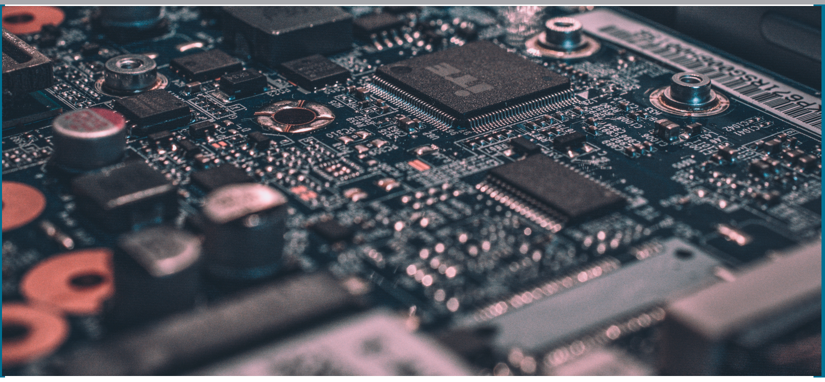
Fraunhofer
ACADEMY



IT SECURITY ANALYSES AND TESTS FOR EMBEDDED SYSTEMS

HOW YOU CAN BENEFIT: AT A GLANCE

After the seminar, you will be able to ...

... assess, plan and carry out IT security analyses for embedded systems;
... understand and precisely track various kinds of security problems;
... analyze security concepts and protocols;
... understand practical procedures for analyzing circuit boards, buses, interfaces and firmware;
... make useful assessments of research results.

This seminar will provide you with ...

... first-hand practical knowledge;
... a comprehensive view of the execution of security analyses;
... current and advanced analysis techniques, such as binary analysis and side-channel attacks;
... practical training and demonstration of various research methods.

The challenge: Comprehensively and efficiently testing the cyber-security of embedded systems

New interfaces and networked interconnections (e.g. IoT products or smart meters) make IT security an important quality feature of embedded systems. Unlike classic safety tests, security problems here are unexpected and hard to foresee. They are exploited by unpredictable attackers, who are intelligent in their work. A systematic approach is necessary in order to obtain a comprehensive and meaningful assessment of IT security within a limited testing period. Due to the special nature of embedded systems, traditional IT testing tools and methods cannot be applied to them, as they do not cover many more specific security aspects.

The solution: methodical and technical expertise

Participants will learn how to efficiently track various types of security problems on both conceptual and implementation levels. Up-to-date, practically-tested research methods and procedures for analyzing embedded systems are clearly demonstrated in hands-on training.

The practical examples are carefully selected to provide participants with a comprehensive view of all the important aspects and concepts. The scope of topics ranges from circuit-board analysis to attacks at semiconductors and bus level, crypto-chip security, fuzzing, binary analysis, and the analysis of protocols for wireless interfaces.

INFORMATION OVERVIEW

Course: IT security analyses and tests for embedded systems

Prerequisites:
- Good understanding of technical systems, ideally, in the field of IoT or embedded systems
- basic knowledge of electronics, IT security, cryptography and programming in C and Python are an advantage

Duration: 2 days in class

Costs: 1.200 €

Organized by:

Fraunhofer SIT

Contents

- Basic overview of IT security
- Effective approach to security analyses
- Special features of embedded systems
- Requirements and threat analysis
- Analysis at the concept and implementation levels
- Analysis techniques and methods with practical examples from the fields of application
  - PCB analysis
  - Cryptographic procedure and protocols
  - Fuzzing
  - Wireless interfaces
  - Reading and analysis of firmware
  - Side-channel analysis
- Documentation and assessment of vulnerabilities

Learning objectives

The participants are provided with a comprehensive overview of the challenges and approaches to carrying out IT security analyses of embedded systems. In addition to an efficient, systematic approach —from requirement analysis to final assessment— the speakers will take a look at the current practical techniques for analyzing security-relevant software, hardware components and protocols.

Target group

- Developers in the field of embedded systems who plan, execute or arrange IT security analyses
- Security experts from the IT field who carry out practical tests on embedded systems

OUR SPEAKERS

The speakers work in the Cyber-Physical Systems Security division of the Fraunhofer Institute for Secure Information Technology (SIT). They have been performing security analyses of embedded systems for many years now, e.g. control devices used in the automotive and transport industry, power supply (smart grid) and specialist medical equipment, advising manufacturers and suppliers on developing and standardizing secure systems and components.

The Cyber-Security Training Lab: Advanced training for the IT security experts of tomorrow

The Cyber-Security Training Lab is a result of a collaborative effort between Fraunhofer and a number of select technical colleges, transferring up-to-date knowledge of cyber-security as part of advanced training offers for companies. All over Germany, specialists and managers in industry and public administration receive compact qualifications in top labs with the latest IT infrastructure.

DO YOU STILL HAVE QUESTIONS ABOUT …

… IT security analyses?

Jan Steffan
Fraunhofer SIT
Phone +49 6151 869-261
jan.steffan@sit.fraunhofer.de

… registration, organization or other courses offered?

Adem Salgin | Fraunhofer Academy
Phone +49 89 1205-1555
cybersicherheit@fraunhofer.de