dissecto
A dSPACE COMPANY

Workshops

Stay ahead in the evolving automotive landscape with our cybersecurity workshops, designed to empower you with **practical, hands-on** skills and insights into embedded and vehicle security.

Explore the fundamentals of automotive protocols, ECUs, and attack surface identification. Learn cutting-edge techniques in hacking real cars, from firmware reverse engineering to OEM design philosophies. **Fully customizable**, our workshops ensure you gain the expertise to safeguard interconnected vehicles against emerging cyber threats.

Features:

- **Attack Surface Identification:** Learn to pinpoint vulnerabilities on Electronic Control Units (ECUs) for effective security assessments
- **Low-Level CAN Communication:** Understand the intricacies of CAN communication and vulnerabilities at the protocol's foundational level
- **Vehicle Architecture Overview:** Gain insights into prevalent vehicle architectures and network topologies for comprehensive understanding
- **Relevant Protocols Mastery:** Acquire knowledge about essential protocols utilized in contemporary vehicles for targeted security analyses
- **Hands-On Network Scanning:** Engage in practical automotive network scans to identify potential vulnerabilities and weaknesses
- **Diagnostic Protocol Exploitation:** Explore techniques to attack diagnostic protocols, including firmware dumping and reverse engineering for in-depth analysis
- **Security Access Breaching:** Break through security access mechanisms deployed in modern vehicles to assess system vulnerabilities effectively
- **Immobilizer Basics:** Get an overview about current immobilizer systems
- **Forensics:** Training in data acquisition and analysis for incident response and forensic investigations
- **Bring Your Own ECU:** Participants are welcome to bring their own control unit – we'll integrate it into the training and tailor the exercises accordingly
- **Automotive Ethernet Expertise:** Benefit from in-house specialization in Automotive Ethernet security testing, supported even by dedicated tooling (dissecto HydraLink)

Exercise Environment

Remote ECU: The remote system facilitates the handling of the ECUs by avoiding wiring efforts. Available Manufacturers: BMW, VW, Opel, Tesla, Mercedes, Audi. Available ECU types: Body Domain Controllers, Gateway ECUs, Telematics ECUs, Airbag ECUs, Dashboard ECUs, Immobilizer ECUs

Physical ECU: Various ECUs will be brought on-site for training in hardware reverse engineering and handling

Virtualized Vehicle: By simulating a vehicle and CAN messages while driving, participants can learn how to handle and manipulate low-level CAN messages

Virtualized ECU: A modified digital twin of a real ECU, which includes various IT security exercises that can be performed by the participants independently

Security Testing, simplified.

www.dissecto.com

dissecto
A dSPACE COMPANY

Workshops

Module Outline

- **Fundamentals of vehicular networks and protocols**

- **Controller and Networks**
  - Low-Level Attacks
  - Scapy CAN layer
  - DBC file format
  - MITM attacks
  - AUTOSAR SecOC
  - Fuzzing techniques

- **ISOTP**
  - Basics
  - MITM attacks
  - Network Scanning

- **UDS/GMLAN**
  - UDS and GMLAN in Scapy
  - Security Access
  - Network Scanning

- **DoIP / HSFZ**
  - Basics of protocols
  - DoIP and HSFZ in Scapy
  - Handling and tools

- **SOME/IP**
  - Basics of SOME/IP
  - Tools

- **CCP / XCP / OBD2**

- **OEM-specific knowledge**
  - Attacks on vehicles
  - Security access implementations
  - Update processes
  - Overview of OEM-specific tools
  - Electronic immobilizers

- **Reverse Engineering**
  - Identification of interfaces
  - Ghidra basics
  - Overview of common processor architectures
  - Handling memory maps
  - Reverse engineering of peripheral components
  - Basics of JTAG
  - Handling of interrupt vector tables
  - Identification of automotive protocols e.g. UDS
  - Reverse engineering of security access algorithms
  - Ways to read out firmware
  - Intercommunication of bootloader and flashloader
  - Reverse engineering of state machines and AUTOSAR

- **Automotive Ethernet Security Testing**
  - Explore Ethernet-based ECU communication
  - IP discovery
  - VLAN configuration
  - SOME/IP and AUTOSAR traffic analysis
  - DoIP-based diagnostic interactions
  - certificate testing workflows
  - hands-on vulnerability assessment using tools such as Scapy, Wireshark, nmap, testssl.sh, and dissecto HydraLink