OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

Side Channel Monitoring for Fuzz Testing of Future Mobility Systems

Autors: Philipp Fuxen, Murad Hachani, Jonas Schmidt, Philipp Zaumseil, Rudolf Hackenberg

Philipp Fuxen
Department of Informatics and Mathematics
Technical University of Applied Sciences Regensburg
Philipp.Fuxen@oth-regensburg.de

The Fourteenth International Conference on Cloud Computing, GRIDs, and Virtualization
CLOUD COMPUTING 2023
June 27th, 2023

Philipp Fuxen

- Currently: Cooperative PhD at OTH Regensburg and FU Berlin
- Degree: Master of Science in Applied Research in Engineering Sciences at OTH Regensburg
- Department of Informatics and Mathematics, OTH Regensburg
- CarSec Laboratory headed by Prof. Dr. Rudolf Hackenberg
- Focus of the lab is automotive security
  - Penetration testing and Test automation
  - IT Security applications
  - Security education
- IT Security applications and investigations based on AI

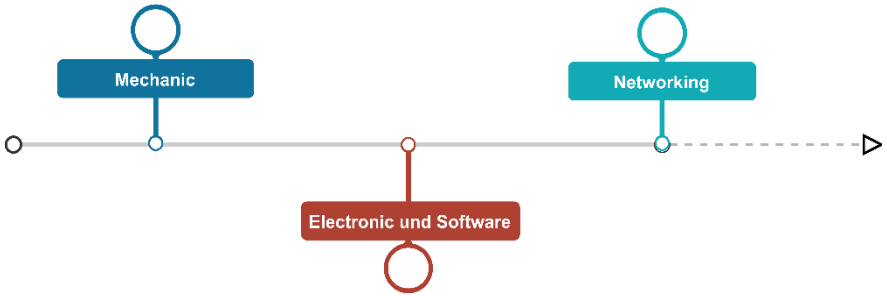
Agenda

1. Introduction to Automotive Security
2. Fuzz Testing
3. Experiment
4. Side Channel Measurement System
5. Conclusion
6. Future Work

Development of the Vehicle

- IT security in vehicles has only taken on an increasingly important role in recent years
- In the past, a vehicle consisted mainly of mechanical components
- In recent years, the vehicle has been equipped primarily with new electronics and software
- Currently and in the future, the degree of networking of vehicles is increasing strongly

➡ The vehicle becomes a cyber-physical system



Car Hacking Reaches new Dimensions

- Probability of occurrence of hacker attacks increases because vehicles are increasingly networked
- In addition, the damage potential increases when an attack occurs
- This is the case because remote attacks on vehicles are becoming possible
- The risk of attacks on multiple vehicles in a fleet must also be expected

Attack Path Demonstration

- The first vulnerabilities in vehicles were published as early as 2010
- The publications were criticized for the fact that it is only possible to exploit these vulnerabilities with physical access
- The two hackers **Dr. Charlie Miller and Chris Valasek** later demonstrated some remote attacks

- **Remote exploitation of an unaltered passenger vehicle** [1]
  - The researchers were able to remotely connect to the vehicle via the infotainment system
  - In addition, they were able to exploit further vulnerabilities in the vehicle network to manipulate the vehicle
  - Thus, they were able to operate the windshield wipers and the air conditioning, for example. Under certain conditions, they could even control the vehicle

Source: https://youtube.com

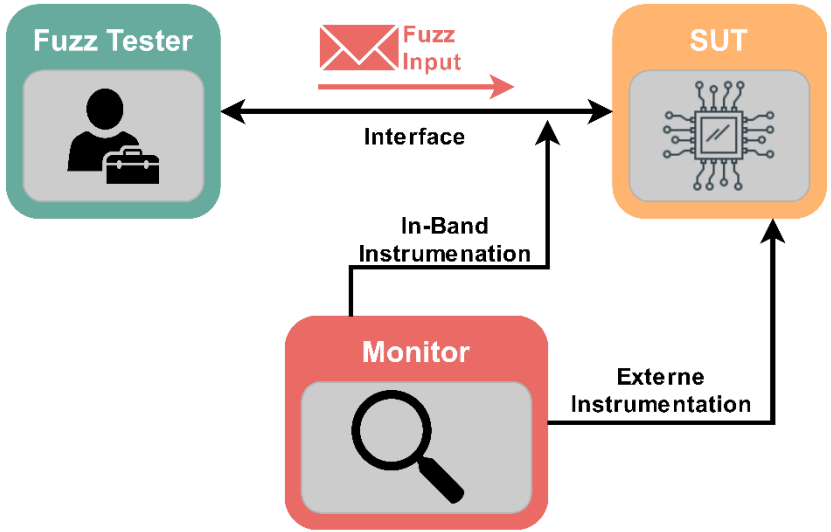
Fuzz Testing in the Automotive Sector

- **ISO/SAE 21434**: International standard for IT security of motor vehicles over the entire life cycle (Concepts, product development, production, operation, maintenance and decommissioning of E/E systems)
- Specifies technical requirements for cybersecurity and risk management of motor vehicles
- One test method proposed by the ISO/SAE 21434 is **fuzz testing**
- **Fuzz testing** is already used successfully in other industries
- There are some challenges in the automotive sector

How does Fuzz Testing work?

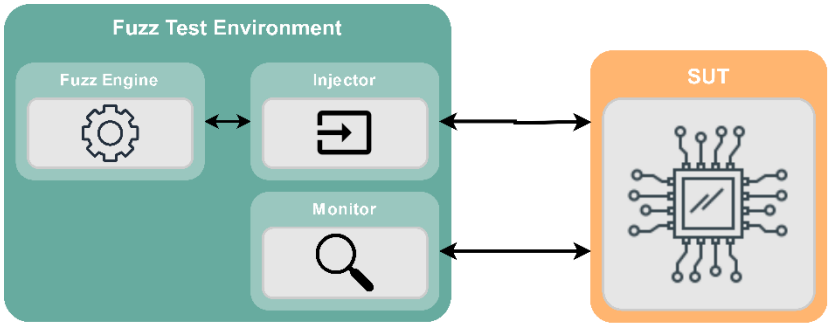
- A fuzz tester generates so-called fuzz data
- This fuzz data is transmitted to the target system
- Some fuzzers look for faults and anomalies while the target system processes the fuzz data

- The goal is to find out what fuzz data causes unwanted system behavior
- This data is then analyzed to see if there is a vulnerability



Fuzz Test Environment

- **Fuzz Engine**: The fuzz engine generates malformed messages, which are then sent to the target system to provoke failures.
- **Injector:** With the Injector, the fuzz data generated by the fuzz engine is passed to the target system using the selected input method.
- **Monitoring:** The Monitoring is responsible for observing the target system for abnormal and unexpected behavior caused by the fuzz inputs.



Challenges in the Automotive Sector

- To use fuzz tests automatically and efficiently for automotive systems, it is necessary to detect abnormal behavior of the target system
- This is particularly difficult for automotive Electronic Control Unit (ECU) because there is often little or no knowledge of the internal processes during testing
- In addition, their monitoring is a challenge due to highly restricted access and hardware limitations
- So-called black box methods are therefore particularly relevant in the automotive sector
- Compared to white box or grey box methods, no initial information about the DUT is required (No knowledge about the internal structure, the source code, …)

Goal: **The main goal of the paper is to improve black box protocol fuzz testing for hardware-based automotive systems using side channel information.**

What is a Side Channel?

- Extra information that can be gathered
- Results from the influence of the system execution
- Information unintentionally leaked through a medium
- Power consumption, execution time, temperature, …

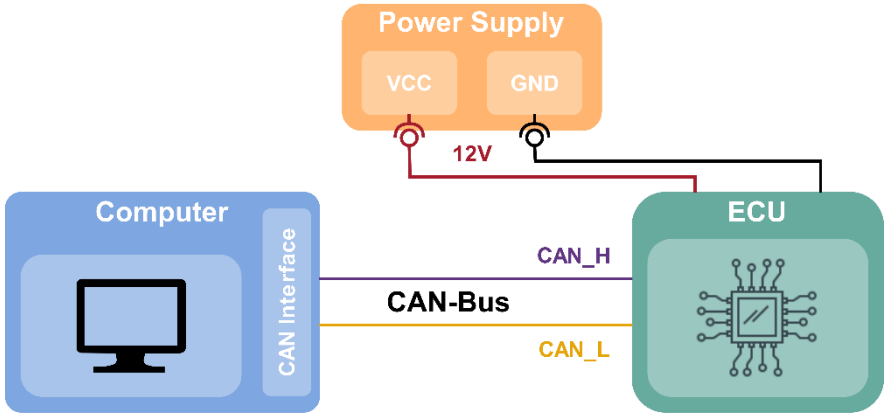
Fuzz Testing Experiment

- Goals:
  - Conducted to collect anomalies and data for later evaluation of the side channels
  - Collect requirements for the implementation of a side-channel-based fuzzer

- Setup:
  - Starting with fuzzing the Controller Area Network (CAN)
  - Self-performed observation of the ECU and with basic analysis methods
  - An anomaly is detected when the ECU behaved in a way that deviated from the normal operating state

Hardware Setup

- ECU connected with Power Supply (12V)
- Connection between ECU and Computer over CAN-to-USB Interface
- CAN-to-USB Interface: OWASP EMB60 [2]
  - Open Source
  - Hardware and Software is accessible
  - Provides two CAN FD channels



Fuzz Test

- Operating System: Ubuntu (Linux)
- CAN-to-USB Interface: SocketCAN with can-utils
- At the beginning so-called Random Fuzzing was performed
  - Fuzzing with Python and python-can
  - Fuzzing with Scapy
  - Fuzzing with Caring Caribou
- Also protocol-specific areas where analyzed with random values
- Monitoring of the ECU was self-performed (Infotainment Displays and Instrument Cluster)

Findings

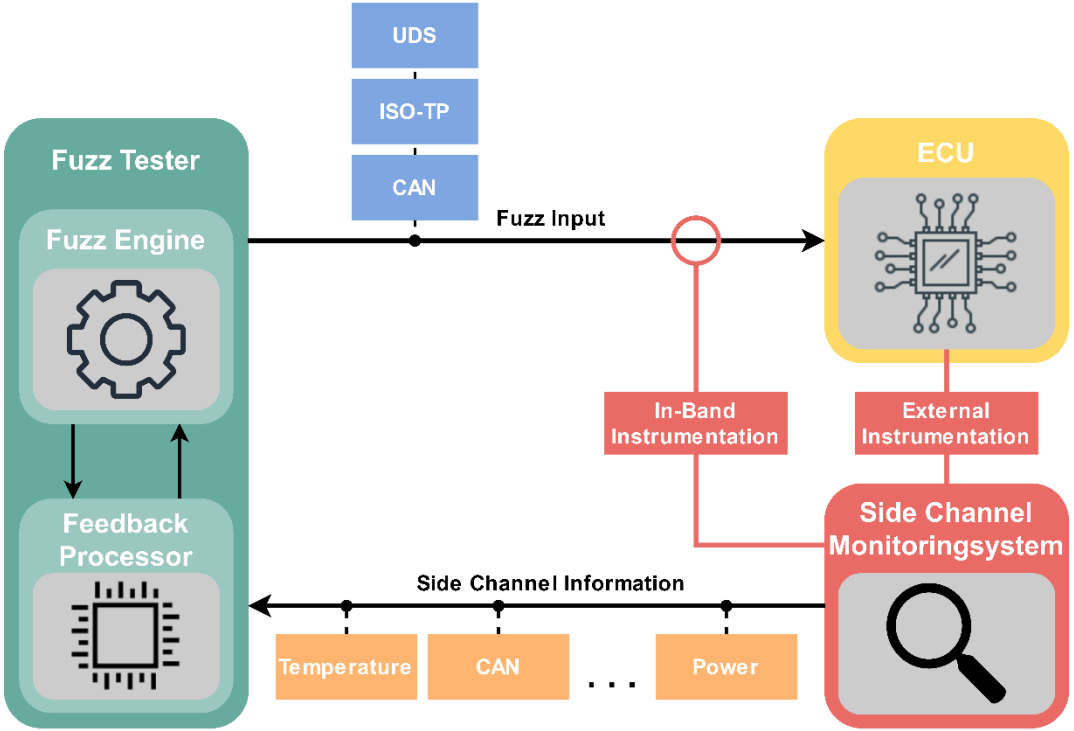
- Identification of fuzz messages that have caused abnormal behavior
  - Analysis of the side channel information
  - Generation of training data for AI models

- Without automated monitoring system the identification of abnormal behavior is very time-consuming

- Also, it is very difficult to see the correlation between fuzz messages and the associated abnormal behavior

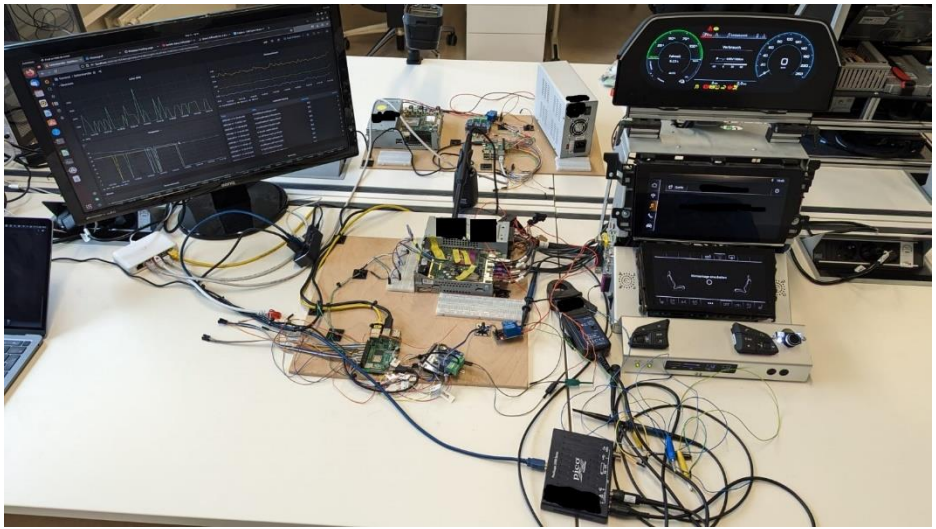
- Therefore, the improvement through the monitoring of side channels is necessary

Concept


UDS
ISO-TP
CAN
Fuzz Tester
Fuzz Engine
Feedback Processor
Fuzz Input
ECU
In-Band Instrumentation
External Instrumentation
Side Channel Monitoringsystem
Side Channel Information
Temperature
CAN
. . .
Power

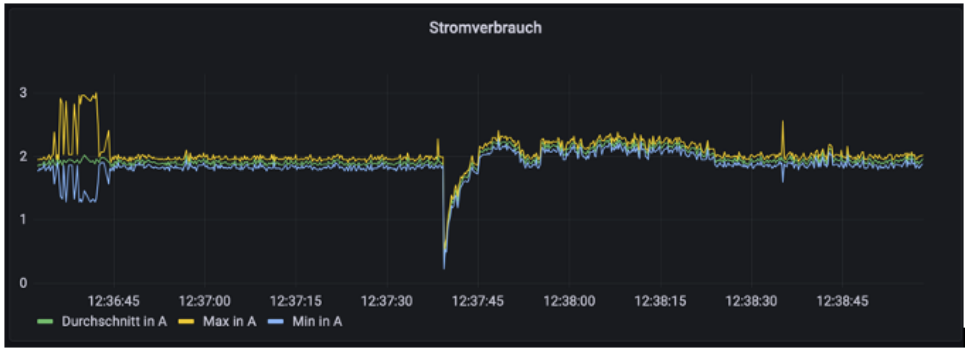
Measurement Setup

- Measured Side Channels:
  - Power
  - Acoustic (FAN)
  - CAN
  - Thermal image
  - Temperature
  - Visual image
- Storage of measured values with InfluxDB
- Visualization with Grafana



Power Example

- Measurement of power consumption
- Calculation of the average, the maximum and the minimum in a time interval
- Abnormal behavior can be observed in the time interval 12:37:35 - 12:38:25
- ECU crashes and then reboots



Conclusion

- The vehicle has changed drastically in recent years as more and more electronic components have been integrated
- In addition, the degree of networking has increased significantly, which is why the importance of car hacking has reached a new dimension
- To counteract this development the ISO/SAE 21434 suggest to perform fuzz tests
- To overcome the challenges of automotive hardware-based fuzz tests, the monitoring of side channels is useful
- Therefore, a Side Channel Measurement System was established

Future Work

- Identify, classify and evaluate the data of the normal and abnormal behavior
- Creation of a dataset for the analyses and AI methods
- Researching methods for anomaly detection and for preprocessing
- Implementation of the Demonstrator of the Side Channel Monitoring

- Researching methods for the smart fuzz data generation
- Implementation of the Demonstrator of the Side Channel Fuzz Engine

- Research on other communication protocols

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

Side Channel Monitoring for Fuzz Testing of Future Mobility Systems

Autors: Philipp Fuxen, Murad Hachani, Jonas Schmidt, Philipp Zaumseil, Rudolf Hackenberg

Philipp Fuxen
Department of Informatics and Mathematics
Technical University of Applied Sciences Regensburg
Philipp.Fuxen@oth-regensburg.de

The Fourteenth International Conference on Cloud Computing, GRIDs, and Virtualization
CLOUD COMPUTING 2023
June 27th, 2023

References

[1] C. Miller and C. Valasek, “Remote exploitation of an unaltered passenger vehicle” *Black Hat USA*, vol. 2015, no. S 91, 2015.

[2] A. Meisel, *Owasp automotive emb 60 - owasp foundation.* [Online]. Available: https://owasp.org/www-project-automotive-emb-60/ (retrieved: 2023-06-08).

[3] P. Biondi, *Scapy: The python-based interactive packet manipulation program & library.* [Online] Available: https://scapy.readthedocs.io/en/latest/index.html (retrieved: 2023-06-08).

[4] mjidhage, kasperkarlsson, TobLans, et al., *Documentation for caring caribou*. [Online]. Available: https://github.com/CaringCaribou/caringcaribou/blob/master/README.md (retrieved: 2023-06-08).