fact sheet

Penetration Test Paket - Hardware Security

Our "Hardware Security" Penetration Testing Package offers comprehensive testing services for your ECUs and microcontrollers. We create detailed test plans, provide comprehensive results reports, and use specialized attack scenarios to uncover security vulnerabilities and recommend protective measures.

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 measures to be taken.
- Description of scope and out-of-scope
- A description of the test procedure
- A description of the test setup (including software and hardware 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: If technically possible, scripts are provided to reproduce the findings.

examination object

The test object is a control unit with the following conditions:

- The component operates in a system network with other components. If a test setup is required, this will be provided by the customer
- The component has 1+ vehicle buses (e.g. CAN, CAN-FD, 10/100/1000BASE-T1/100BASE-TX Ethernet)
- The component has 1+ microcontrollers that provide debugging interfaces on the PCB (e.g. UART, JTAG)
- The microcontrollers may have hardware-based protection mechanisms (e.g. JTAG lock, HSM).

scope of testing

1. Design and execution of a clock, voltage, or EM glitching attack to bypass JTAG locking and similar mechanisms

OR

2. Design and execution of a side-channel attack (timing, power, EM) on performed cryptographic operations to extract secret information (e.g., key material).

OR

3. Bypassing JTAG locking and similar mechanisms by manipulating at the PCB level (e.g., microcontroller configuration pins).

requirements

- The customer provides all necessary documents in due time
- The client provides at least two test setups or control units
- The client designates a fixed contact person who is available for queries during the penetration test

dissecto