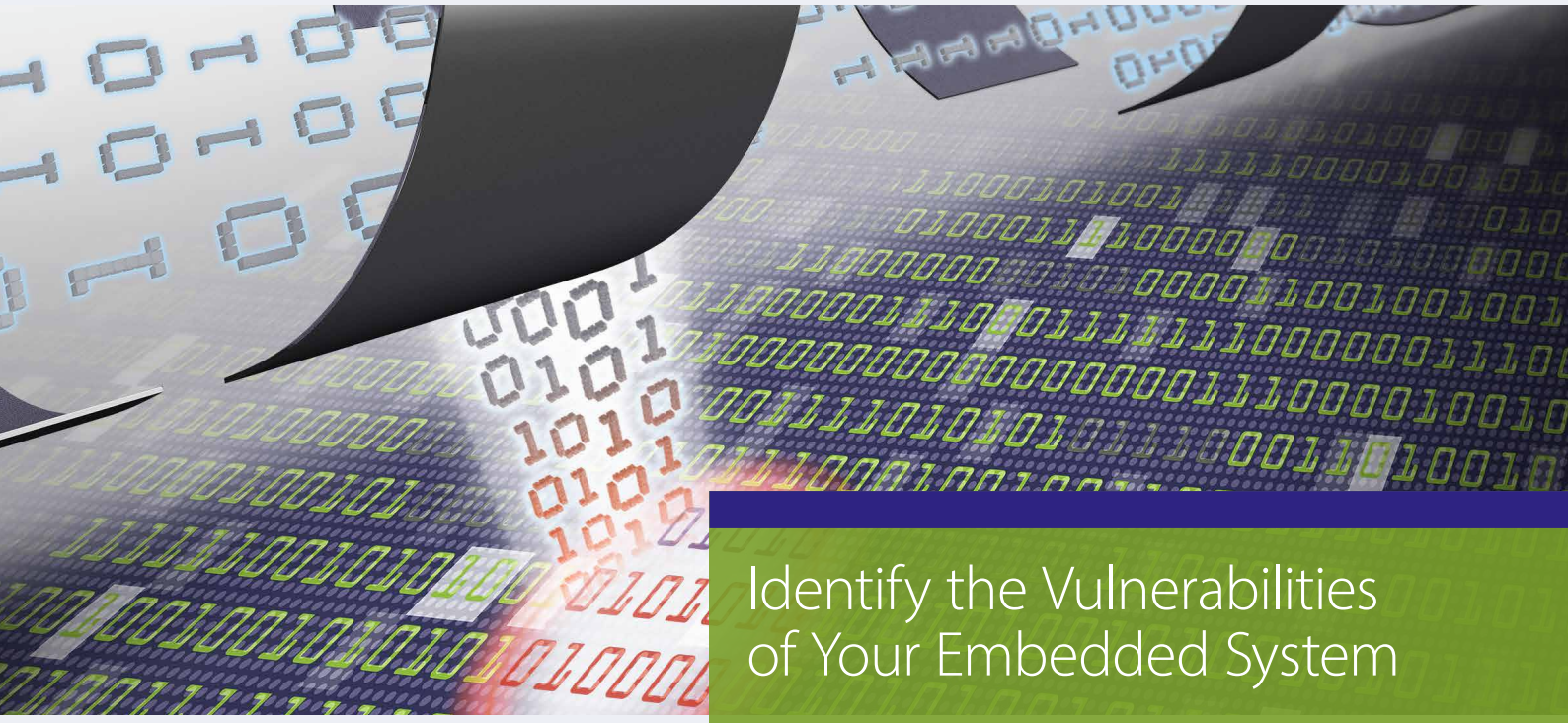
escrypt
SECURITY. TRUST. SUCCESS.

Security Testing Services



Identify the Vulnerabilities of Your Embedded System

Understand How Hackers Work

Keeping data secure is one of the top priorities for companies today. Unfortunately, new vulnerabilities are discovered every day and it is nearly impossible to keep pace with all of them. That is why it is essential to test your embedded system with seasoned security experts. The professionals from ESCRYPT will dig deep to uncover the security weaknesses that can cost you time, money and reputation. With several test methods they simulate the strategical and technical actions of a real world attacker with the goal of finding the security vulnerabilities and providing comprehensive assistance in how to fix them.

Your Benefits

- Prevent hacker attacks that put your organization's reputation and trustworthiness at stake
- Ensure a cost-efficient risk management
- Avoid the cost of system downtime
- Meet regulatory requirements and avoid fines
- Maintain positive corporate image and customer loyalty

Available Testing Methods

Code Review

In some cases a code review is the only efficient way that several key security controls can be verified including access control, encryption, data protection, logging, back-end system communications and usage.

Penetration Testing

Penetration tests turn known attack theories or newly identified vulnerabilities into real proof-of-concept attacks to fulfill a realistic attack goal and identify physical weaknesses often not covered by other security tests. A penetration test can include following modules:

- Vulnerability scans
- Systematic fuzzing
- Exploration/exploitation tests
- Reverse engineering
- Implementation attacks

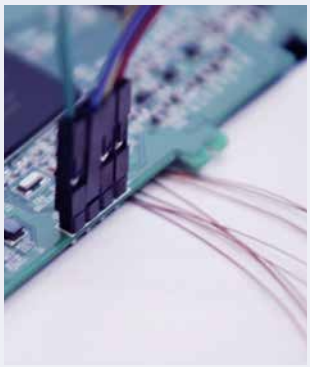
Functional Testing

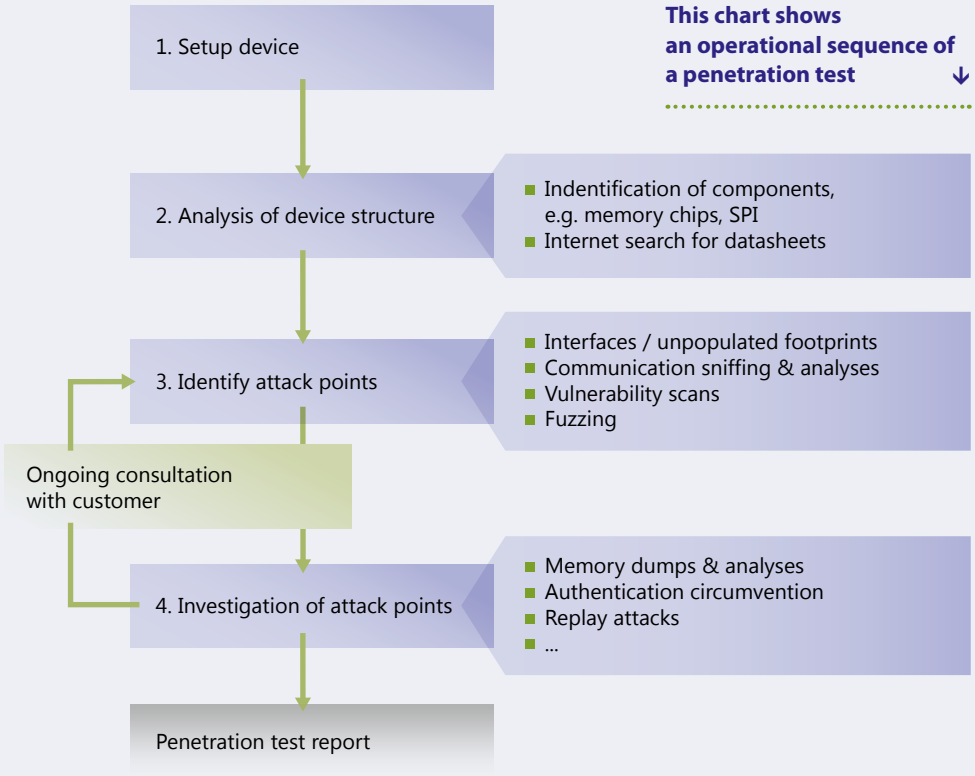
With functional security tests the good performance, correctness and robustness of already implemented security functionality can be verified (e.g., encryption algorithms, security protocols).

ESCRYPT 2018/05

escrypt
SECURITY. TRUST. SUCCESS.

Security Testing Services





Our Service at a Glance

- Identification of critical security threats of your embedded system at implementation and deployment level before it leads to real safety or financial or PR damage
- Demonstration of how difficult or how easy it is to break into your embedded system based on realistic proof-of-concept attacks
- Check existing protections in your embedded system if they are (still) capable to defend actual security attacks
- Detailed documentation describing the result of every attack
- Accurate evaluation and risk assessment for each finding by the experienced testing team
- Risk assessment based on CVSS possible
- Detailed recommendations of state-of-the-art protection mechanisms, which reduce identified security risks to an acceptable level in order to enable economic security

Testing Packages

ESCRYPT offers individual testing packages tailored to the special requirements of the embedded system. All available testing methods and modules can be combined and the testing scope can be adapted accordingly. A typical penetration testing package for embedded devices consists of the modules vulnerability scanning, fuzzing, and exploration & exploitation. Optionally this can be expanded by other test modules, e.g., reverse engineering. Or the penetration test can be conducted together with a code review of critical code parts or functional testing.

A special testing trial package gives a quick overview about potential security risks and potential attacks for your product (if any) and suggests where further investigations might become necessary in order to ensure a cost-efficient, result-oriented testing approach.

Any Questions?

Please contact us any time at
info@escrypt.com
or via phone:
+49 234 43870-200