fact sheet

Training - Automotive Networks-, Controllers & Systems

Automotive Security is becoming more and more important, but entrance into this research field is still very difficult. This training covers basics of automotive protocols and systems which are required to understand all details and specialties of attack surfaces on modern ECUs. We provide physical ECUs for hardware reverse engineering and explanation, a virtualized and remote environment to overcome the usual difficulties during practical work on hardware systems.

In the automotive industry, every OEM has its own design philosophy. We introduce relevant tools and background information, necessary for the hacking of real cars and ECUs. Furthermore, we introduce basics on firmware reverse engineering of automotive systems. Last but not least, we show automation strategies for automotive network security and system security assessments.

key learning objectives

- How to identify attack surfaces on ECUs
- Understand low level CAN communication and attacks
- Obtain an overview on common vehicle architectures and network topologies
- Know the most relevant protocols in current vehicles
- Receive hands-on experience in automotive network scans
- Attack diagnostic protocols, including firmware dumping and reverse engineering
- Break security access mechanisms in some current cars
- Execute your own code on insecure ECUs
- Get an overview on tool chains of OEMs and their software update mechanisms
- Know basics about current immobilizer systems

requirements

- Laptop with Wi-Fi/ Ethernet and root privileges
- (Arch) Linux is the preferred OS
- SSH client
- Installation of latest Ghidra version
- Installation of Wireshark and Python3
- CAN interface with Linux support
- TTL-to-USB cable, JTAG adapter (optional)
- ECU for investigation (optional)

prerequisites

- Basic knowledge of programming (C, Python)
- Basic knowledge of Linux
- Basic knowledge of embedded systems is a plus, but not required
- Basic knowledge of firmware reversing with Ghidra is a plus, but not required
- Basic knowledge of Wireshark or Scapy is a plus, but not required

dissecto

module outline

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

exercise environment

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

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

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

Physical ECUs
Various ECUs will be brought on-site for training in hardware reverse engineering as well as handling ECUs.