Cybersecurity Testing Solutions

Automotive Cybersecurity Test Benches

Don't Let Your Sub-System be a Warranty Liability

The Danlaw cybersecurity test bench provides a clean and compact test platform, which is a much better and cheaper alternative to a vehicle. The use cases range from pure fuzzing, to compliance testing, and research activities.

Fuzzing

While Danlaw provides fuzzing as a service, some customers may want to do it themselves. With the cybersecurity test bench, the ECU to be fuzzed is connected with other vehicle modules, allowing it to behave the way it would in the vehicle. The bench exposes the various attack surfaces, allowing the fuzzing of the interfaces and protocols of interest.

Penetration Testing

Penetration testing is an exhaustive post- breach exploitation based on a small set of attack vectors. The cybersecurity test bench allows custom penetration testing activities to be performed in the lab. Such back box testing activities can then be executed in an environment that is both open and more manageable than a vehicle.

Cybersecurity Research Activities

Cybersecurity test benches provide an open framework for the study and characterization of particular types of attacks during certain operation modes, such as ignition cycles and diagnostic interactions. It encourages the study of cybersecurity alternatives.

Overview

- Open access provided for the various attack surfaces: CAN, Ethernet, USB, BT, RF, and other connections
- Open access for external instrumentation to support start up sequences, transients, fuzzing, and penetration testing
- Ability to easily reproduce tests, experiments, and results
- Custom-designed to fit your application and budget

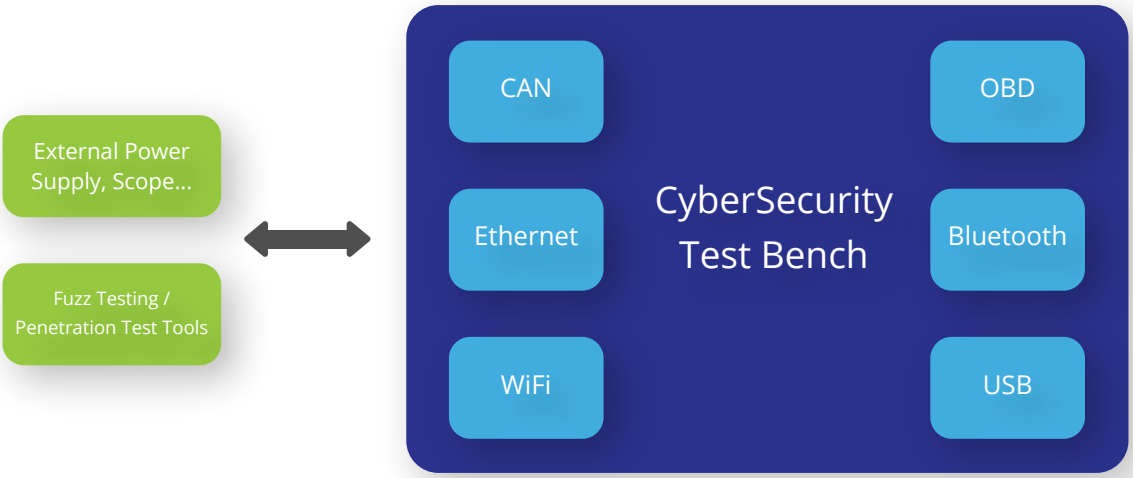
Danlaw has built hundreds of automotive test benches for various OEMs and Tier suppliers providing an expandable and scalable solution that takes the worry out of the in-house build and maintenance process.

Contact Us

Danlaw, Inc.
41131 Vincenti Court
Novi, Michigan 48375 USA
Tel: 1 (248) 476-5571
Fax: 1 (248) 471-4485
solutions@danlawinc.com

Attack Surfaces

Cybersecurity attack surfaces are the ways a cyber-physical system, such as a vehicle, can be accessed.



Bench Content

The cybersecurity test bench includes all the modules that compose a modern automotive infotainment sub-system. The modules are production units that have been wired per the OEM specification, offering a complete turn-key solution. No other external hardware/software is provided.

Common Use Cases

- Fuzz testing of any module on the bench
- Penetration testing of any module on the bench
- Study of sub-system behavior during power off/power on transients
- Study of sub-system behavior at various voltages

Connectivity to the bench

Access points to the attack surfaces are provided on the cybersecurity test bench:

- CAN: via dedicated connector
- Ethernet: via Automotive Ethernet connection point
- OBD: via standard 16-pin OBD connector
- USB: via standard USB connector

Contact Us at: solutions@danlawinc.com

Contact Us

Danlaw, Inc.
41131 Vincenti Court
Novi, Michigan 48375 USA
Tel: 1 (248) 476-5571
Fax: 1 (248) 471-4485
solutions@danlawinc.com