and ranges)
  - Monitoring of the three data streams (mass storage, main memory, network), access to network data is the easiest, involves wire tracing if lacking schematics

A concept for a demonstrator to identify hidden data in vehicles – network data

- Tapping into bus communication using interface PCBs, such as CANtact [Eve18], CANtact truly open source, down to component level



[Eve18] E. Evenchick: CANtact-The Open Source Car Tool. http://linklayer.github.io/cantact/, accessed 02/05/2018

# A concept for a demonstrator to identify hidden data in vehicles – network data

- Bus systems often separated according to functionality, e.g. powertrain-bus, instrumentation bus, etc.
- Various implementation methods for bus systems, e.g. twisted copper wire, glass fibre etc. and topologies (star, ring, etc.)
- Central gateway ECU to manage buses (incl. inter-bus communication)
- Challenge: add semantics to collected raw data, especially with payloads spanning over multiple message frames

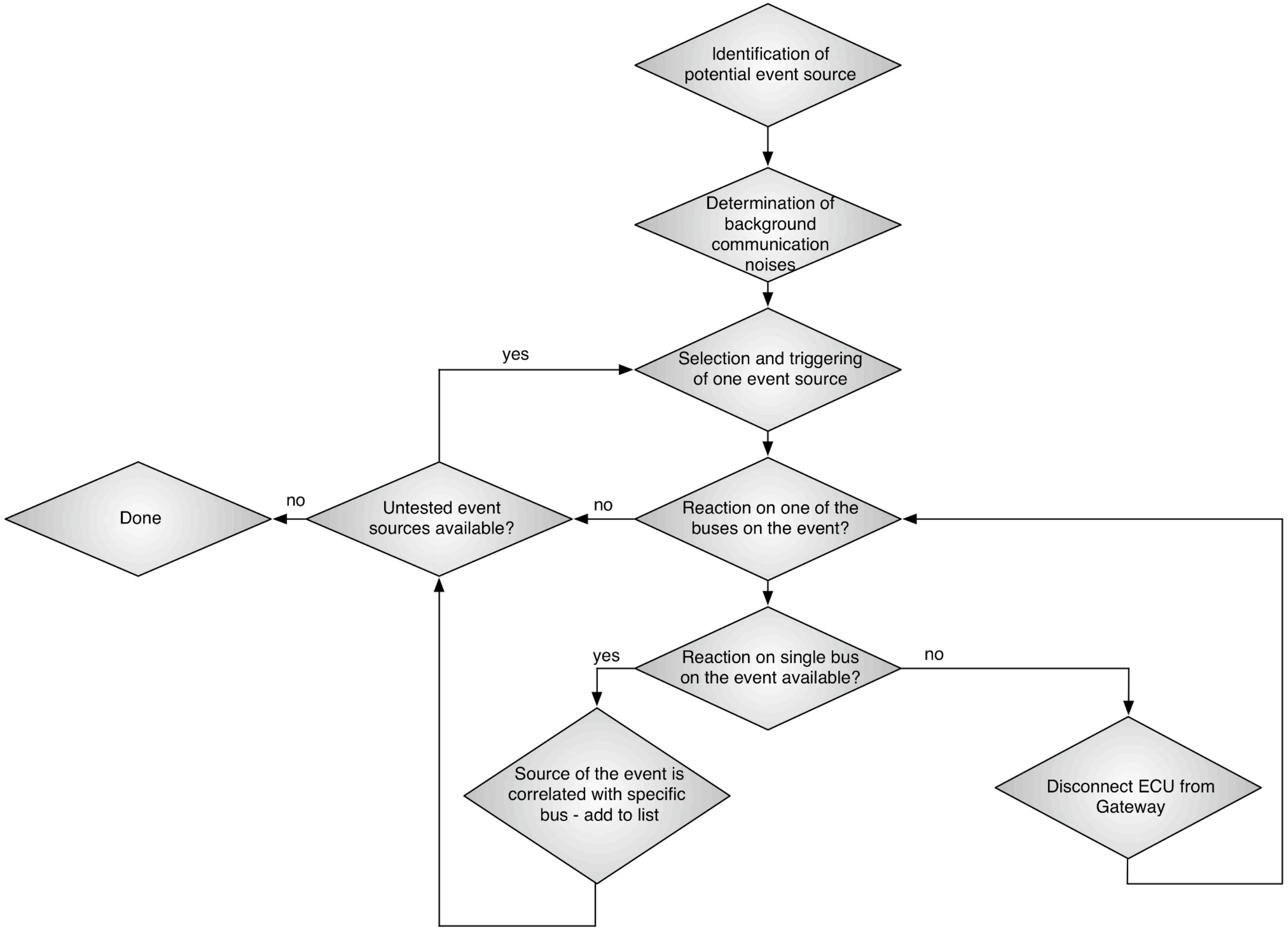
| Field | Start-of-Frame | Identifier (ID) | Remote transmission flag | Identifier extension bit | Reserved | Data length code | Data | CRC | CRC delimited | ACK slot | ACK delimiter | End of Frame |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Bits | 1 | 11 | 1 | 1 | 1 | 4 | 0-64 | 15 | 1 | 1 | 1 | 7 |

Exemplary CAN bus [Cor18] frame

[Cor18] Corrigan, S.: Introduction to the Controller Area Network (CAN) http://www.ti.com/lit/an/sloa101b/sloa101b.pdf, accessed 02/05/2018

# A concept for a demonstrator to identify hidden data in vehicles – network data

- Solving the semantic challenge: systematic testing



# A concept for a demonstrator to identify hidden data in vehicles – mass storage data

- Access to mass storage as external chips typically using the Serial Programming Interface (SPI) [Mot17]
- Mass storage in MCU maybe accessible using debug interfaces, e.g. JTAG [Joh17], BDM [Fre17]
- Fuses can thwart read attempts, often used to protect intellectual property

[Mot17] Motorola Inc.: SPI Block Guide V0306. https://web.archive.org/web/20150413003534/http://www.ee.nmt.edu/~teare/ee308l/datasheets/S12SPIV3.pdf, accessed 14/12/2017
[Fre17] Freescale Semiconductor: Introduction to HCS08 Background Debug Mode, http://www.nxp.com/assets/documents/data/en/application-notes/AN3335.pdf, accessed: 12/12/2017
[Joh17] Johnson, R.; Christie,S.: JTAG 101 IEEE 1149.x and Software Debug, https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/jtag-101-ieee-1149x-paper.pdf, 2009, accessed: 12/12/2017

## A concept for a demonstrator to identify hidden data in vehicles – mass storage data

- Access typicall requires component-level modification (soldering of wires etc.)

- High-level access to a subset of mass storage using diagnostic equipment (often EEPROM configuration data, FLASH for programme memory)

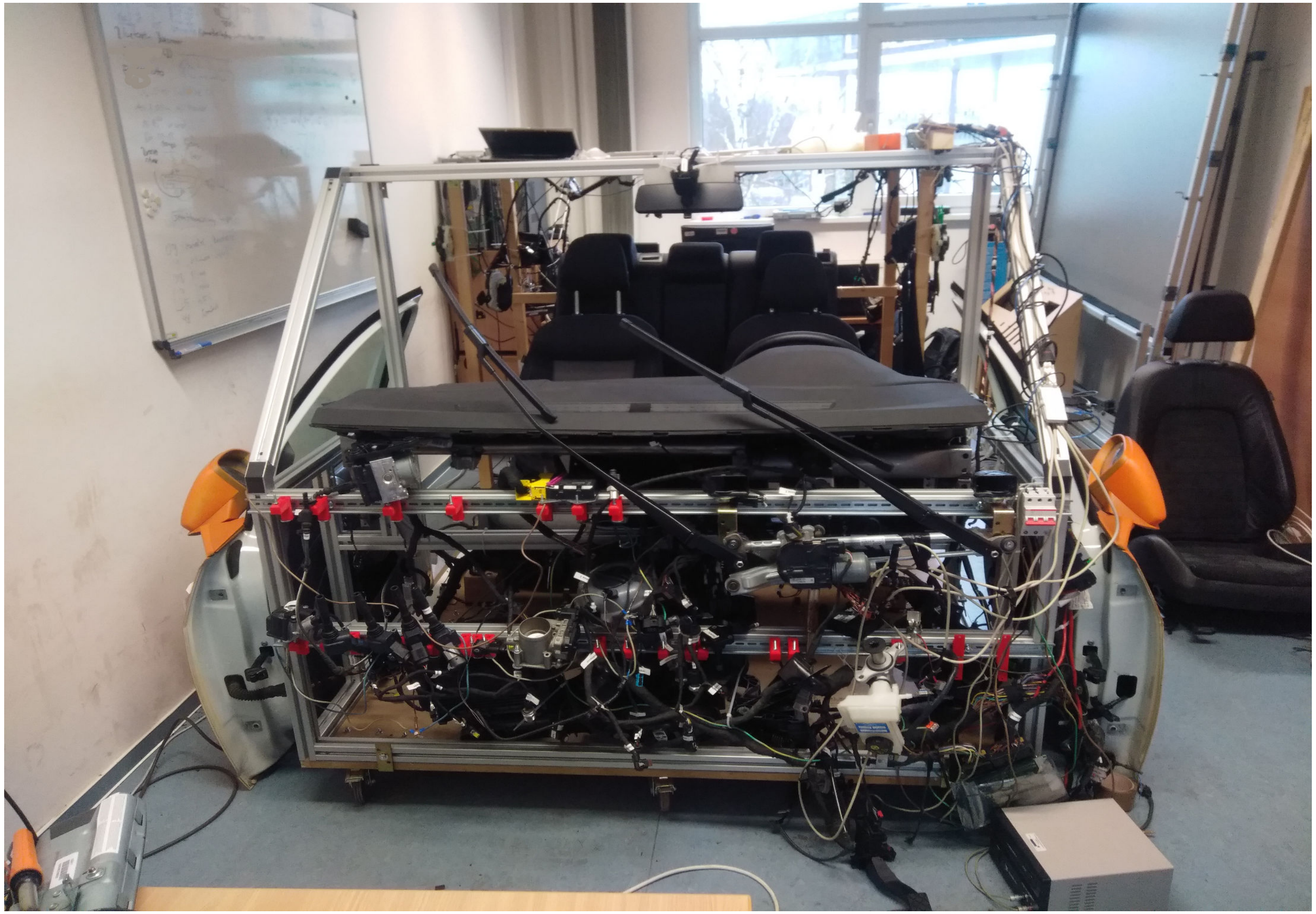
- Integrity/Authenticity with garage equipment is not ensured!

# A concept for a demonstrator to identify hidden data in vehicles – main memory data (volatile)

- Main memory data most volatile, often only valid for fractions of a second
- Raw access to process, programme and real-time data most challenging
- Debug interfaces might be successful, but very unlikely
- Preprocessed real-time data, as understood by the ECU, retrievable using garage equipment
- Integrity/Authenticity with garage equipment is not ensured!

# Practical implementation of a demonstrator to identify hidden data in vehicles – front section

- Updating an existing demonstrator with VW Golf Mk 7 parts

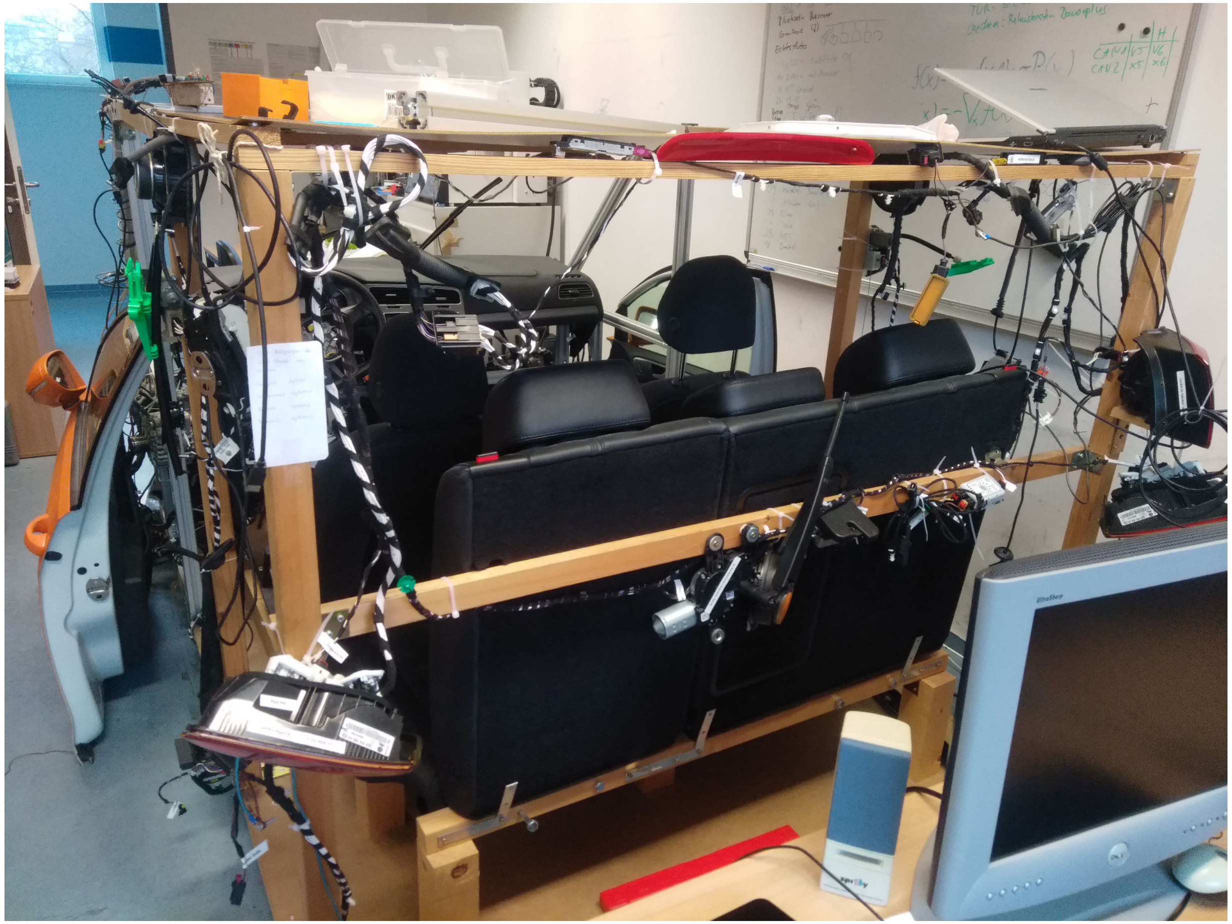


# Practical implementation of a demonstrator to identify hidden data in vehicles – middle section

- Updating an existing demonstrator with VW Golf Mk 7 parts

# Practical implementation of a demonstrator to identify hidden data in vehicles – rear section

- Updating an existing demonstrator with VW Golf Mk 7 parts



# Practical implementation of a demonstrator to identify hidden data in vehicles – CAN access

- Using existing packages cansniffer [canu17] and canutils [canu17] access to CAN bus network using CANtact [Eve18] hardware

```
45 delta   ID  data ...                  < cansniffer comfort # l=20 h=100 t=500 >
0.199902   40  9B 01 00 09 C1 00 00 00 ........
0.199494   FD  49 DF 1F 80 00 00 04 00 I.......
0.199953  101  4F 00 91 00 82 02 40 00 O.....@.
0.200142  116  8B 09 00 00 20 80 00 FF .... ...
0.999618  184  A2 0B 00 00 00 00 00 00 ........
0.200303  30B  7F 21 00 00 08 00 00 00 .!......
0.249778  30D  05 00 00 00             ....
0.199547  31B  D3 7F 00 00 41 00 00 00 ....A...
0.199885  31E  C2 ED 3F 00 00 00 00 00 ..?.....
0.200246  3C0  35 0F 03 00             5...
0.200523  3C7  FE 00 24 00 00 40 A3 00 ..$..@..
1.000372  3D4  42 0F 80 06 00 00 00 00 B.......
0.200493  3D5  98 0F 00 04 00 00 00 00 ........
0.200259  3D6  0F 00 01 00 00 00 00 00 ........
0.000000  3DA  38 06 1A 00 00 F1 FF 00 8.......
0.199276  520  15 0C 00 08 00 0A 00 00 ........
0.200192  584  BD 07 00 00 00 00       ......
1.429899  5F0  84 00 64 00 00 00 00 00 ..d.....
1.460590  5F2  1D 00                   ..
1.000350  641  EB 1C 1F 4F 14 0C 4D 02 ...O..M.
0.499435  647  5C FD FF 7F 00 00 00 0B \.......
1.000456  65D  60 3B 2B 12 00 42 62 7A `;+..Bbz
1.000366  6B0  B0 01 79 02 7F 37       ..y..7
0.999756  6B2  01 42 31 20 59 0E 04 09 .B1 Y...
0.200222  6B4  02 57 31 37 34 33 30 36 .W174306
1.000355  6B6  B0 12 1C 00 02 13       ......
```

```
comfort  1B00004B   [8]  4B 00 04 04 11 00 00 00
comfort       0FD   [8]  52 D9 1F 80 00 00 04 00
comfort       3B5   [8]  00 FE 20 02 0C 00 28 00
comfort       3E9   [8]  FE F8 DF FF 00 00 00 00
comfort       5EA   [8]  00 00 00 36 F8 FE FB FF
comfort       5EB   [8]  00 00 FE FE FB 0F 80 FF
comfort  17F00046   [8]  20 46 00 00 00 00 00 80
comfort       6B5   [8]  FD 83 FD 03 FD 00 FD 07
comfort       3CE   [8]  00 00 00 00 00 00 00 00
comfort       3D0   [8]  02 00 00 00 04 00 00 00
comfort       107   [8]  00 00 00 00 40 00 00 00
comfort       101   [8]  62 0A 91 00 82 00 00 00
comfort       3BE   [8]  00 00 07 01 22 C0 E8 07
comfort       0FD   [8]  1E DA 1F 80 00 00 04 00
comfort       3CF   [8]  00 00 00 00 00 00 00 00
comfort       551   [8]  E1 22 64 23 02 00 00 00
comfort       3D1   [8]  02 00 00 00 04 00 00 00
comfort       107   [8]  00 00 00 00 40 00 00 00
comfort       101   [8]  06 0B 91 00 82 00 00 00
comfort       30D   [4]  01 00 00 00
comfort       30B   [8]  7F 29 00 00 08 00 00 00
comfort       31E   [8]  2D E5 3F 00 00 00 00 00
comfort       3DC   [8]  FC 00 00 00 00 41 00 00
comfort       3DA   [8]  38 06 1A 00 00 F1 FF 00
comfort       040   [8]  CA 09 00 09 C1 00 00 00
comfort       0FD   [8]  31 DB 1F 80 00 00 04 00
comfort       31B   [8]  76 77 00 00 41 00 00 00
comfort       3EB   [8]  FD FE 00 FE 00 00 00 00
comfort       107   [8]  00 00 00 00 40 00 00 00
comfort       6B4   [8]  00 B8 21 84 1A 57 56 57
comfort       101   [8]  15 0C 91 00 82 00 00 00
comfort  1B000014   [8]  14 00 04 03 01 00 00 00
comfort       3C0   [4]  C5 0C 03 00
comfort       3D5   [8]  65 0C 00 04 00 00 00 00
comfort       3D6   [8]  0C 00 01 00 00 00 00 00
comfort       583   [8]  00 10 05 00 00 00 54 00
comfort       584   [6]  17 0E 00 00 00 00
comfort       5A0   [5]  FE FE 03 0E 00
comfort       5E1   [8]  8E 2A 00 60 FE 00 00 00
comfort       5F0   [8]  83 00 64 00 00 00 00 00
comfort  17F0000C   [8]  20 0C 00 00 00 00 00 80
comfort       0FD   [8]  A8 DC 1F 80 00 00 04 00
```

[canu17] can-utils, https://packages.ubuntu.com/de/source/trusty/can-utils, accessed: 12/12/2017
[Eve18] E. Evenchick: CANtact-The Open Source Car Tool. http://linklayer.github.io/cantact/, accessed 02/05/2018

Advanced Multimedia and Security Lab

# Practical implementation of a demonstrator to identify hidden data in vehicles – first reconstructions

- First semantics discovered using the decision tree and the CAN HW/SW

| ID | DL C | Position | | | | | | | | | | | | | | | | Meaning |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | |
| 366 | 16 | | | | | 1/0/8 | | | | | | | | | | | | hazard warning lights/ direction indicator left/ right |
| | | | | | | | | | 1 | | | | | | | | | sound right |
| | | | | | | | | | 2/3 | | | | | | | | | indicator left |
| | | | | | | | | | 4/5 | | | | | | | | | indicator right |
| | | | | | | | | | 6/7 | | | | | | | | | indicator left+right |
| | | | | | | | | | 8/9 | | | | | | | | | control light + sound left |
| | | | | | | | | | A/B | | | | | | | | | control light + sound + indicator left |
| | | | | | | | | | C/D | | | | | | | | | control light + sound left + indicator right |
| | | | | | | | | | E/F | | | | | | | | | sound + control light + indicator left + indicator right |
| | | | | | | | | Z | | | | | | | | | | Z = odd numbers: control light + sound right |
| | | ? | ? | ? | ? | ? | ? | | | ? | ? | ? | ? | ? | ? | ? | ? | |

Steering column lever functionality

## Practical implementation of a demonstrator to identify hidden data in vehicles – first reconstructions

- First semantics discovered using the decision tree and the CAN HW/SW

| ID | DLC | Position | | | | | | | | | | | | | | | | Meaning |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | |
| | | | | | | | | | 0/1/4/5/6 | | | | | | | | | Error airbag |
| | | | | | | | | | 2/3/7 | | | | | | | | | Airbag/ belt tensioners off + Error Airbag |
| | | | | | | | | | 8/9 | | | | | | | | | no Error (maybe because all Airbags are working) |
| | | | | | | | | | C/D | | | | | | | | | passenger airbag off |
| 40 | 16 | | | | | | | | A/B/E/F | | | | | | | | | Airbag/ belt tensioners off |
| | | | | | | | | | | | 0 | | | | | | | all strapped |
| | | | | | | | | | | | 1 | | | | | | | driver not strapped + passenger strapped |
| | | | | | | | | | | | 2 | | | | | | | driver strapped + passenger not strapped |
| | | | | | | | | | | | 3 | | | | | | | no one strapped |
| | | ? | ? | ? | ? | ? | ? | ? | | ? | | ? | ? | ? | ? | ? | ? | |

SRS Sensors

## Conclusion and future questions

- Establishment of a demonstrator for forensics and privacy research
- Usage of actual automotive parts and control circuits (incl. sensors and acutators) to gain realistic results
- Identification of data sources in ECU mass storage, main memory and network communication using IT-forensic principles and models
- Full low-level access to field bus networks established, research into semantics by cause and effect monitoring

## Conclusion and future questions

- Future research to gain low-level access to main memory and mass storage data
- Generally establishment of forensically sound retrieval software
- Capability extension to investigate car2x communication

OTTO VON GUERICKE UNIVERSITÄT MAGDEBURG
AMSL Advanced Multimedia and Security Lab

Thank you very much for your attention!

# References

[NSF18] National Science Foundation: Cyber-Physical Systems (CPS); https://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm, accessed: 09/02/18

[MiV15] C. Miller andC. Valesek,"Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, 2015.

[USC18] US Congress: H.R.3388 - SELF DRIVE Act; https://www.congress.gov/bill/115th-congress/house-bill/3388/text, accessed: 09/02/18

[StVG18] Straßenverkehrsgesetz. https://www.gesetze-im-internet.de/stvg/BJNR004370909.html#BJNR004370909BJNG000800116, accessed: 12/12/2017

[FIA17]FIA: What EU legislation says about car data - Legal Memorandum on connected vehicles and data. http://mycarmydata.eu/wp-content/uploads/2017/06/20170516-Legal-Memorandum-on-Personal-Data-in-Connected-Vehicles-www.pdf, accessed: 12/12/2017

[Pri17] Privacycompany: Overview of the EU General Data Protection Regulation(GDPR). https://www.privacycompany.eu/files/factsheet_GDPR.pd, accessed: 12/12/2017 ref

[ADAC17] ADAC: Welche Daten erzeugt ein modernes Auto?. https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/daten_im_auto/default.aspx?ComponentId=260789&SourcePageId=8749&quer=daten, accessed: 12/12/2017

[NHT+17] NHTSA EDR Working Group: Event Data Recorders. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/nhtsa_edrtruckbusfinal.pdf, accessed: 12/12/2017

[KDV15] Kiltz, S.; Dittmann, J.; Vielhauer, C.: Supporting Forensic Design - a Course Profile to Teach Forensics, IMF 2015, 2015

[Eve18] E. Evenchick: CANtact-The Open Source Car Tool. http://linklayer.github.io/cantact/, accessed 02/05/2018

[Cor18] Corrigan, S.: Introduction to the Controller Area Network (CAN) http://www.ti.com/lit/an/sloa101b/sloa101b.pdf, accessed 02/05/2018

[Mot17] Motorola Inc.: SPI Block Guide V0306. https://web.archive.org/web/20150413003534/http://www.ee.nmt.edu/~teare/ee308l/datasheets/S12SPIV3.pdf, accessed 14/12/2017

[Fre17] Freescale Semiconductor: Introduction to HCS08 Background Debug Mode, http://www.nxp.com/assets/documents/data/en/application-notes/AN3335.pdf, accessed: 12/12/2017

[Joh17] Johnson, R.; Christie,S.: JTAG 101 IEEE 1149.x and Software Debug, https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/jtag-101-ieee-1149x-paper.pdf, 2009, accessed: 12/12/2017

[canu17] can-utils, https://packages.ubuntu.com/de/source/trusty/can-utils, accessed: 12/12/2017