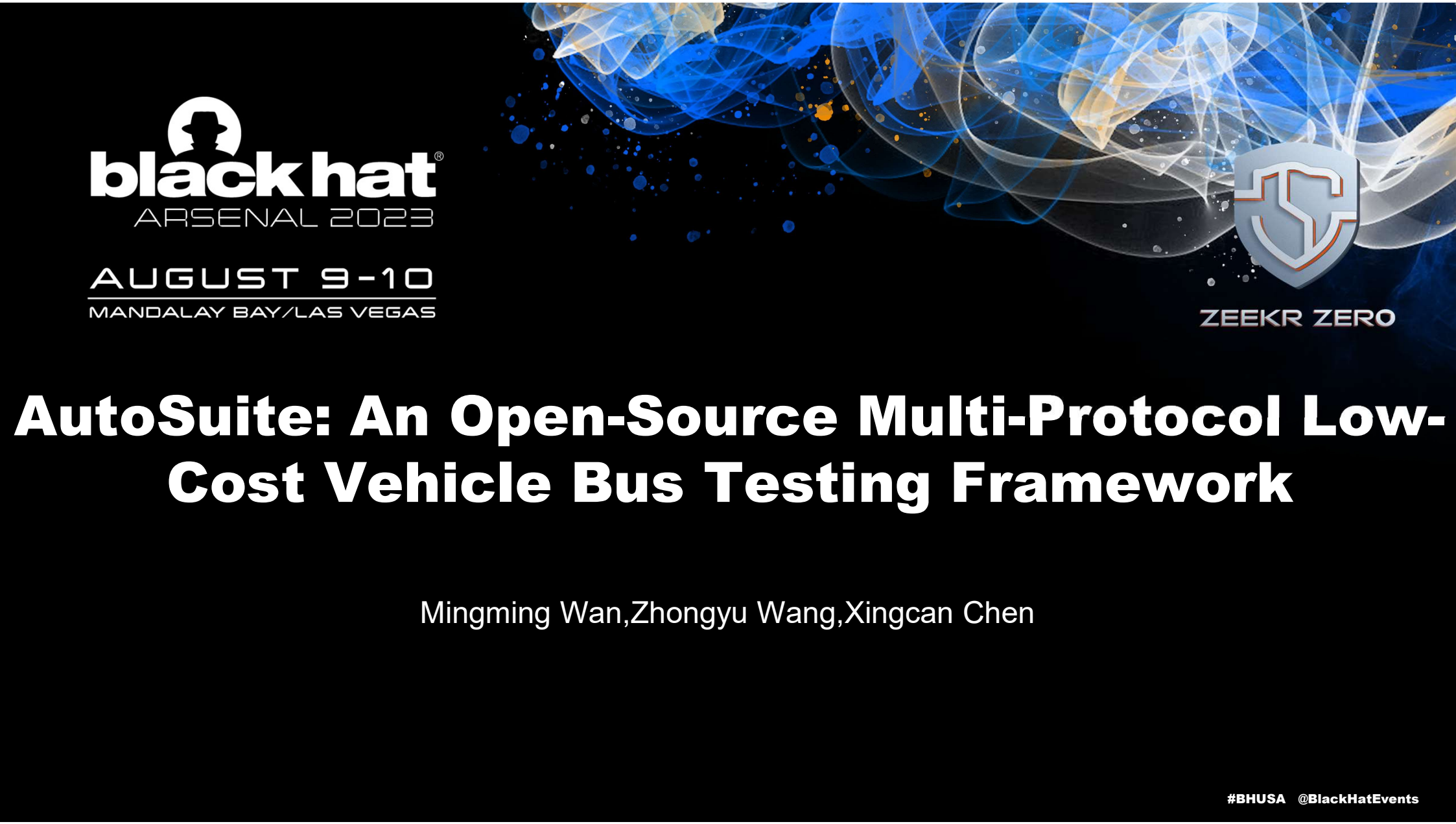


AutoSuite: An Open-Source Multi-Protocol Low-Cost Vehicle Bus Testing Framework

Mingming Wan,Zhongyu Wang,Xingcan Chen

About US

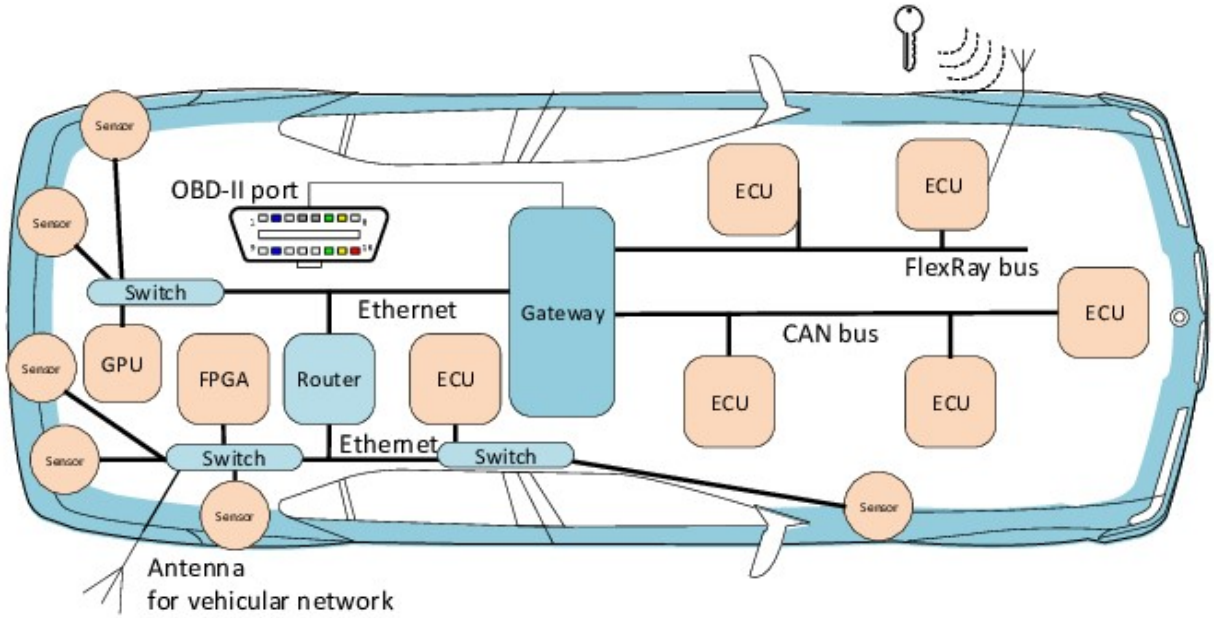
Mingming Wan
BlackHat USA 2017 Briefings Speaker
Senior Hardware Engineer
of **ZEEKR AUTO**
wanmingming2008@gmail.com

Zhongyu Wang
IoT Group Head
of **ZEEKR AUTO**
wang3919379@gmail.com

Xingcan Chen
Hardware Security Engineer
of **ZEEKR AUTO**
icon.xxxc@gmail.com

Vehicle Bus

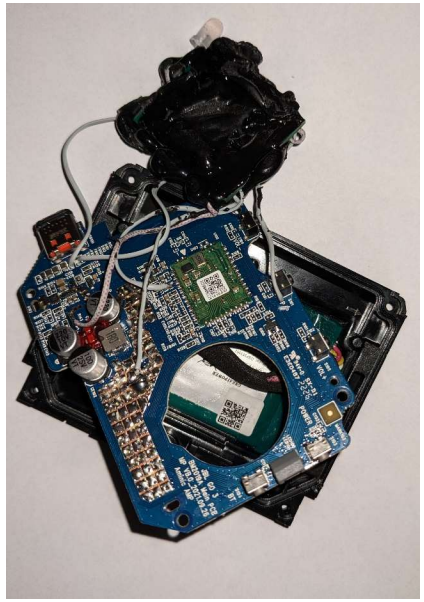
- Communication among different systems
- Data Transfer in the form of signals
- FlexRay, CAN, LIN, ETH(DoIP)
- Diagnostics for Troubleshooting



Vehicle Bus Vulnerabilities

CVE-2017-14937

The airbag detonation algorithm allows injury to passenger-car occupants via predictable Security Access (SA) data to the internal CAN bus (or the OBD connector).



CVE-2023-29389

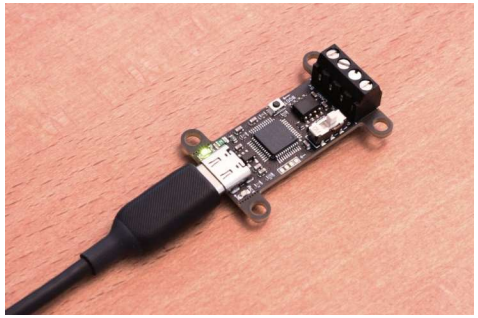
Toyota RAV4 2021 vehicles automatically trust messages from other ECUs on a CAN bus, which allows physically proximate attackers to drive a vehicle by accessing the control CAN bus after pulling the bumper away and reaching the headlight connector

Vehicle bus Tools

Vector VN7640

FlexRay, CAN, LIN

$50K



CANable,CANdelight

Open Source

CAN ONLY

Panda

OBD Port

CAN,LIN

What is AutoSuite ?

- Open-source
- Multi-protocol supported
- Low-cost
- Functional Fuzz

CAN
CAN FD

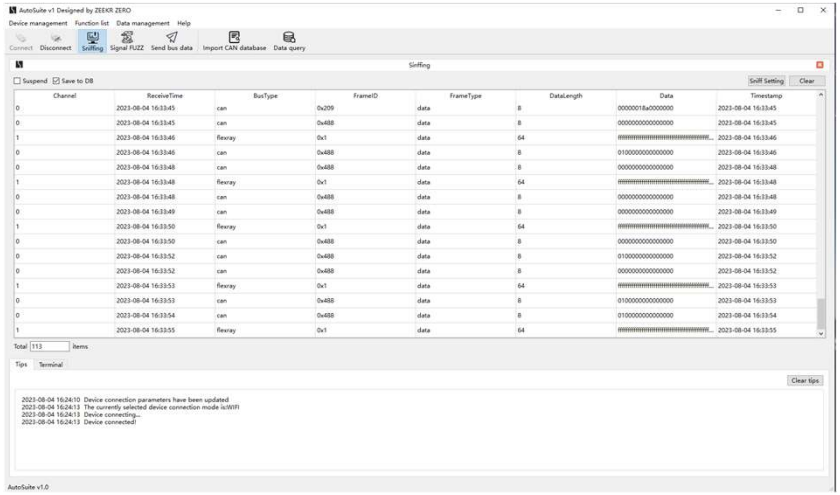
FlexRay™

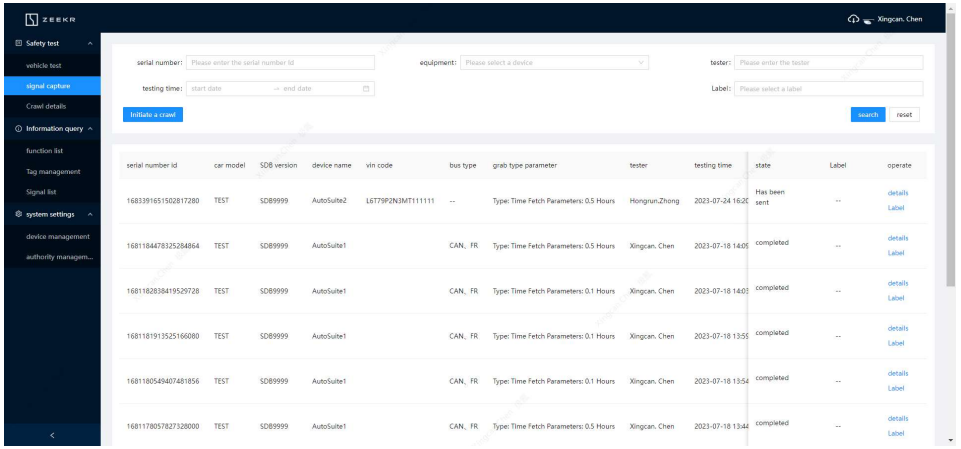
LOCAL INTERCONNECT NETWORK

ETHERNET

AutoSuite Features

- **Plug-in Supported : Developed with PySider6**
- **Cross-Platform: Windows, Linux, MAC**
- **Flexible application : Client and Website**



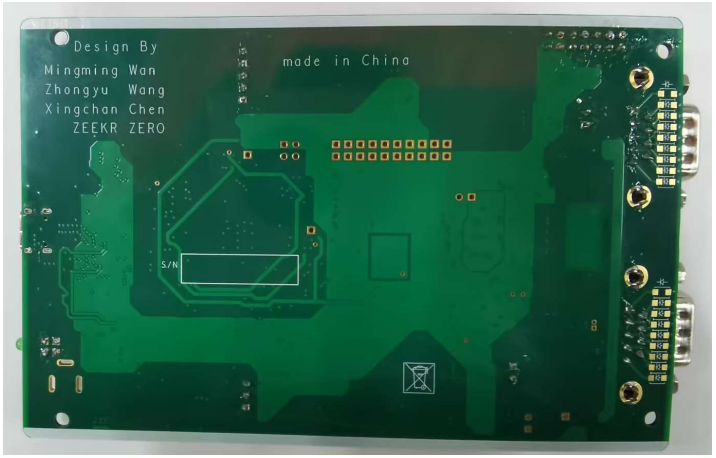


AutoSuite Features

- **6-Layer PCB**
- **Both USB Type-C 5V and OBD power 12V options available**
- **WiFi Connect**

	FlexRay	CAN/CANFD	LIN	ETH
Support	√	√	√	√
Current Channels	1	2	1	1
Max Channels	2	8	16	2

- **Coming soon**:
  - 5G module
  - SD card storage
  - 100BASE-T1

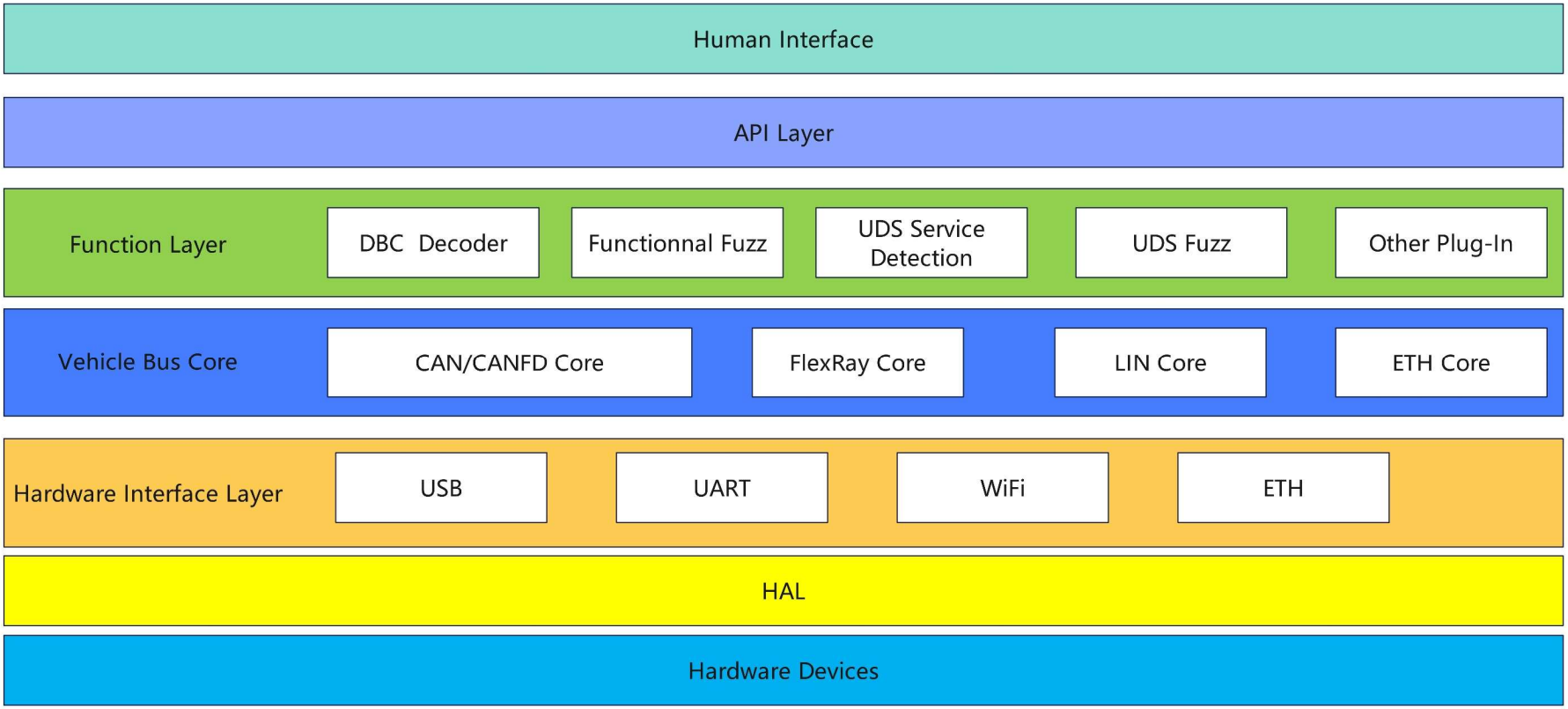


AutoSuite Ports

1:DB9 Port 1
2:DB9 Port 2

3:Status Indicators
4:Type-C Port
5:WIFi Antenna

AutoSuite Architecture



How AutoSuite Work

OBD(On-board diagnostics)

- There are lots of OBD ports for testing reserved in vehicle R&D stage.
- R&D engineer, functional safety testers and cyber security testers can directly and use AutoBox for testing.
- Including FlexRay, CAN/CANFD, LIN and ETH.
- If OBD port for testing is not reserved, broken cable tool is helpful.

OBD in Vehicle

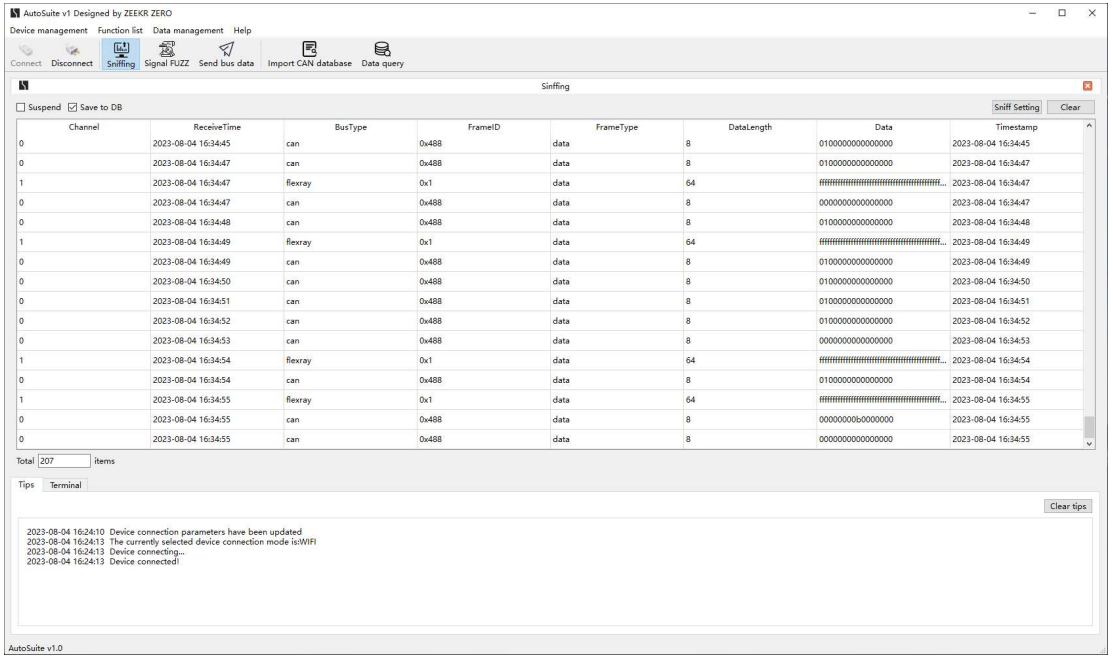
OBD converter

OBD converter

Broken cable tool

AutoSuite Sniff

Connect AutoSuite to Vehicle



Start to Sniffing Vehicle Bus Data

Demo1 Vehicle Bus Sniffing

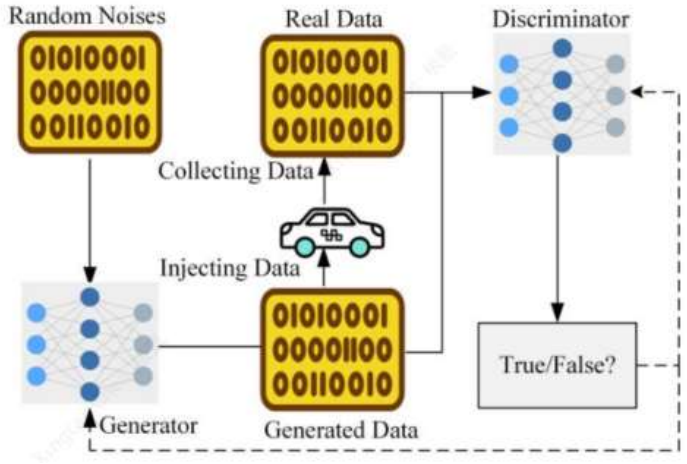
AutoSuite Functional Fuzz

caringcaribou / caringcaribou / modules / fuzzer.py

Code | Blame | 794 lines (670 loc) · 31.1 KB

```
152
153  def get_random_arbitration_id(min_id, max_id):
154      """
155      Returns a random arbitration ID in the range min_id <= arb_id <= max_id
156
157      :param min_id: int minimum allowed arbitration ID (inclusive)
158      :param max_id: int maximum allowed arbitration ID (inclusive)
159      :return: int arbitration ID
160      """
161      arb_id = random.randint(min_id, max_id)
162      return arb_id
163
164
165  def get_random_data(min_length, max_length):
166      """
167      Generates a list of random data bytes, whose length lies in the interval 'min_length' to 'max_length'
168
169      :param min_length: int minimum length
170      :param max_length: int maximum length
171      :return: list of randomized bytes
172      """
173      # Decide number of bytes to generate
174      data_length = random.randint(min_length, max_length)
175      # Generate random bytes
176      data = []
177      for i in range(data_length):
178          data_byte = random.randint(BYTE_MIN, BYTE_MAX)
179          data.append(data_byte)
180      return data
181
```

CaringCaribou Fuzzer

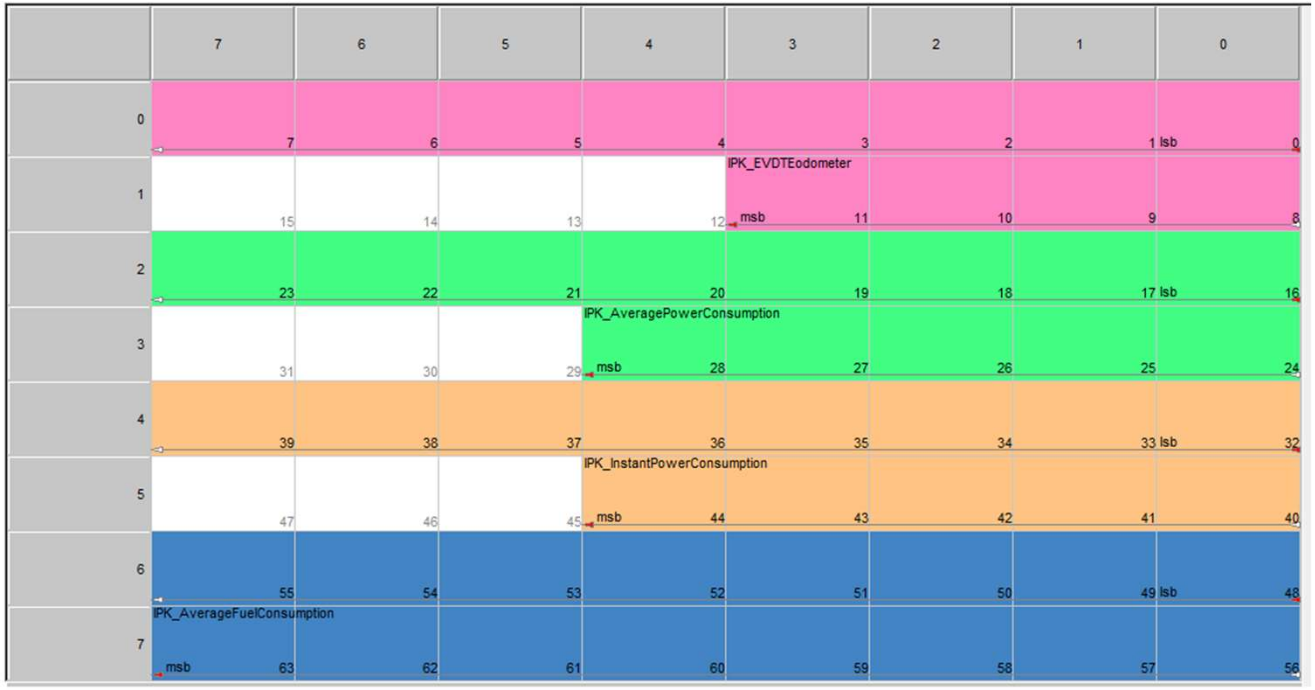


CAN-FT

- Current Vehicle Fuzzing tools only focus on random generate frame ID or data frame
- Hard to location root cause

AutoSuite Functional Fuzz

- **Functional-level Fuzzing**
- **DBC Decode**
- **DTC Detection**
- **UDS Fuzz**



Signal Layout in CAN Frame

AutoSuite Functional Fuzz

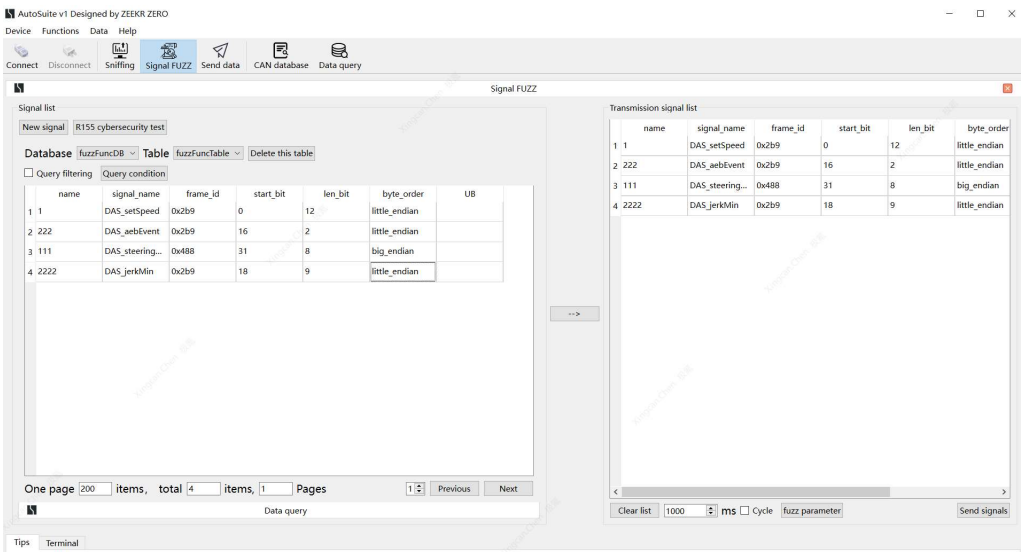
Workflow of Functional Fuzzer

AutoSuite R155 Cybersecurity Test

R155 Annex 5

11	Messages received by the vehicle (for example X2V or diagnostic messages), or transmitted within it, contain malicious content	11.1	Malicious **internal** (e.g. CAN) **messages**
		11.2	Malicious **V2X messages,** e.g. infrastructure to vehicle or vehicle-vehicle messages (e.g. CAM, DENM)
		11.3	Malicious diagnostic messages
		11.4	Malicious **proprietary messages** (e.g. those normally sent from OEM or component/system/function supplier)
18	Devices connected to external interfaces e.g. USB ports, OBD port, used as a means to attack vehicle systems	18.1	**External interfaces** such as USB or other ports used as a point of attack, for example through code injection
		18.2	Media infected with a **virus** connected to a vehicle system
		18.3	**Diagnostic access (e.g. dongles in OBD port)** used to facilitate an attack, e.g. manipulate vehicle parameters (directly or indirectly)
24	Disruption of systems or operations	24.1	**Denial of service**, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging

AutoSuite R155 Cybersecurity Test



Demo2 Functional Fuzz

Autosuite Application Scenarios

Auto Cyber Security Testing

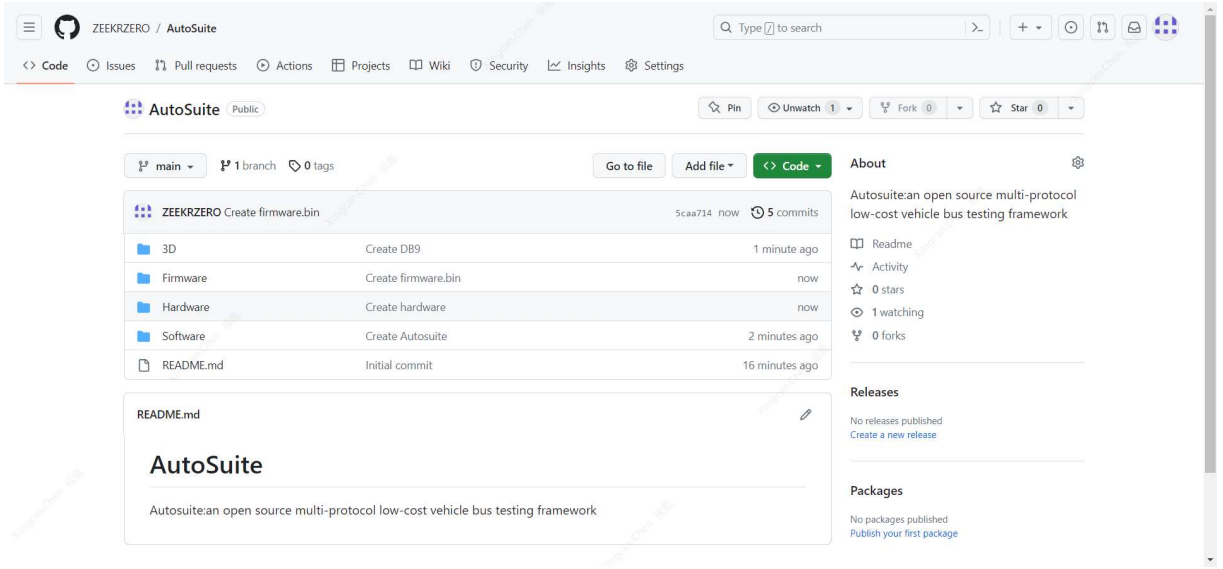
- ✓ For WP.R155 Testing
- ✓ For Chinese Vehicle security Law Testing
- ✓ For Vehicle Charge Pile Testing

Personal Security Research

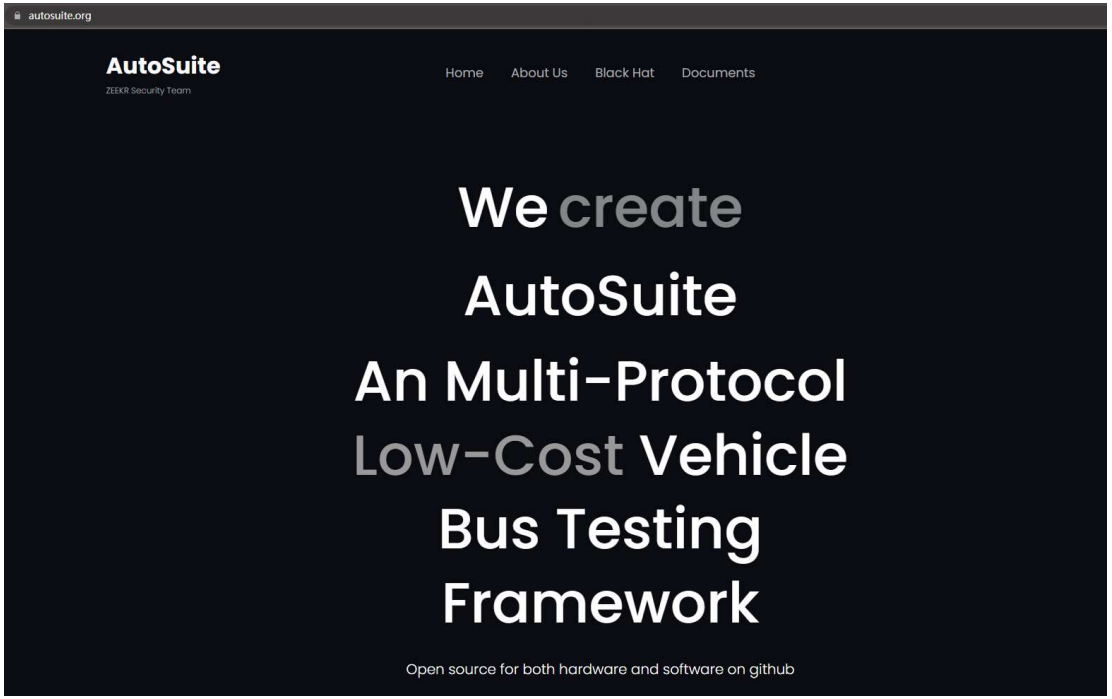
- ✓ Personal vehicle security researcher
- ✓ Easy to use
- ✓ Low-Cost

AutoSuite Opensource

- ✓ GitHub.or www.Autosuite.org
- ✓ AutoSuite software has uploaded
- ✓ All PCB components can be purchased on Alibaba or DigiKey. You can make AutoSuite by yourself in $200.



TO DO



- High-risk vulnerabilities, integrated POC (Proof of Concept), modularization.
- Additional hardware support for in-vehicle bus systems such as automotive Ethernet 100M/10M and CANXL protocol.

Please Access www.autosuite.org To Get Latest Information

Acknowledgments

@Safe4
@Fengli Jiang
@Alex Wang
@Lakka
@Jiantao Yan
@Cawan

POC2022: Chen Nan & Chongyang Bao & Jiaming Tao, "Explore 'BUS' Mysteries via Automotive fuzzing'

Thank you