Date | Version: 18.12.2023 | 1.0 |
Responsible: T. Weber

CyberDanube:
Automotive Pentesting

In-Depth Technical Security Assessments of Automotive Hardware

Electronic Control Units (ECUs) are used in every part of modern cars. Especially for vehicles with ADAS technologies, security of electronic systems is just as important as safety. Protection and testing of such electronic components does not only prevent IP theft, it can save life.

Preparation

- Kick-off Appointment
- Typically three hardware devices (ECUs)
- If possible development ECU
- If possible Adapters for custom interfaces
- Restbus/remaining bus simulation & license

The preparation phase of an Automotive/ECU technical security assessment includes a scope definition during a kick-off appointment. Frame conditions like the number of available ECUs, available development ECUs and restbus/remaining bus simulation software (incl. license) are clarified during such a meeting. A comprehensive technical ECU test contains hardware and firmware security testing as well as security testing of the exposed bus interfaces (CAN, FlexRay, Automotive Ethernet).

Technical Assessment

Testing in the Security Lab in Vienna

- Secure Boot / Authenticated Boot
- Hardware Pentesting (Debug interfaces, Microcontroller Glitching, Data extraction)
- Secure On-board Communication (SecOC) Tests
- Technical Firmware Assessments
- Over-The-Air (OTA) Updates
- Bus Inteface Testing
- Data Flow Tests (for Telemetrics)
- AUTOSAR testing

During the technical assessment of an ECU, the full stack from electronic components up to the services exposed to the automotive bus interfaces and entertainment-system applications is tested. This includes testing of secure/authenticated boot, secure on-board communications, over-the-air updates, debug interfaces on the electronic components with different techniques, reveres engineering of firmware and testing of communication operating systems like AUTOSAR. Moreover, there is an increasing number of car telemetrics with connections to the Cloud (via M2M) for autonomous driving. Such attack vectors are also covered by the tests if needed by the customer.

CyberDanube's outstanding service, namely building a digital twin, has also been leveraged multiple times when testing devices like automotive ECUs. This way, much deeper hidden vulnerabilities can be uncovered in such devices in contrast to testing only on the real hardware.

Typical Challenges

The test setup for ECUs can be challenging for more complex devices with many I/Os and requirements for the bus restbus simulation. In case of tests for CAN and FlexRay interfaces, custom hardware and software is used by CyberDanube experts. The 1000BaseT1 (Automotive Ethernet) interfaces are not providing a traditional Ethernet plug as RJ45. To access them via Gigabit Ethernet, special adapters are needed. Further challenges are special hardware for debug-interfaces and removing/interfacing memory chips from the circuit board. Such issues do not pose a problem for CyberDanube experts in the hardware lab in Vienna.

Typical Findings

- Secure/Authenticated Boot Bypass
- Race Conditions in complex ECUs (e.g. Entertainment Systems)
- Exposed Vulnerable Services in the Automotive Ethernet

Due to the variety of operating systems in ECUs, different vulnerabilities have been identified in past technical security assessments. Real-Time Operating Systems (OS) often tend to simpler memory leaks in local and network services, whereas Linux-based operating systems are vulnerable on a higher application level. Such vulnerabilities can often be identified by static version searches in firmware and verified on digital twins. Identified hardware vulnerabilities (e.g. unprotected JTAG), in contrast to OS specific issues, remain the same – no matter which firmware was deployed.

Experts Contact

Thomas Weber

Founder &
Technical Director

About CyberDanube

CyberDanube is a specialized cyber security company, offering OT, (I)IoT & Embedded Security testing services. CyberDanube provides a unique security toolset & technical consulting, e.g. penetration testing capability with a dedicated hardware lab for in-depth product analysis. With a proven track record in pentesting, research and published advisories including zero-day vulnerabilities, CyberDanube is a trusted authority (CNA) which operates independently from manufactures & investors as trustworthy partner in the security industry.

If you need a Automotive Cyber Security Pentest for an ECU,

Contact us via : ✉ office@cyberdanube.com

This Whitepaper has been inspired by real word projects.