fact sheet

Penetration Test Paket - Automotive Systems

Our Penetration Test Package "Automotive Systems (Networks & Interfaces)" offers comprehensive testing services for vehicle control units. Using reverse engineering, hardware checks, protocol fuzzing and more, we identify vulnerabilities and assist in improving vehicle security.

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

examination object

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

- The component works in a system network with other components. Test setup is 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 component has a diagnostic stack that can be used to process diagnostic messages and to program the ECU (flashing). Likewise, variants are configured via the UDS diagnostic protocol (coding)

continuous security testing with dissecto HydraVision

With the help of our fully automated "Platform as a Service" (PaaS) testing system dissecto HydraVision, the client receives detailed reports about vulnerabilities of the integrated control units. After a penetration tests have been completed, we integrate the ECU into our test system hydraVision which performs further security tests for 1 year.

Our tests are regularlyand provide additional security for the foreseeable future. Access to the system as well as its results are via a personal access for the client. Our dashboard as well as regularly generated reports thus provide security as well as easy access to the hardware for further projects and tests.

dissecto

scope of testing

1. Reverse engineering of the ECU and identification of attack surfaces.
2. Examination for hardware security vulnerabilities at board and processor level.
3. Up to 8 standard test cases, including e.g.:
   a. Diagnostic scanning and matching with documentation to identify undocumented UDS services, sessions, Security Access, Data- and routine identifiers
   b. Checking the shutdown of debugging and calibration interfaces (JTAG, UART, DLT, XCP, HTTP web server)
   c. Checking the configuration on installed Ethernet switches with regard to port isolation and configuration interfaces
   d. Checking the mode switching and function activation mechanisms for typical logic errors
   e. Analysis of the provided flash container, e.g. readable artifacts in the binary that provide information on code layout, keys, etc.
   f. Additional test cases will be agreed upon between the client and dissecto during the course of the project.
4. Robustness tests of the implementation by fuzzing:
   a. Development of an effective, ECU-specific strategy to detect crashes and watchdog interventions on the analysis object.
   b. Fuzzing of system function protocols such as UDS, SecOC, SOME/IP, DLT,XCP IPv4 and IPv6 stacks, IPsec, MACsec.
   c. Fuzzing of specific protocols of the control device (e.g. ISO-TP, MQTT)
   d. If source code was provided: Adaptation of the fuzzing strategy based on the provided source code.
   e. Analysis of the exploitability of fuzzing results in consultation with the customer or, if source code was provided, on the basis of the provided source code.
5. Functional test of implemented security mechanisms (e.g. software signatures, immobilizer)
6. After completion of the test we integrate the ECU into our test system dissecto HydraVision which performs further security tests for 1 year.

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