



Towards Building a Better Automotive Security Testing Platform

Sekar Kulandaivel* and Wenjuan Lu§

Joint work with Jorge Guajardo* and Brandon Barry§

*Robert Bosch LLC – Research and Technology Center

§Block Harbor Cybersecurity

Our background



Research Engineer

Robert Bosch – Research & Technology Center

- Previously ProdSec Lead at Locomotion
- PhD in ECE from Carnegie Mellon University
- First-author publications in IEEE S&P, USENIX Security, ESCAR USA and Europe
- First-place team prize at DEF CON 24's CHV challenge by Craig Smith



Director of Product

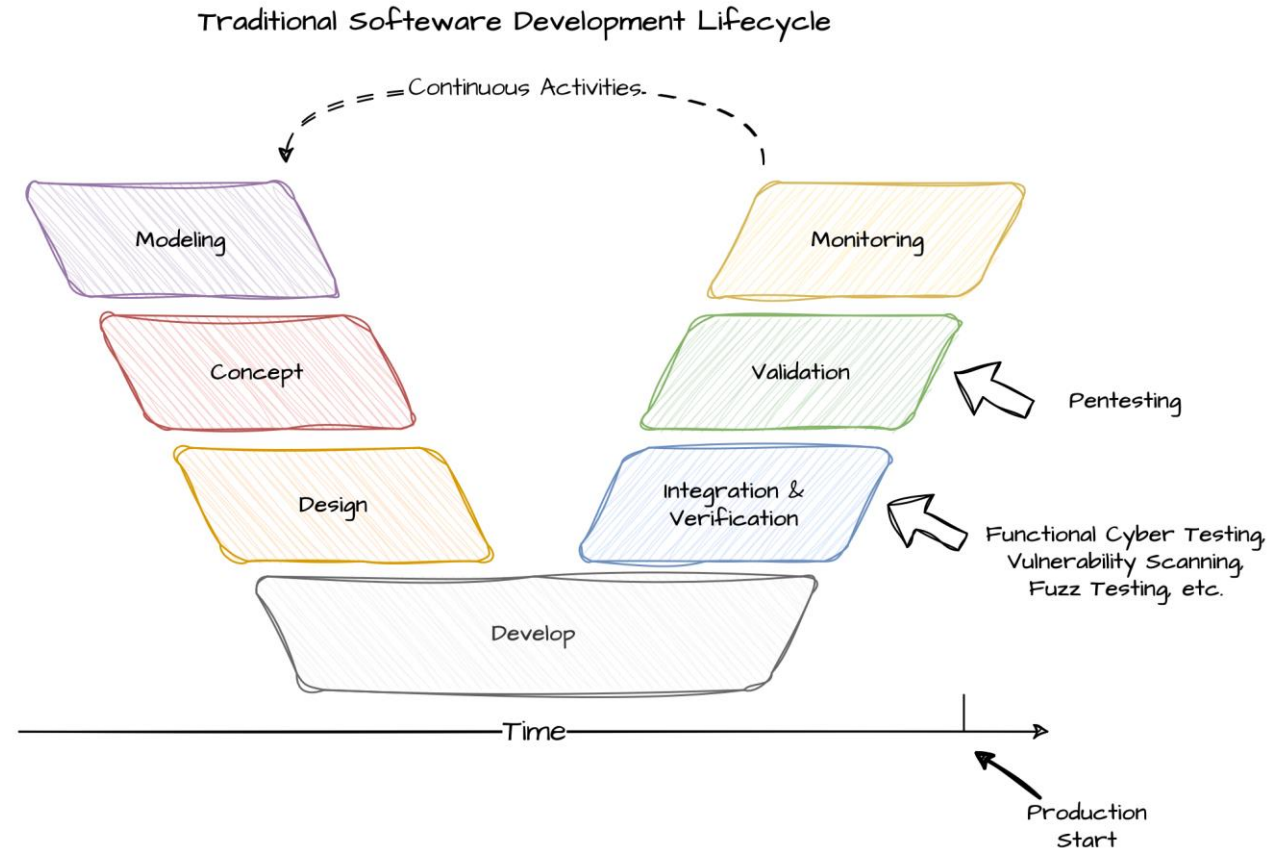
Block Harbor Cybersecurity

- Previously Embedded Cybersecurity Architect at Dana and Aptiv
- Typical embedded software engineer who happened to work on crypto drivers for GPUs
- Loves to go fast around corners

Security testing is challenging

Looking forward: SDV increases frequency of tests

- Lots of testing methodologies within cybersecurity
- SDV will require an increase in frequency of testing and flexibility
- Need to test earlier and explore concepts
- Difficult and expensive to test the integrated/combined security of the system



New solutions for testing are not enough

We need a solution that works for all types of testers

General Challenges for Security Testing

- Testbeds are often highly customized and short-lived, difficult/costly to rebuild a testbed
- Testers want customization and as many capabilities as possible (while remotely working)

Our Unique Challenges

- Block Harbor: Couldn't access enough skilled pentesters in local region
- Bosch Research: Couldn't access hardware benches of real ECUs and ECU networks
- **Current security testing products have interesting features but do not solve all our needs**

Nothing on the market? So, let's build our own!

Combine testing features into a better platform

Configurable, practical, and user-friendly

One platform for engineers, pentesters, and researchers

Target Use Cases

- Global teams working collaboratively on same project
- Isolating ECUs on a network without physical access
- Supporting remote engineers with specialized HW staff
- Remote access to measurement tools
- Demo security applications on real hardware

We aim to demonstrate a platform with real-world examples

**Remote Linux environment
with user access control**

**Configurable network of
ECUs in hardware**

**Centralized HW to make
testing more accessible**

**Adding custom applications
for security testing**

Vehicle Security Engineering Cloud (VSEC)



VSEC: Garage

Remote Access to Vehicle Cybersecurity Lab

Current Enterprise
BH Internal

wen_lu


ADMIN PANEL

SCHEDULE BENCH


CREATE BENCH

Search Vehicles...


Test benches



Bosch Research Bench
Hostname: buck2014vf
Interfaces: can0, eth0, wlan0, wlan1
Testing System: Cloud
Last Seen: a few seconds ago




Wireless Bench
Hostname: NUC5i5RYH
Interfaces: can0, docker0, enp0s25, wlp2s0, ...
Testing System: Cloud
Last Seen: a few seconds ago




BH CAN Bench
Hostname: 2014wk
Interfaces: can0, eth0, wlan0
Testing System: Cloud
Last Seen: a few seconds ago

Simulations

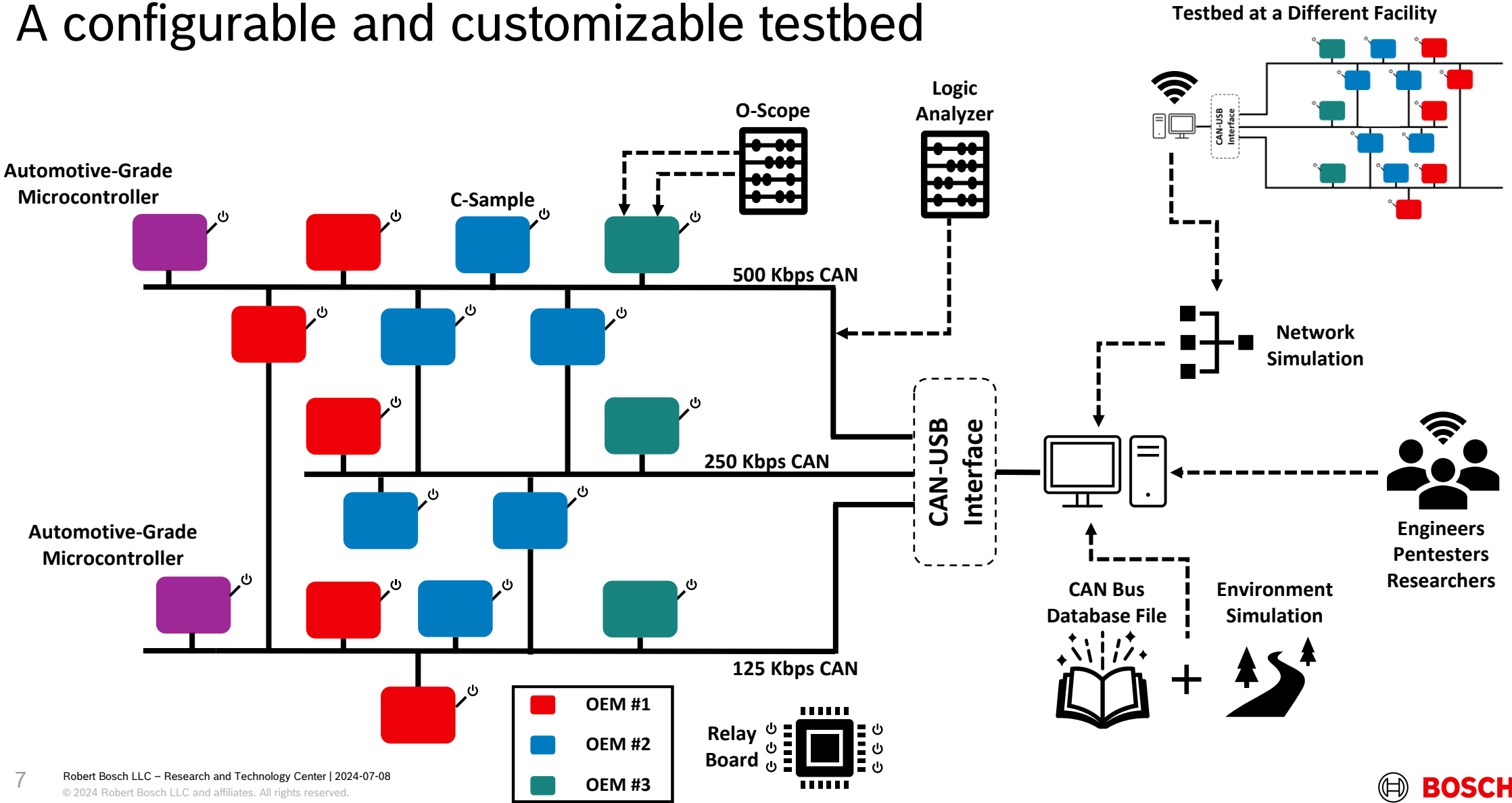


UDS Challenge (simulation)
Testing System: Cloud



User Space Diagnostics Challenge (simulation)
Testing System: Cloud

A configurable and customizable testbed

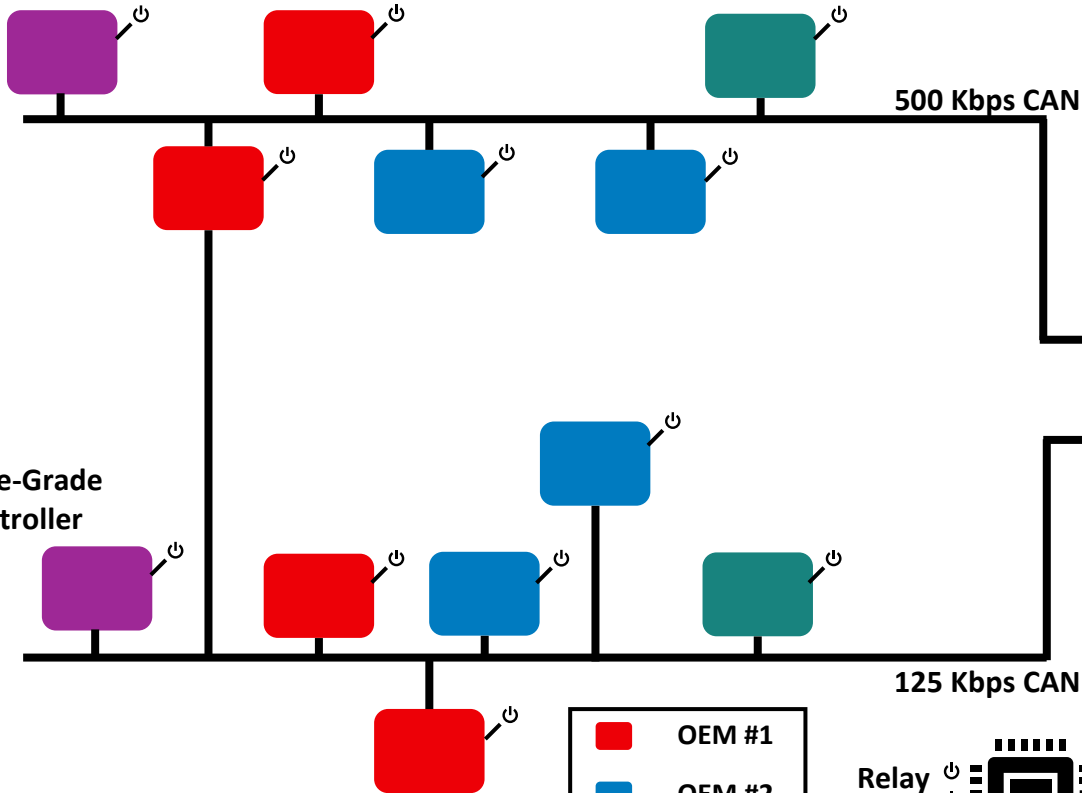


Research example #1: CANvas network mapper¹

Advantages

1. Scale # of ECUs while developing
2. Ensure mapper works with diff. OEMs
3. Microcontroller for HW-level timing

Automotive-Grade
Microcontroller



Research example #2: CANnon disruption attack²

Advantages

1. Scale # of ECUs while developing
2. Diff. OEMs transmit differently
3. Logic analyzer observes CAN bits



Researchers



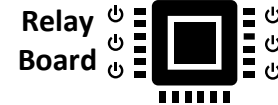
CAN-USB Interface



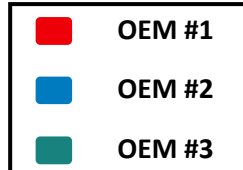
Logic Analyzer

500 Kbps CAN

125 Kbps CAN



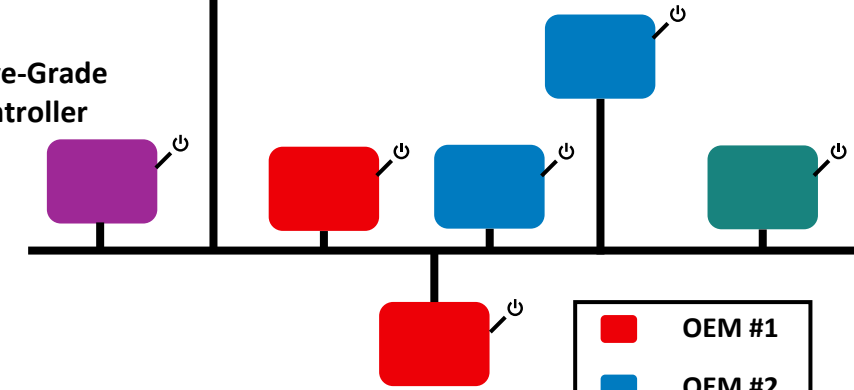
Relay Board



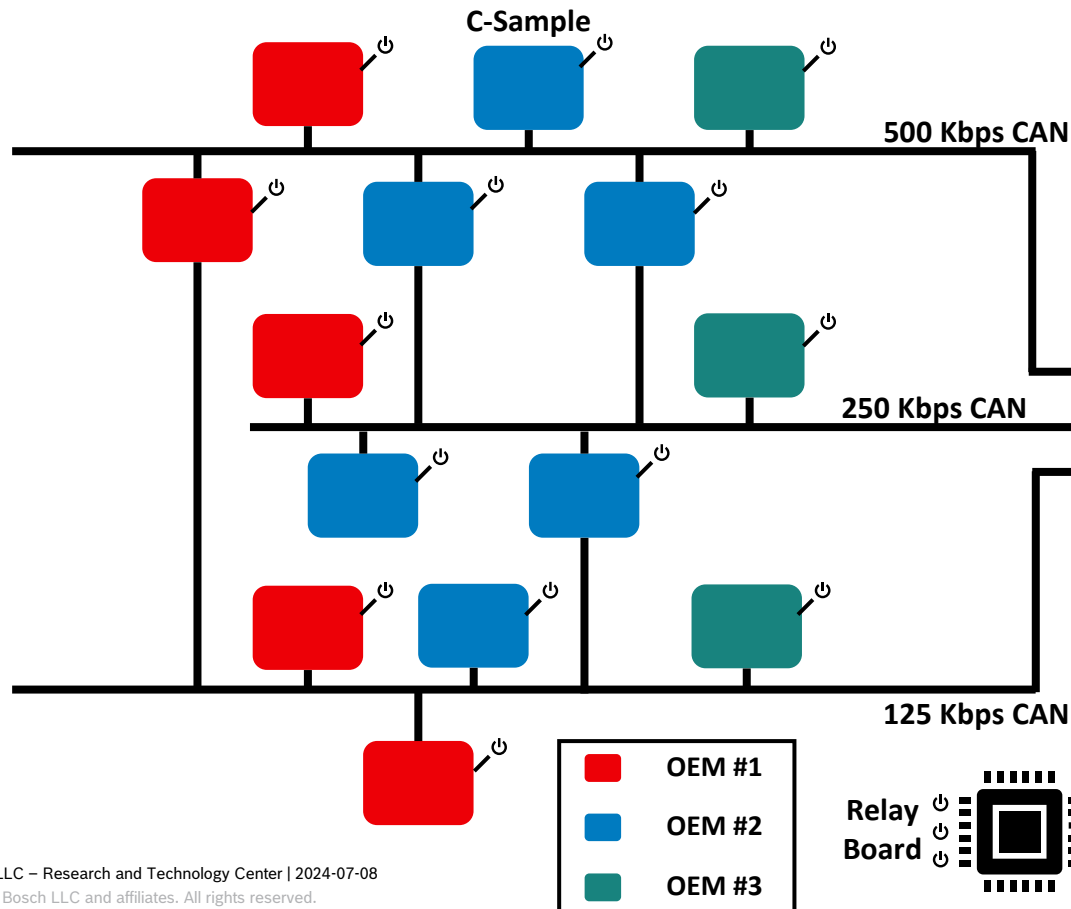
Automotive-Grade Microcontroller



Automotive-Grade Microcontroller

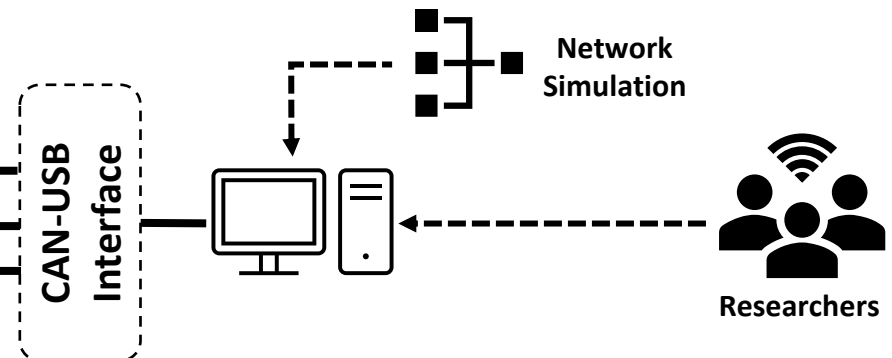


Research example #3: CANdid authentication bypass³

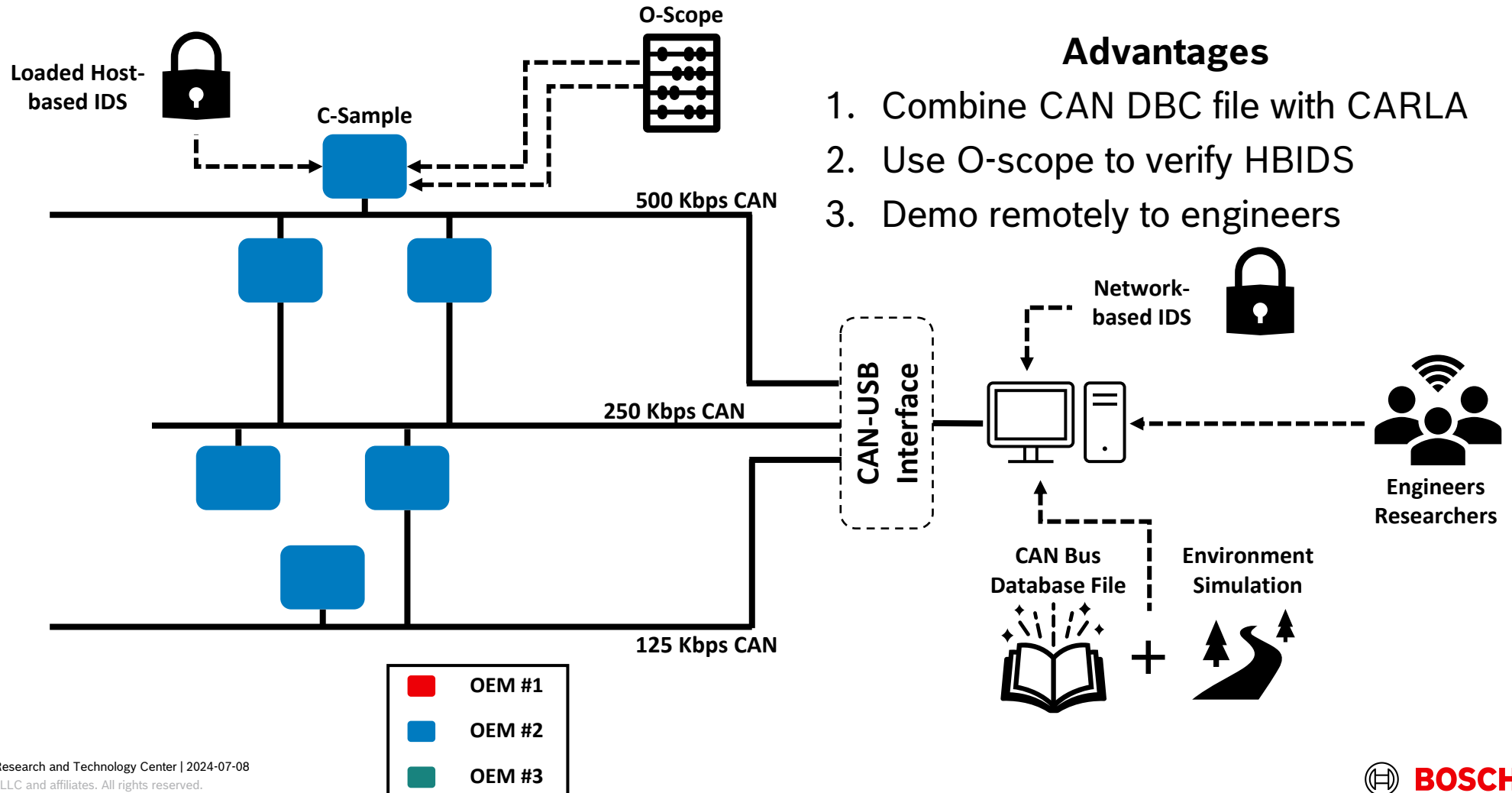


Advantages

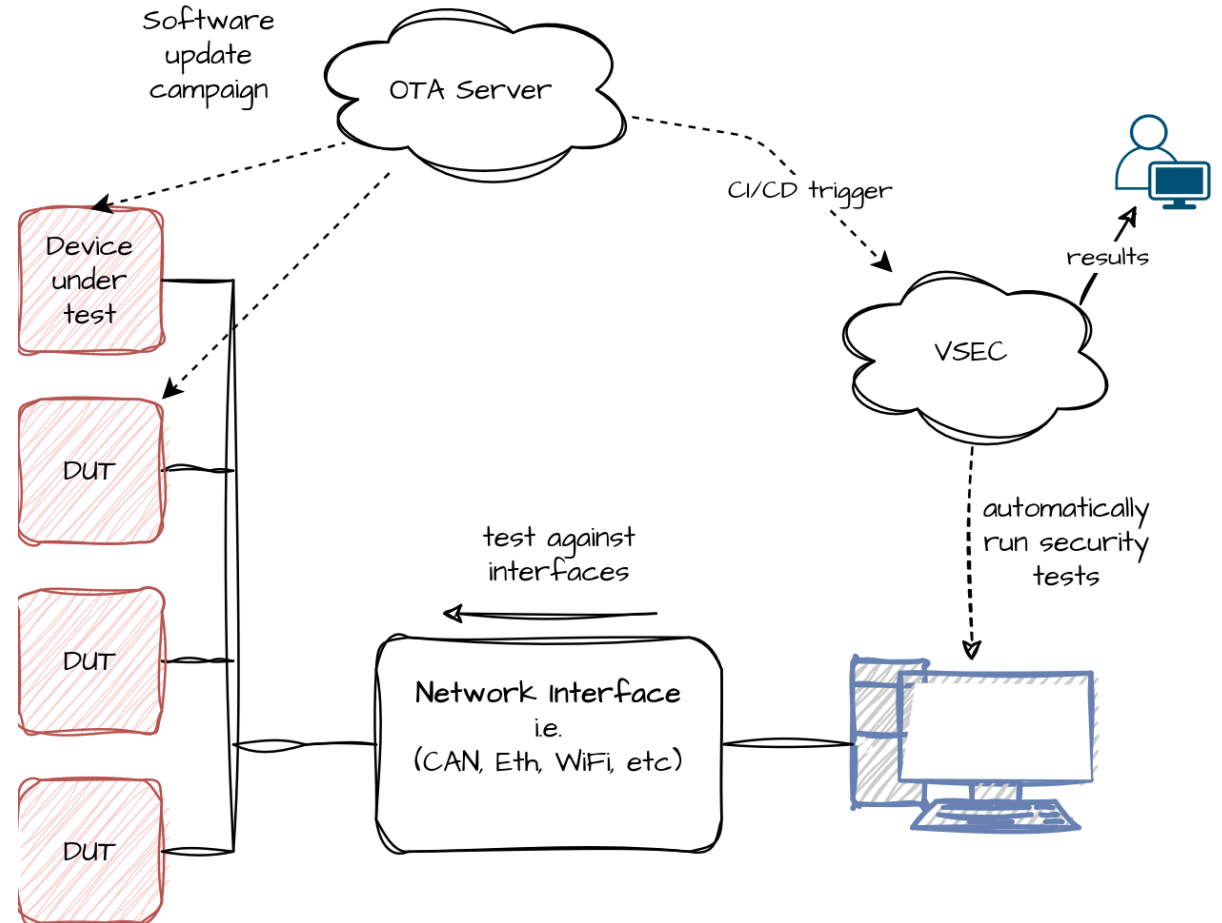
1. Simulate conn. to dealership tool
2. Access C-sample ECUs
3. Evaluate on many OEMs very quickly



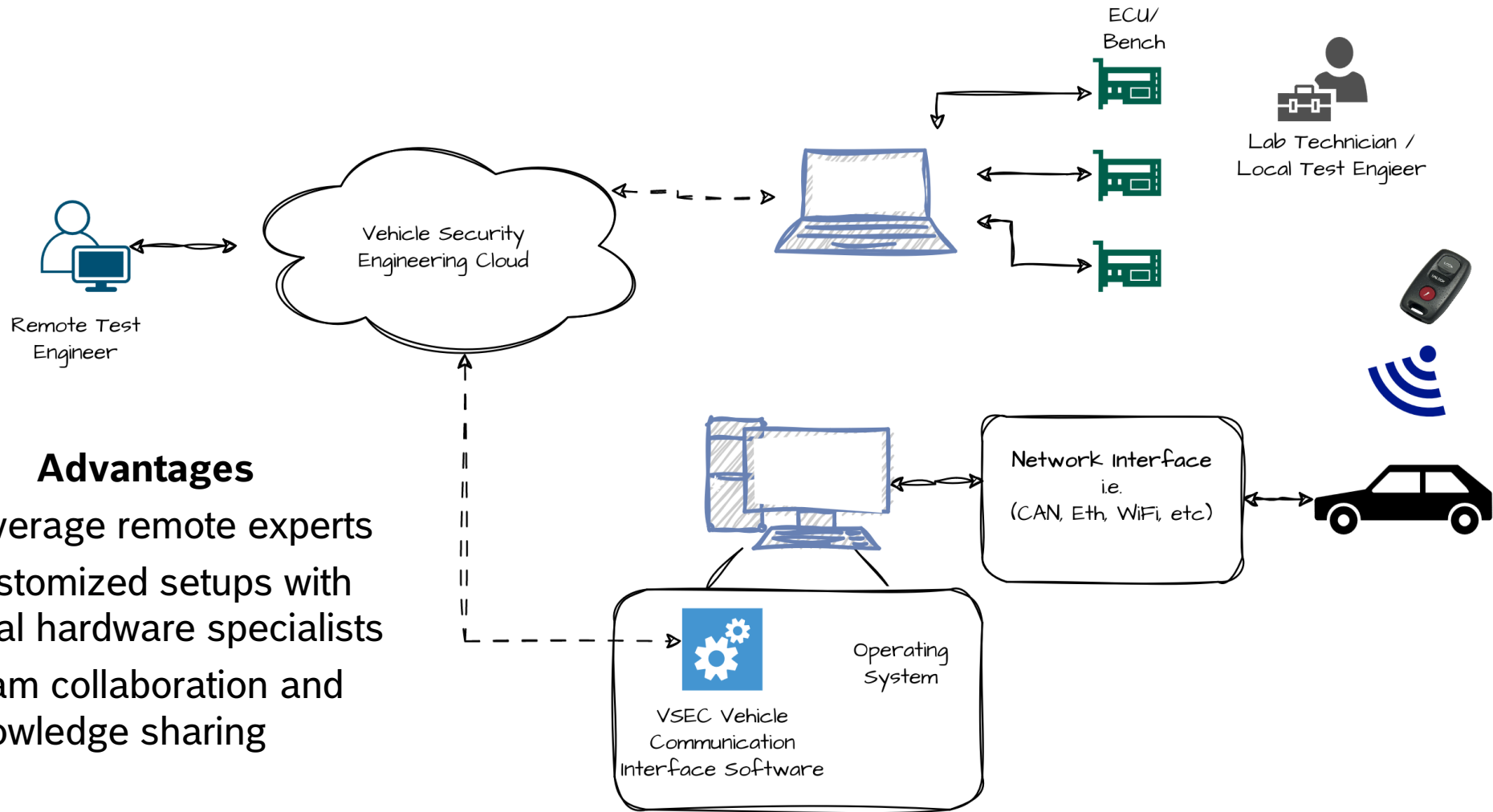
Research example #4: Demonstration of two IDSeS



Continuous Security Testing



Partner Pentesting



Advantages


1. Leverage remote experts
2. Customized setups with local hardware specialists
3. Team collaboration and knowledge sharing

VSEC Features

Bench Access

 **VSEC: Garage**
Virtual vehicle cybersecurity garage for training and testing.

Vehicle Topology

 **Bosch Research Bench**
VIN:
Available Interfaces: can0, eth0, wlan0, wlan1

Testing System: Cloud
Last Seen: a few seconds ago

Access Bench

Submit Finding

Configuration

Open Terminal

File Explorer

Go to Scheduler

```
Welcome to your VSEC Garage VCI

You are connected to buck2014vf
Available Interfaces: can0 eth0 lo tailscale0 wlan0

Check out our YouTube to get started: https://youtube.com/@blockharbor

root@buck2014vf: / # candump can0
can0 0810A000 [5] 04 FA 40 00 C0
can0 0C1CA000 [8] 00 00 00 0F 01 00 00 A8
can0 0810A000 [5] 04 FA 44 00 C0
can0 0A28A000 [8] 00 00 80 00 00 00 00 C5
can0 0810A000 [5] 04 FA 48 00 C0
can0 0810A000 [5] 04 FA 4C 00 C0
can0 0810A000 [5] 04 FA 40 00 C0
can0 0810A000 [5] 04 FA 44 00 C0
can0 0810A000 [5] 04 FA 48 00 C0
```

VSEC Features

Test Management

TEST RUNS **TEST SPECS**

Test Specifications

Demo Scan Interfaces

Demo Test Spec

CREATE TEST SPEC

Demo Test Spec

This demo test specification contains tests on common vehicle interfaces.

ADD TEST CASES CREATE TEST CASE EXPORT TO EXCEL				🔍	☰	☰	☰	🗑️
arp_query	Automotive Ethernet	{ "iface": "enp0s25", "cidr": "10.1.0.0/24" }	Sends ARP queries for all IPs in a subnet and listens for responses. ARP should not be enabled in a production state.	✎	🗑️			
supported_tls_ciphers	Automotive Ethernet	{ "iface": "enp0s25", "server": "10.1.0.2", "port": "35804" }	Iterates through all known TLS ciphers and attempts a connection to the web server with each. Accepted ciphers are reported.	✎	🗑️			
wifi_supported_auth_types	WiFi	{ "iface": "wlp2s0", "ssid": "Hotspot", "bssid": "" }	The test will look for weak authentication types on a detected WiFi Access Points	✎	🗑️			
uds_service_scan	CAN	{ "device": "can0", "extended_id": "false", "req_arb": "0x456", "resp_arb": "0x656" }	Probes for UDS services on a UDS Server by sending a payload of each valid service ID to the server, and watching for a positive or negative response.	✎	🗑️			
uds_comm_control	CAN	{ "device": "can0", "extended_id": "false",	Attempts to toggle the communication state of a module via UDS. Disabling communication of a module can cause	✎	🗑️			

Rows per page 10 ▾ 1-10 of 12 < >

VSEC Features

Test Execution

TEST RUNS TEST SPECS

Test Specifications:

- Demo Scan Interfaces
- Demo Test Spec

Bench Name:

- Bosch Research Bench
- Wireless Bench
- BH CAN Bench
- UDS Challenge
- User Space Diagnostics

Challenge

CREATE TEST RUN

▼	Wireless Bench	Demo Scan Interfaces	✓	1 ✓ 0 ✗ 0 ⚠	🗑️
▲	Wireless Bench	Demo Test Spec	✓	8 ✓ 3 ✗ 2 ⚠	🗑️

DHCP Query Scan
Results: DHCP Query Complete
DHCP inactive on the network. Test passed

Check Internet Forwarding
Results: Internet Forwarding Test Complete
Connected to 1.1.1.1 port 53 via enp0s25
Connected to 8.8.8.8 port 53 via enp0s25
Internet connections forwarded. Test failed

Supported TLS Cipher Scan
Results: Supported TLS Cipher Scan Complete
Allowed Cipher Suites:

Rows per page 10 1-4 of 4 < >

Conclusions

- Easier shared access to logistically challenging and costly hardware
- Access to larger (global) talent pool and accessible to more engineers
- Cloud-based platform reduces costs, increasing participation in Bug Bounties

- The ideal platform is one that is used and implemented AND can adapt/be flexible in the future
- Multiple demos of real enabled testing methodologies for engineers, pentesters, and researchers

[Sekar Kulandaivel*, Wenjuan Lu[§], Brandon Barry[§], and Jorge Guajardo*. "Towards a New Configurable and Practical Remote Automotive Security Testing Platform." arXiv preprint arXiv:2404.02291 \(2024\).](#)

Bosch*: sekar.kulandaivel@bosch.com

Block Harbor [§]: wen@blockharbor.io