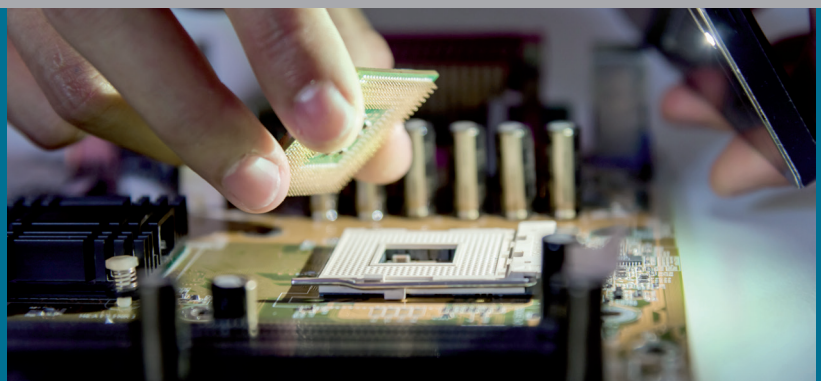
Fraunhofer
ACADEMY

SEMINAR



HOW YOU CAN BENEFIT: AT A GLANCE

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

... understand and assess various kinds of threats.
... understand and categorize the basic concepts of IT security and cryptography.
... carry out threat and risk analyses.
... systematically develop security concepts and protocols.
... practically implement security solutions.
... assess the efficiency of the security solutions developed.

This workshop will provide you with ...

... first-hand practical knowledge (from various fields of application).
... a comprehensive overview of security solution development processes for embedded systems.
... up-to-date knowledge of research in security solutions for embedded systems.
... practical exercises and demonstrations for implementing security solutions.

www.academy.fraunhofer.de/cybersecurity

EMBEDDED SECURITY ENGINEERING

With practical examples for the automotive industry and IoT

The challenge: Systematically developing and implementing cybersecurity in embedded systems

Embedded systems are used in many fields such as the automotive industry, industrial automation, or Internet of Things (IoT). As interconnection in networks expands, they are increasingly exposed to cyberattacks. While in the past, it was sufficient to take measures to ensure functional safety, nowadays IT security measures are necessary. To implement suitable IT security measures many different factors must be taken into account. As such, a systematic development methodology is required, for example, SAE-J3061, which is a requirement in the automotive industry. Likewise, there is a demand for information regarding specific requirements (e.g. interactions between safety and security, long-term security) and suitable technical IT security measures.

The solution: Methodical and technical expertise

The participants will become familiarized with a development process for embedded systems, both theoretically and practically, based on a specific application case. Security concepts, procedures and protocols are systematically developed on the basis of typical threats and weaknesses. Different question will be addressed, such as: implementation of lightweight cryptography with appropriate key management; using hardware security concepts such as TPM 2.0; or developing protocols, e.g. for secure over-the-air code updates. Hot topics, such as post-quantum cryptography and its practical feasibility in embedded systems, will also be considered.

INFORMATION OVERVIEW

Course: Embedded security engineering

Requirements: Good understanding of technical systems, ideally in the field of embedded systems

Duration: 2 days in class

Costs: 1.200 €

Organized by:

Fraunhofer SIT

Contents

- IT security development processes
- Basics of IT security and cryptography
- Challenges of securing embedded systems
- Lightweight cryptography and key management for embedded systems
- Long-term security for embedded systems (e.g. migration strategies, post-quantum cryptography)
- Network security and cryptographic protocols (e.g. secure over-the-air code updates)
- Hardware security (e.g. TPM 2.0, lightweight alternatives)
- Separation and isolation solutions (e.g. microkernel operating systems)
- Platform integrity and device identity (e.g. attestation protocols, secure booting)
- Standardization, e.g. SAE-J3061, ISO15118

Learning objectives

The participants are provided with a comprehensive overview of the challenges and approaches to developing IT security solutions for embedded systems. In addition to an efficient, systematic approach —from requirement analysis to final assessment of the solution developed— the speakers will also be considering the current solutions and their feasibility.

Target group

- Developers in the fields of automotive industry, IoT and other fields related to embedded systems that develop IT security solutions
- IT security experts who would like to expand their knowledge in new domains

OUR SPEAKERS

The speakers work in the Cyber-Physical Systems Security division of the Fraunhofer Institute for Secure Information Technology (SIT). For many years, they have been analyzing and developing security solutions for embedded systems in various fields, consulting with vehicle manufacturers, suppliers, and industrial automation engineers in developing and standardizing their own embedded systems.

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 ...

... Embedded Security Engineering?

Prof. Dr. Christoph Krauß
Fraunhofer SIT
Phone +49 6151 869-116
christoph.krauss@sit.fraunhofer.de

... registration, organization or other courses offered?

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