Thoroughly Tested From A to Z

AUTHORS

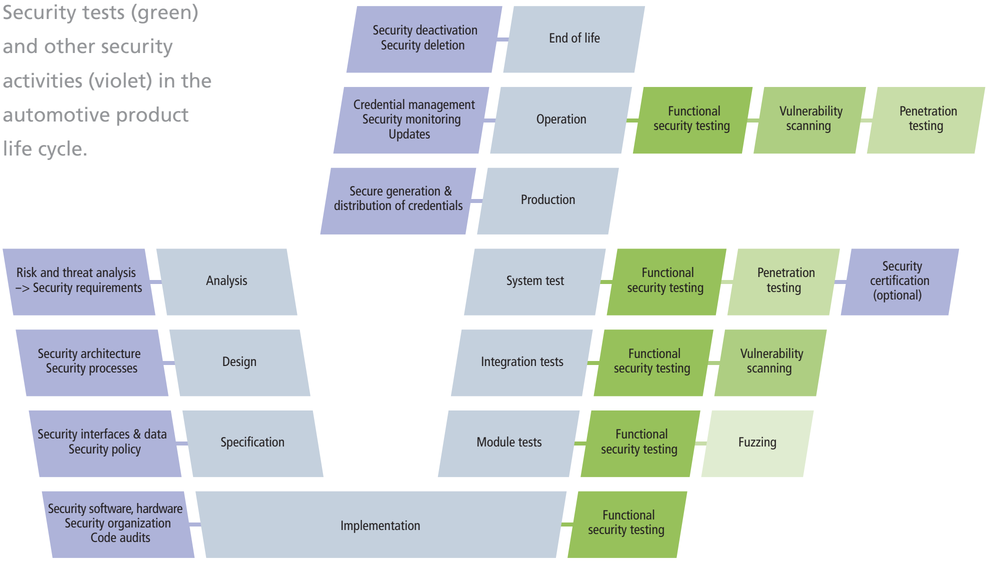
Dr. Markus Kögel is Expert Security Consultant at **ESCRYPT GmbH**.

Dr.-Ing. Marko Wolf is Head of Consulting and Engineering at **ESCRYPT GmbH**.

ESCRYPT is a 100-percent subsidiary of ETAS GmbH and offers security solutions for embedded systems.

Security testing for the entire vehicle life cycle

Effective information security requires security testing throughout the entire vehicle life cycle. This is because in contrast to conventional testing for driving safety, in which the boundary conditions are mostly determined by physical laws and subsequently do not change, the assumptions and boundary conditions for security testing are subject to the eternal battle between attackers and defenders. For this reason, regular security testing is required even after the start of production, right up until the vehicle is decommissioned, so as to check for newly developed cyber attacks and previously undetected security loopholes and, where necessary, provide an effective response.



Security tests (green) and other security activities (violet) in the automotive product life cycle.

Automotive security testing methods for every phase

Automotive security testing essentially distinguishes four different testing methods which, as shown in the figure, are located on the ascending side of the extended V model, specifically: functional security testing, automated vulnerability scanning, fuzzing, and penetration tests. ESCRYPT offers comprehensive consulting and services in all these areas.

Functional security testing checks whether the specification of the used security mechanisms has been correctly and fully implemented. This step is similar to general functional testing, but focuses on security functionality. To this end, the implementation, for instance of encryption algorithms or authentication protocols, is tested for general compliance and the performance and resource consumption of the implementation is monitored, for example in order to identify potential conflicts with run-time requirements or memory capacity requirements.

Fuzzing is used in addition to functional security testing to systematically detect unstable or even erroneous behavior of the system through a variety of unexpected, invalid or implausible input.

Vulnerability scanning on the other hand tests the system for common access points, security loopholes, and vulnerabilities for cyber attacks. These tests usually use a continuously updated database of all known vulnerabilities for the test object at the time of testing.

Penetration tests are usually only applied to the release candidates of new automotive IT systems. These extended security tests follow the principle that an IT system is only sufficiently tested when a realistic attacker in the form of a human tester tries to exploit all the vulnerabilities found by applying all available knowledge, skills, and tools.

ETAS and ESCRYPT offer various test systems in addition to consulting and services (see page 12). In particular, ESCRYPT has conducted security testing for automotive security applications for over a decade and is a partner to many OEMs and suppliers. The ETAS subsidiary has a state-of-the-art testing laboratory and is ideally equipped to cope with diverse hacking methods – regardless of whether penetration testing of hardware, software, or automotive networks.