

Embedded Security Engineering

Seminar zu praxisnahen Beispielen aus Automotive und IoT

In diesem Kurs lernen Sie, Sicherheitslösungen für eingebettete Systeme zu entwickeln und umzusetzen. Sie erfahren, wie Sie Bedrohungen analysieren, Sicherheitsprotokolle entwickeln und kryptografische Methoden wie TPM 2.0 und Post-Quanten-Kryptographie anwenden. Praxisorientierte Übungen runden das Wissen ab.

Embedded Security Engineering – Sicherheitslösungen für IoT und Automobilindustrie entwickeln

Bereits bei der Entwicklung der Produkte müssen Funktionssicherheit und Schutzmaßnahmen gegen Angriffe mitgedacht werden.

Dies ist auch wichtig für die Umsetzung der Anforderungen aus dem neuen Cyber Resilience Act (CRA). Der Kurs „Embedded Security Engineering“ vermittelt Wissen zur Entwicklung von Sicherheitslösungen für eingebettete Systeme.

In einem praxisnahen Anwendungsfall werden Methoden und Prozesse zur sicheren Gestaltung solcher Systeme aufgezeigt.

Dabei werden grundlegende Themen wie Bedrohungs- und Risikoanalysen, die Implementierung Kryptografie sowie Hardware-Sicherheitslösungen behandelt. Ein Fokus liegt auf der Anwendung von Technologien wie TPM 2.0 und der Entwicklung von Protokollen.

Kursdetails auf einen Blick

- Für **Entwickler*innen, Technische Leitungen in Entwicklungsprojekten**
- **offene Schulung** oder **Inhouse Training**
- Dauer: **2 ½ Tage**
- Format: **Präsenz**
- Kosten: 1.800,00 Euro (zzgl. MwSt.)

Sicherheitskonzepte für eingebettete Systeme – von aktueller Forschung bis zur Umsetzung

Teilnehmende lernen, wie sie Sicherheitsmaßnahmen systematisch entwickeln – von der Bedrohungsanalyse und Risikobewertung bis hin zur Umsetzung in realen Systemumgebungen.

Der Kurs behandelt dabei nicht nur bewährte Methoden der IT-Sicherheit, sondern greift auch aktuelle Forschungsthemen auf und zeigt, wie diese in eingebetteten Systemen effizient umgesetzt werden können. Ergänzend dazu werden Übungen durchgeführt, in denen die Absicherung von Hardware- und Softwarekomponenten trainiert wird, etwa durch den Einsatz kryptografischer Verfahren, die Implementierung Boot-Mechanismen oder den Schutz vor Seitenkanalangriffen.

Der Kurs richtet sich an Entwickler:innen, Architekt:innen und technische Leiter:innen, die Sicherheitslösungen für eingebettete Systeme konzipieren und umsetzen möchten. Nach der Teilnahme sind die Teilnehmenden in der Lage, eigenständig robuste Sicherheitskonzepte zu entwickeln, vorhandene Sicherheitslösungen kritisch zu bewerten und die Langzeitsicherheit von Systemen auch im Hinblick auf zukünftige Bedrohungen und technologische Entwicklungen zu gewährleisten.

Nach dem Seminar können Sie:

- **Bedrohungen und Risiken** in eingebetteten Systemen erkennen und bewerten.
- **Sicherheitskonzepte und -protokolle** systematisch entwickeln und in der Praxis umsetzen.
- **Sicherheitslösungen** auf ihre Wirksamkeit hin bewerten und weiter optimieren.

Alle Kursdetails und die Anmeldung finden Sie hier:



<https://s.fhg.de/Embedded-Security-Engineering>

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

Grundlagen

- IT-Sicherheit und Kryptografie
- Entwicklungsprozesse
- Herausforderungen bei der Absicherung eingebetteter Systeme

Kryptografie für eingebettete Systeme

- Leichtgewichtige Kryptografie und Schlüsselmanagement
- Langzeitsicherheit (z.B. Migrationsstrategien, Post-Quantum Kryptografie)
- Netzwerksicherheit und kryptografische Protokolle (z.B. Secure Over-the-air Code Update)

Hardware-Sicherheit, Plattformintegrität und Geräteidentität

- TPM 2.0, leichtgewichtige Alternativen
- Attestierungsprotokolle
- Secure Boot

Separations- und Isoationslösungen

- z.B. Mikrokern-Betriebssysteme

Standardisierung

- ISO / SAE 21434, ISO 15118

Fachlicher Ansprechpartner am Fraunhofer SIT

Dr. Dirk Scheuermann
Tel. +49 6151 869-290
dirk.scheuermann@sit.fraunhofer.de

Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt

