dissecto Pentesting

We are offering pentests of embedded systems, automotive systems and hardware components. The process targets specific systems and goals, using various methods to breach security. Results inform the client of vulnerabilities and recommend mitigation strategies.

Penetration testing is integral to security audits, mandated by standards like **UNECE R155, ISO 21434 or GB 44495** and supporting risk assessments. Penetration tests can be tailored to meet your individual requirements!

Features:

- **Comprehensive Systems Testing:** We conduct thorough security tests for entire vehicles, including ECUs and embedded systems, ensuring robust protection against potential vulnerabilities.
- **Specialized Network and Interface Testing:** Our package offers in-depth testing services for vehicle control units, using reverse engineering, hardware checks, and protocol fuzzing to identify vulnerabilities and enhance vehicle security.
- **Hardware-Security Analysis:** We carefully examine hardware components like processors and microcontrollers to uncover potential security gaps and recommend measures to fortify ECUs and microcontrollers against threats
- **Proof of Concept Attacks and Showcases:** We craft practical attack demonstrations to showcase potential vulnerabilities and provide actionable insights for strengthening security measures.
- **Customized Scope of Testing:** Our testing scope includes reverse engineering, hardware security assessments, and robustness testing through fuzzing, ensuring comprehensive coverage of potential attack vectors. However, the specific scope is always agreed with the customer in advance.
- **Detailed Reporting and Results:** Clients receive detailed reports outlining findings, risk assessments, and proposed countermeasures, along with technical scripts where feasible for reproducing findings.

Work Results

Result 1: At the start of the project a test plan is created, which shows the individual steps and processes.

Result 2: dissecto GmbH delivers a results report with the following contents:
Management summary, summary of top risks with attack paths and requirements for counter measures
Description of scope and out-of-scope
A description of the test procedure
A description of the test setup (incl. SW/HW versions of all components involved)
All findings including concrete traces that show the security problem mentioned, classification of the findings according to the specified risk metrics and proposed countermeasures

Result 3: With the help of our fully automated Platform as a Service HydraVision, the client will receive continuous detailed reports on weak points of the integrated control units (continuous re-testing)

Result 4: If technically possible, scripts are provided to reproduce the findings.

Security Testing, simplified.

dissecto GmbH, Franz-Mayer-Str. 1, 93053 Regensburg, GERMANY
www.dissecto.com