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

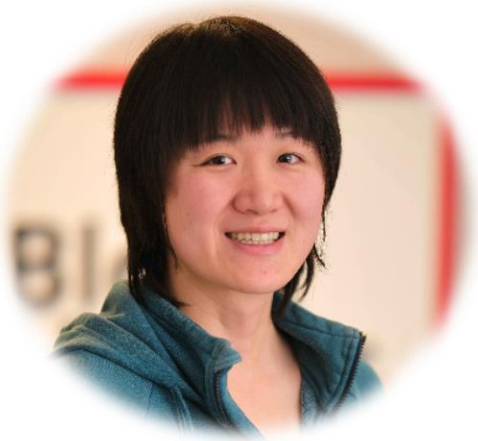
BOSCH

Our background

Research Engineer

Robert Bosch – Research & Technology Center

- Previously ProdSec Lead at Locomation
- 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



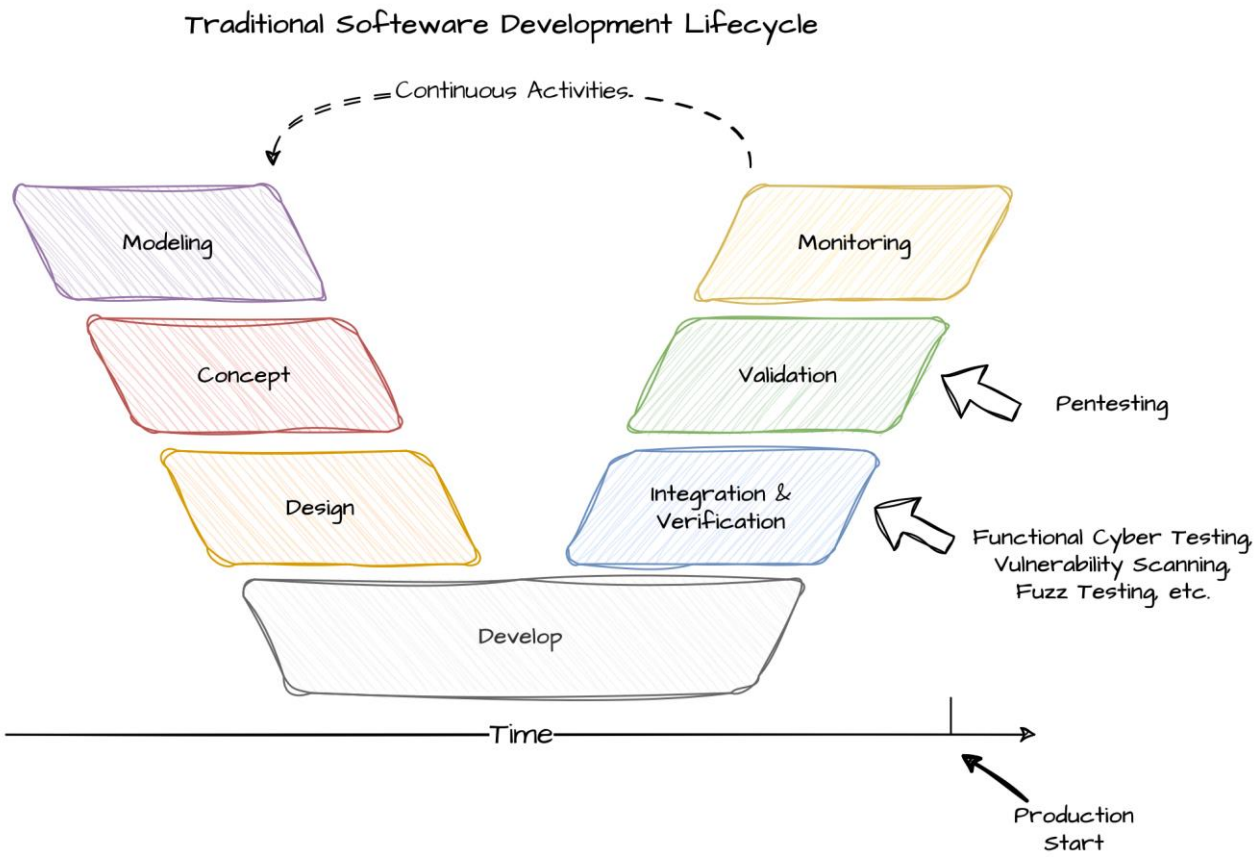
Director of Product

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

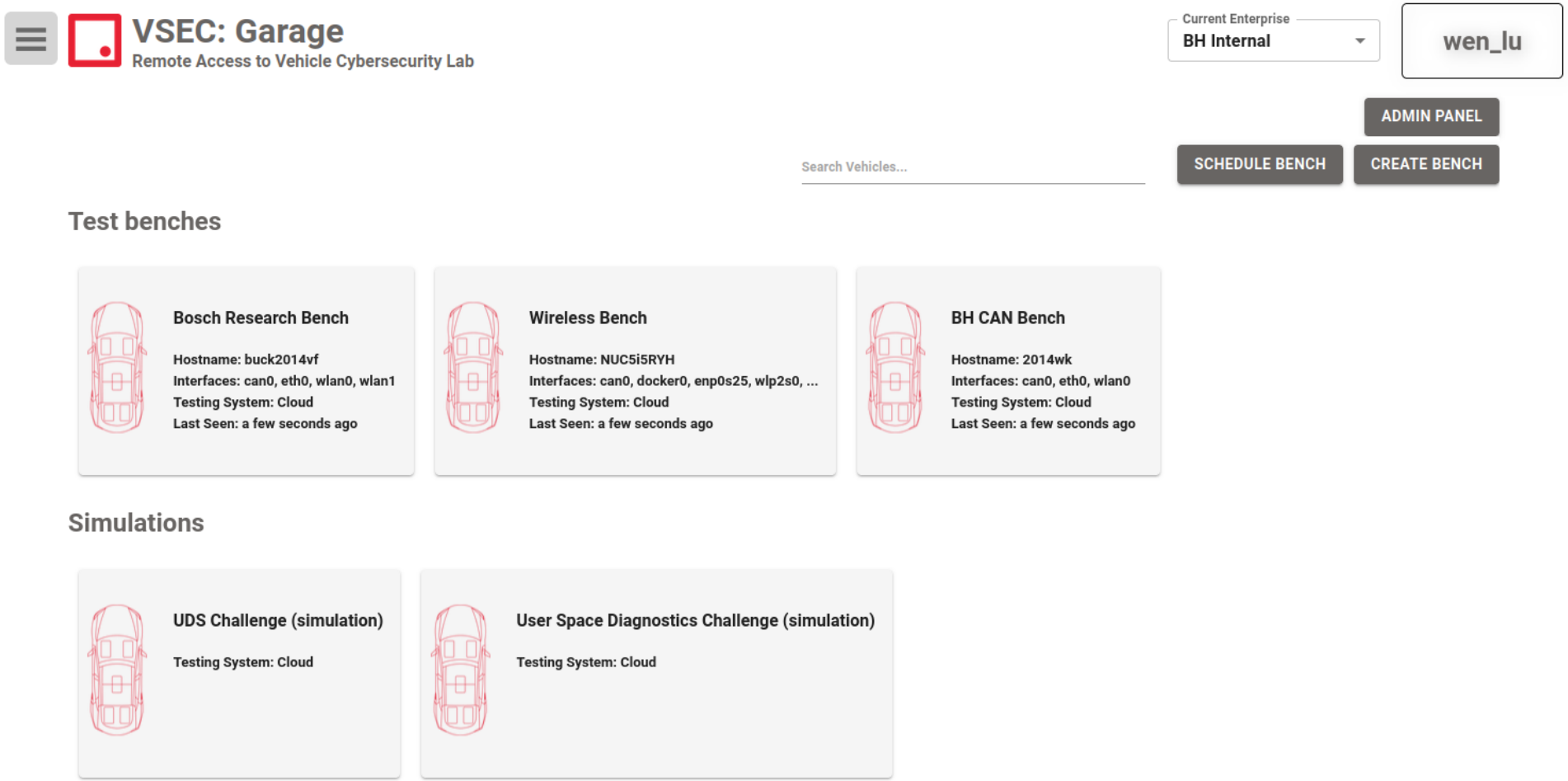
Remote Linux environment with user access control

Configurable network of ECUs in hardware

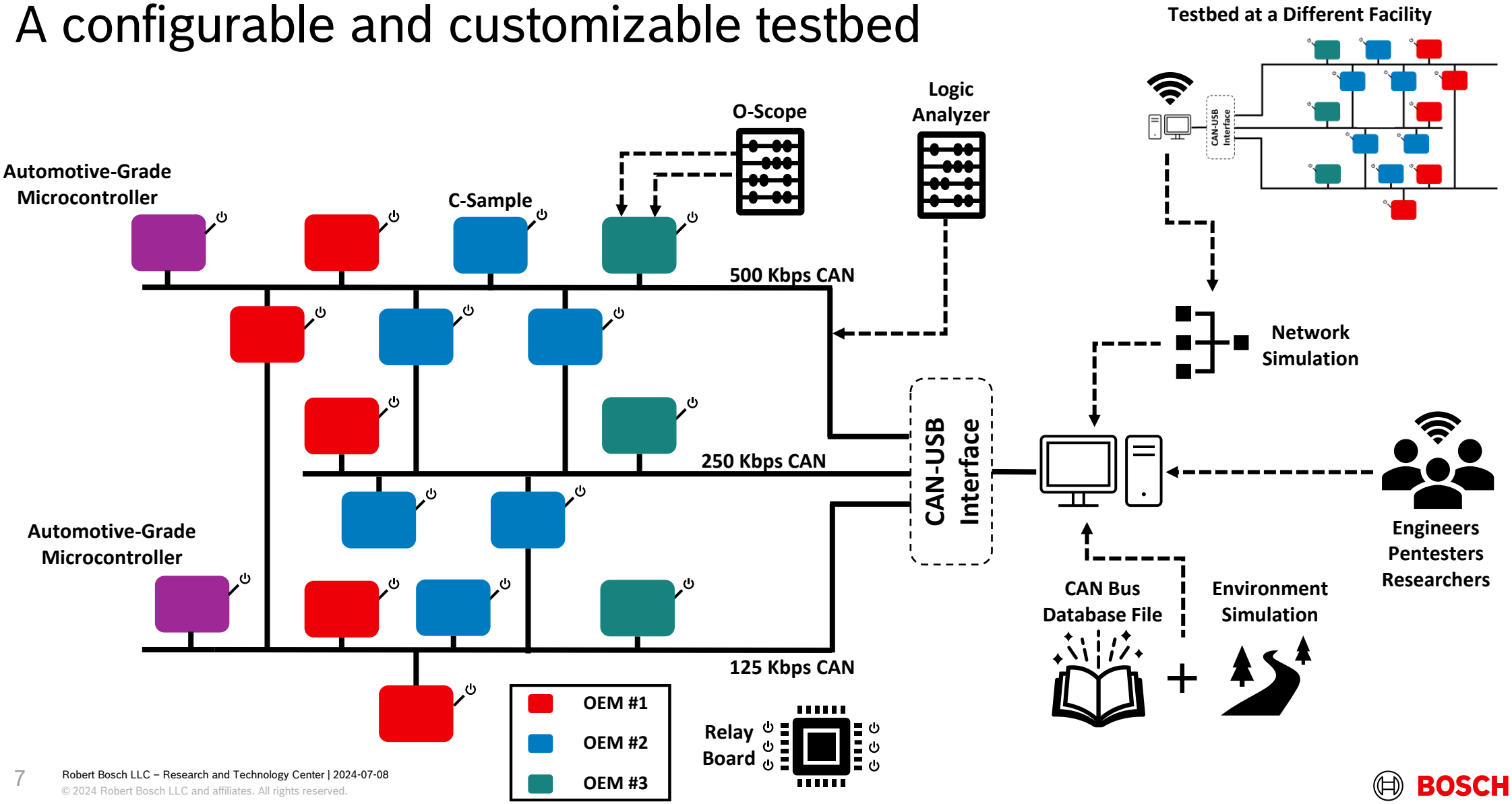
Centralized HW to make testing more accessible

Adding custom applications for security testing

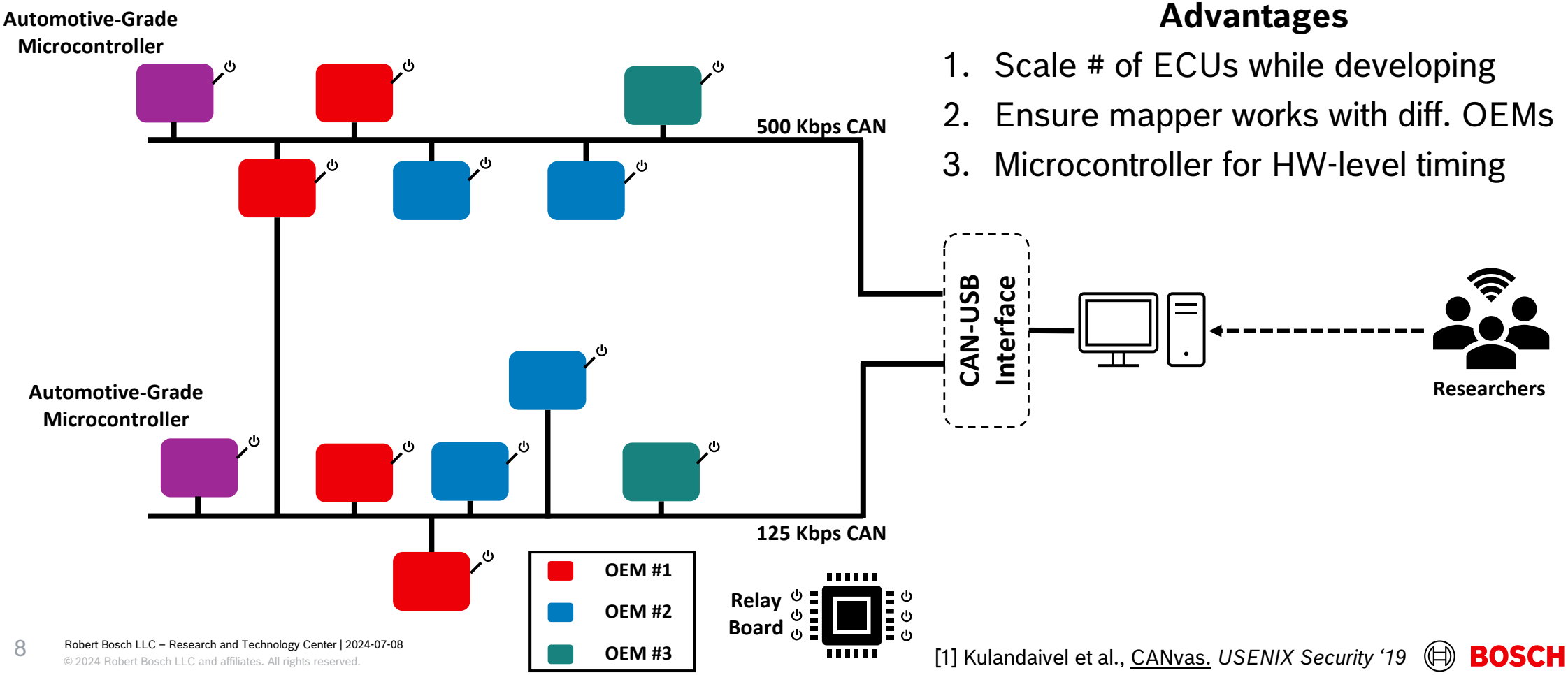
Vehicle Security Engineering Cloud (VSEC)



A configurable and customizable testbed



Research example #1: CANvas network mapper[1]

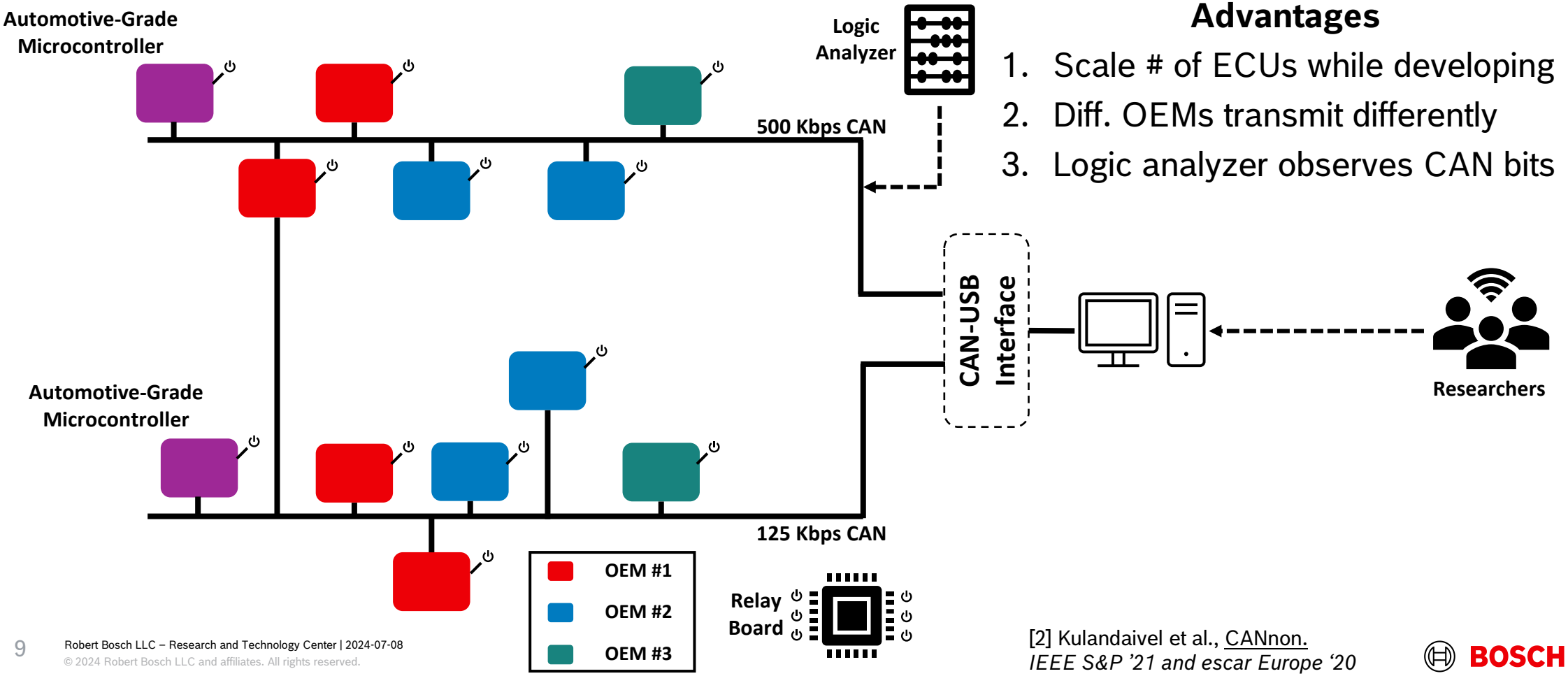


Advantages

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

[1] Kulandaivel et al., CANvas. *USENIX Security '19*

Research example #2: CANnon disruption attack[2]

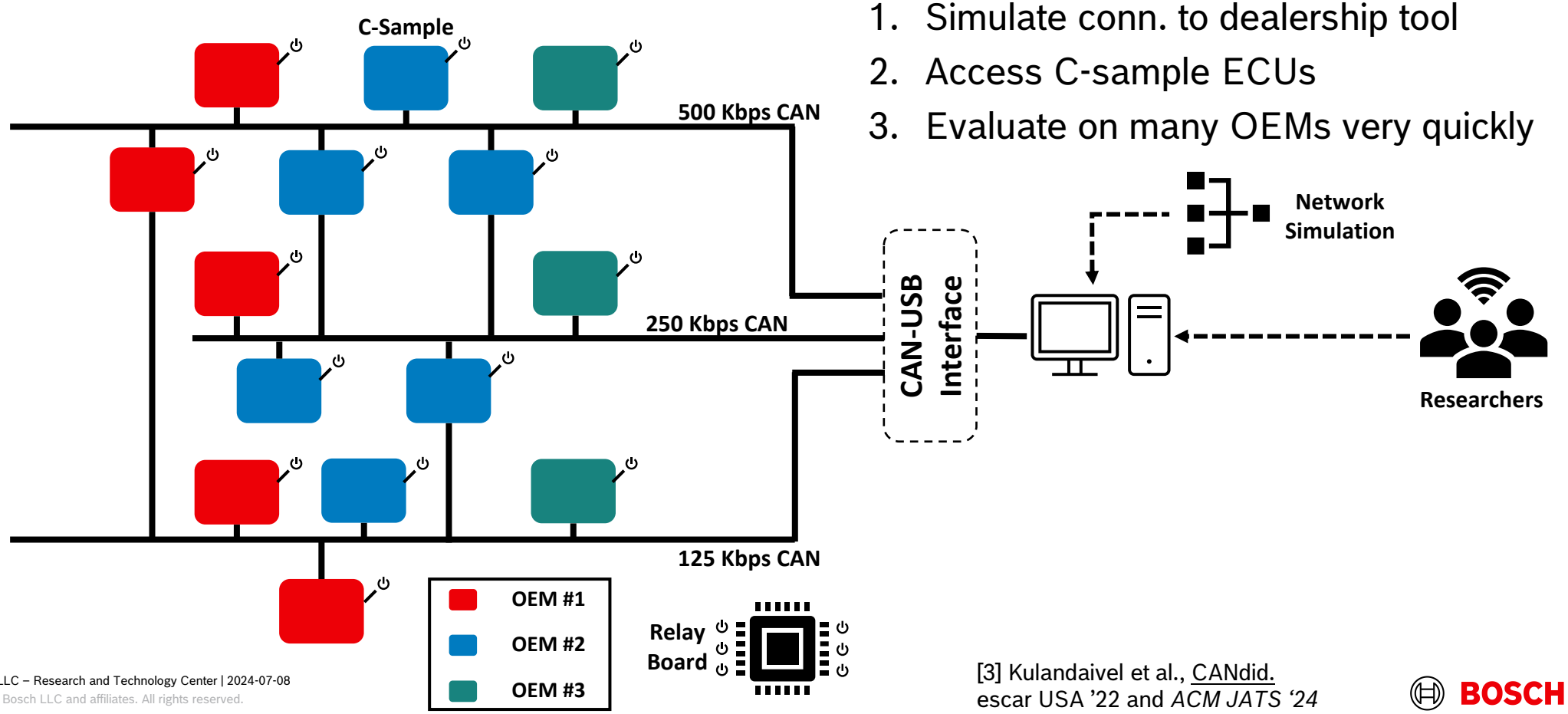


Advantages

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

[2] Kulandaivel et al., CANnon.
IEEE S&P '21 and escar Europe '20

Research example #3: CANdid authentication bypass[3]

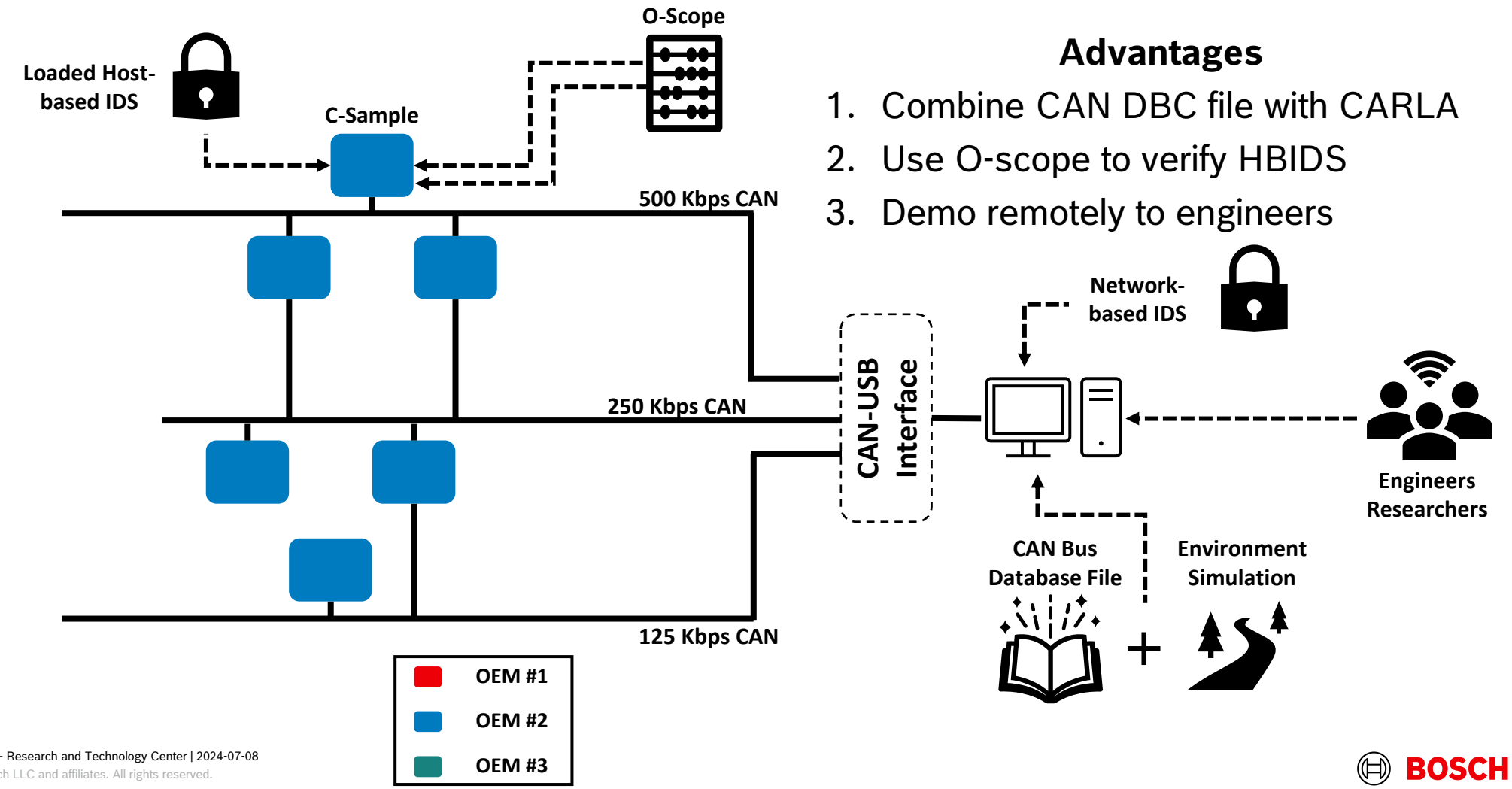


Advantages

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

[3] Kulandaivel et al., CANdid. escar USA '22 and *ACM JATS '24*

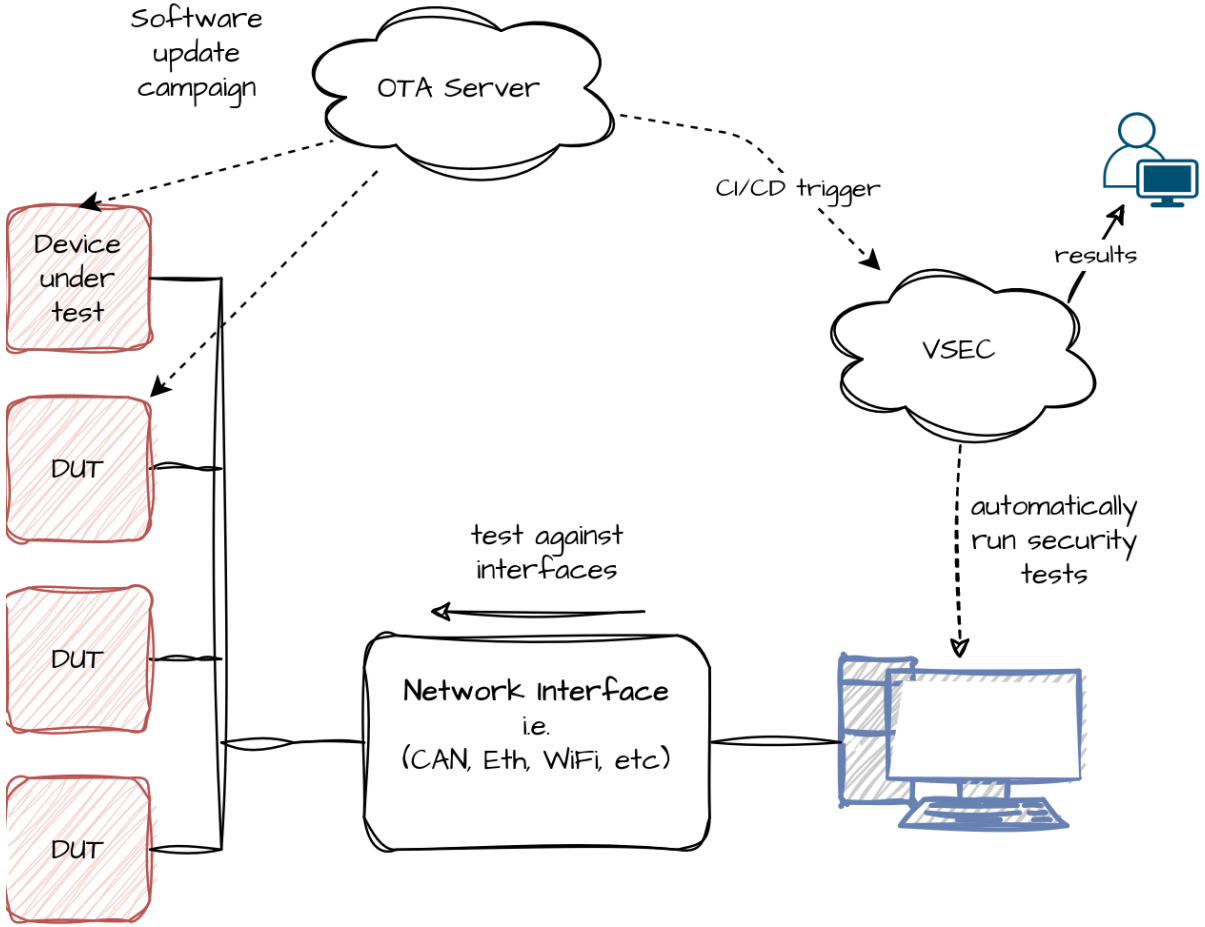
Research example #4: Demonstration of two IDSes



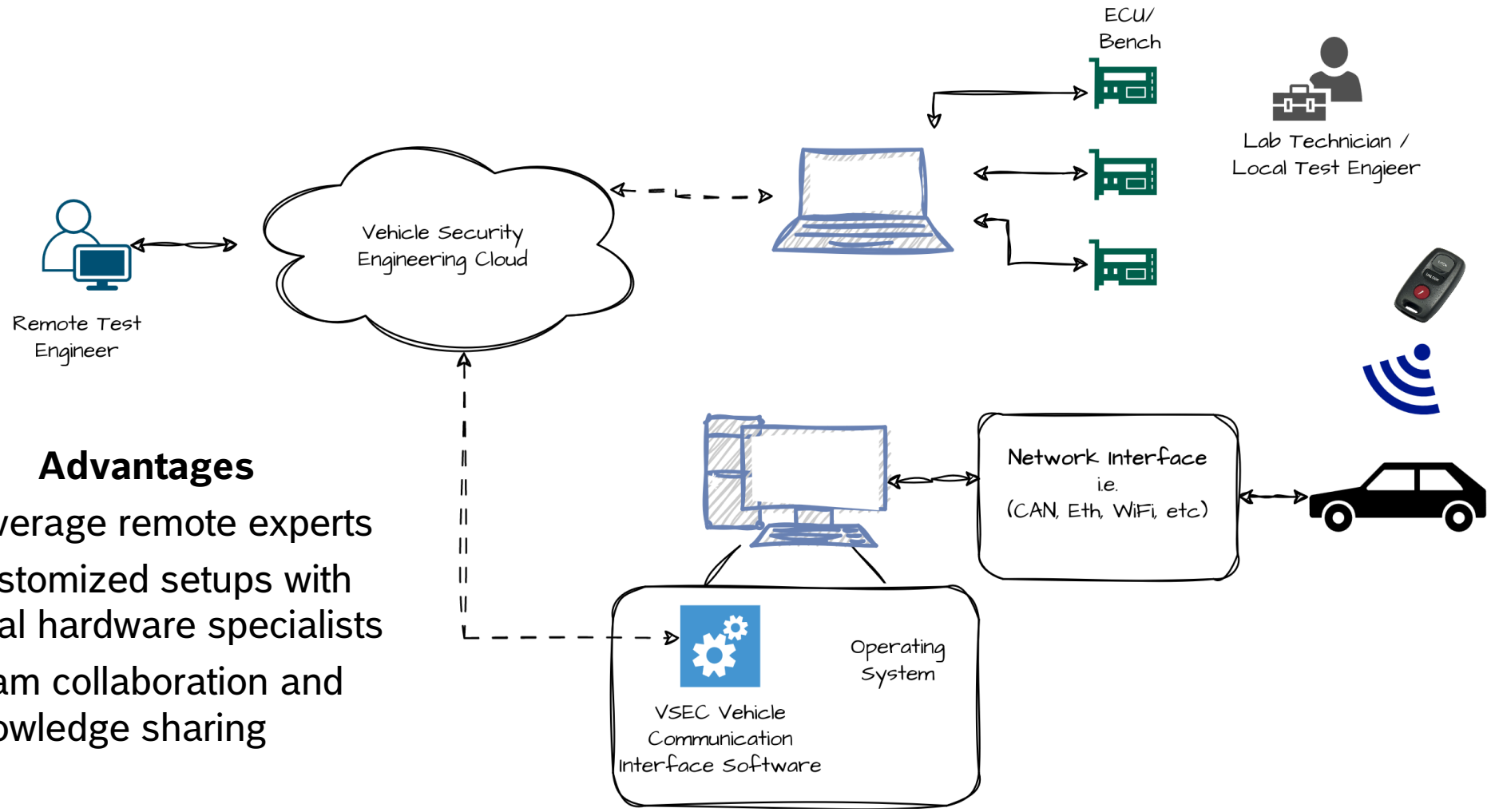
Advantages

1. Combine CAN DBC file with CARLA
2. Use O-scope to verify HBIDS
3. Demo remotely to engineers

Continuous Security Testing



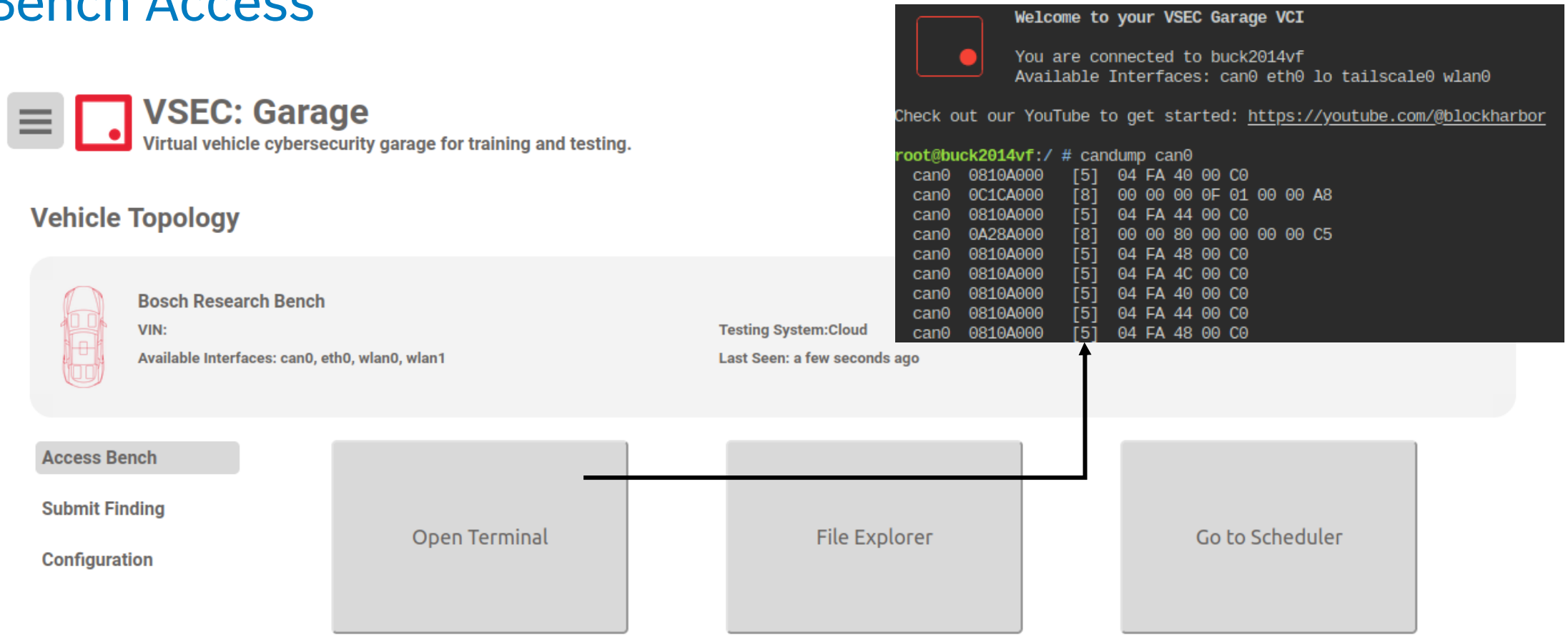
Partner Pentesting



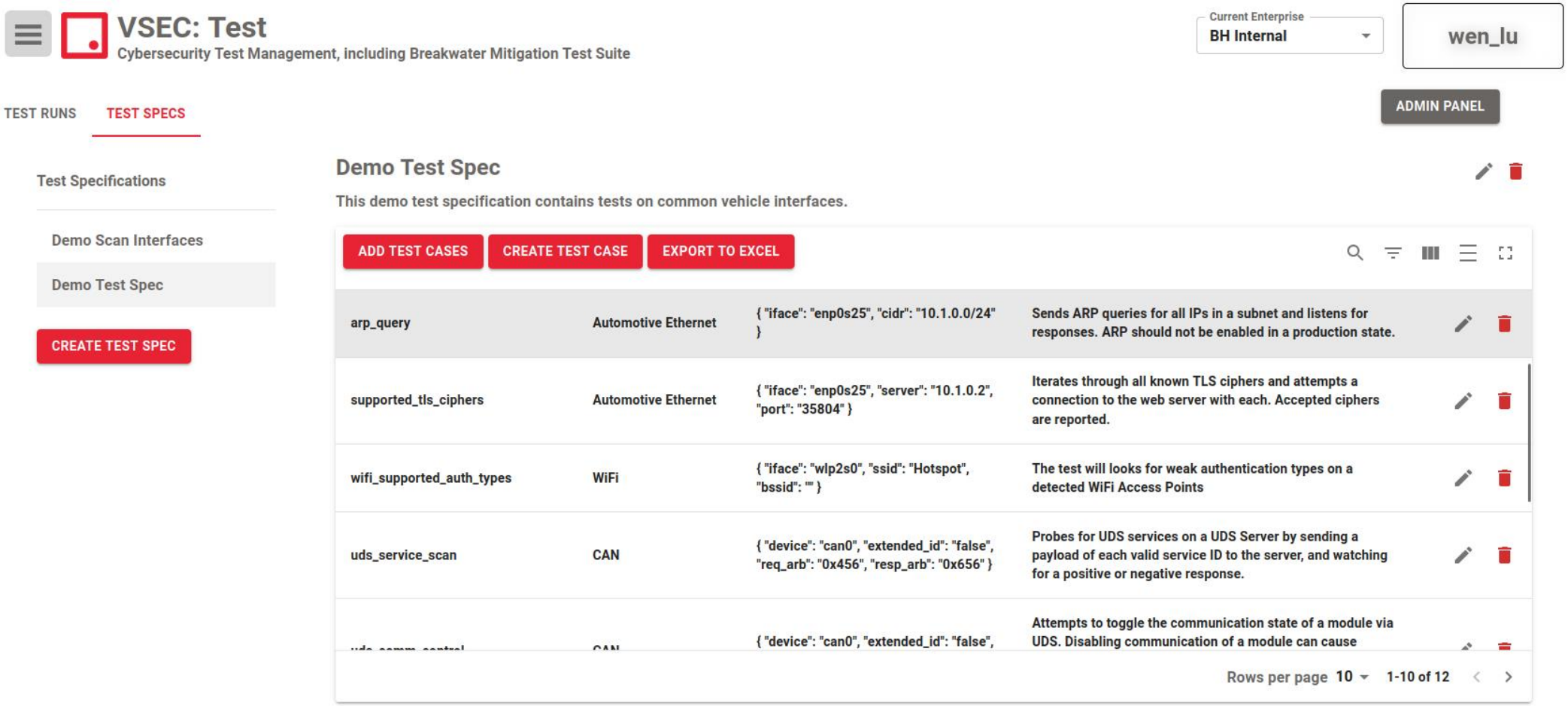
Advantages

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

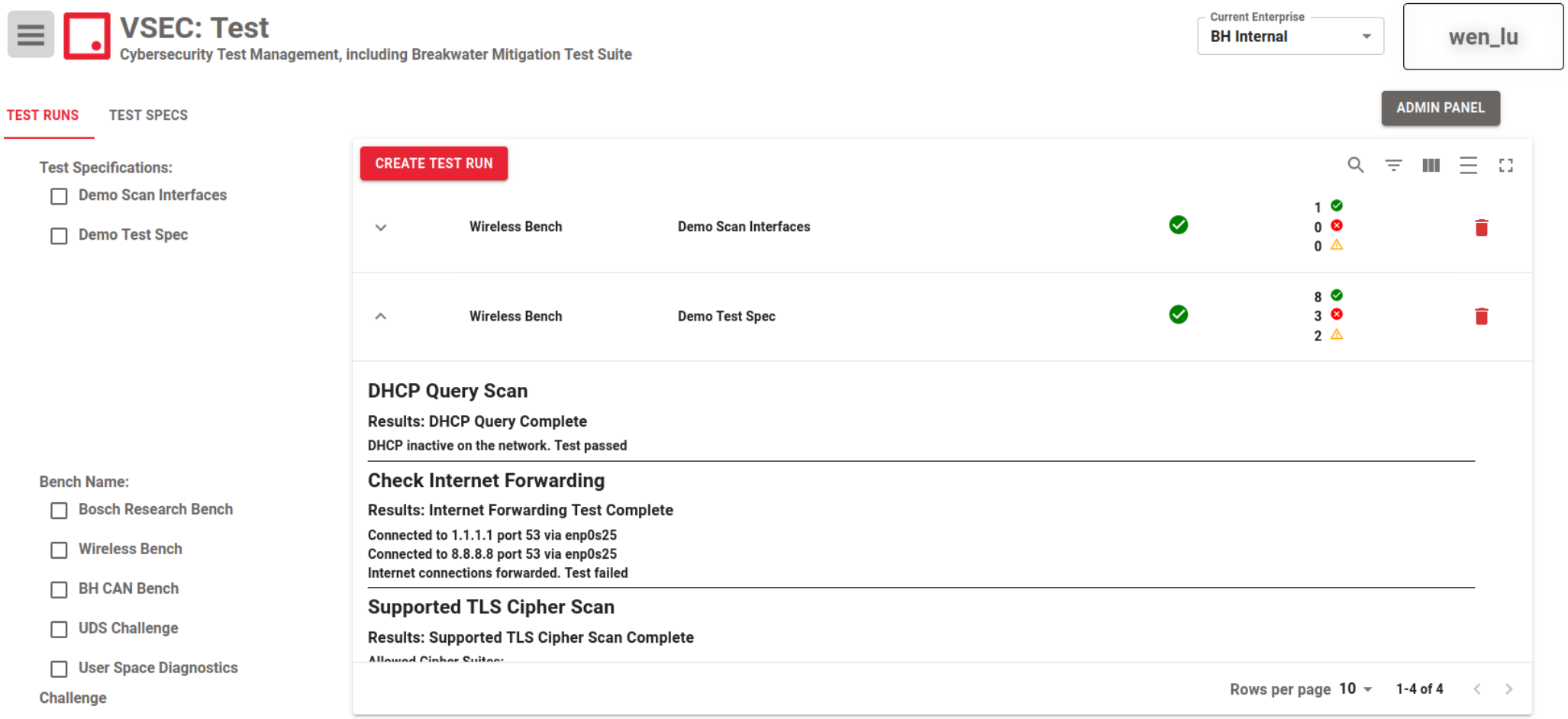
VSEC Features
Bench Access



VSEC Features
Test Management



VSEC Features
Test Execution



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**