Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Prof. Dr. Eric Bodden
Rheinstrasse 75
64295 Darmstadt
Germany

Phone +49 6151 16-7542
Fax +49 6151 869-224
eric.bodden@sit.fraunhofer.de
testlab.sit.fraunhofer.de

TEST LAB

PRACTICAL IT SECURITY ASSESSMENT

In IT systems security represents a crucial quality feature and it is becoming increasingly important in the licensing and purchasing of software, IT services and IT-based devices. But neither the IT system manufacturer nor the customer can determine without major effort whether the expected and required security level has been reached. The Fraunhofer SIT test lab supports companies in assessing essential security features quickly and manufacturer independent. It is a holistic approach that considers the security concept, the practical realization and actual use scenarios, while providing high practical relevance. Extensive test reports deliver detailed results and concrete recommendations: This way, users receive informative assessments on IT security, data protection and compliance in a speedy manner. Providers, on the other hand, receive a conclusive security proof of their proprietary products and valuable ideas for improvements.

If desired, the security properties may be published in the form of an attestation report, i. e. an independent expert report. This evaluation also represents a valuable documentation of a product's security properties and configuration recommendations. Of course, an external security analysis also helps in the quality assurance and improvement of own products, for example prior to their licensing or market introduction. Possible vulnerabilities will be detected, security measures will be compared to the state of scientific knowledge and possible improvements suggested.

Neither penetration tests nor compliance audits are suitable to eliminate vulnerabilities in a system. A meaningful security assessment is only viable on the basis of an extensive analysis that includes all the security relevant parts and aspects. This is why the Fraunhofer SIT test lab considers all the relevant parts of an IT system with regard to a multitude of error types, while searching for vulnerabilities on all levels, in the design or algorithms itself, in implementation or configuration.

To detect IT security vulnerabilities and facilitate an efficient and targeted approach in doing so, a profound understanding of the technologies used, the operating environment, and current threats and attack techniques is required. The test lab staff at Fraunhofer SIT are renowned IT security experts and have many years of experience in assessing IT security architectures and carrying out practical attacks. Additional technological competencies are provided by domain specialists from the institute's various scientific departments, complementing the test expert team if necessary.

Approach

In an extensive security analysis, the Fraunhofer SIT test lab evaluates if the chosen security measures fit the respective threats, if they have been implemented correctly or if vulnerabilities exist that would permit circumvention of the security measures. The evaluation comprises the following interrelated steps that have been chosen in such a manner that fundamental issues can be detected as early as possible:

1. Demarcation of the test object and threat modeling: Which security feature does a user expect of the test object?

2. Conceptual analysis: Do the security measures correspond to the state of the art? Are they adequate?

3. Implementation review: Were security measures and cryptographic functions implemented correctly?

4. Vulnerability analysis: Applying practical tests, the team checks the test object systematically for faults.

5. Final report: All the steps and results of the assessment will be documented precisely and replicably.

Benefits for manufacturers:

- Fast verification of existing IT security
- Quality assurance and improvement proposals
- Competitive advantage due to verifiable security
- Informative documentation of the security features

Benefits for the user:

- Independent evaluation of all security relevant aspects
- Expert evaluation of the security level
- Comparison with scientific knowledge
- Precise configuration recommendations
- Matching security properties with user's own requirements

Evaluation Criteria	**Penetration Test**	**Fraunhofer SIT Test Lab**	**Common Criteria**	**Compliance Audit**
All relevant threats are considered		✓		
All security related components are considered		✓		
Review of a subset of security measures			✓	✓
Security measures are suitable		✓	✓	✓
Security measures complement each other		✓		
Security measures are implemented correctly		✓	✓	
No known vulnerabilities	✓	✓	✓	
No insecure configurations		✓		
Organizational measures are considered				✓
Development process meets formal requirements			✓	
Evaluation meets formal standards			✓	✓
Project Characteristics				
Effort	•	• •	• • •	•
Test object	Products, Running Systems	Products	Products	Running systems
Objective	Identify obvious vulnerabilities	Comprehensive review of security properties	Verification of selected security properties	Verification of basic security requirements