

## WORKSHOP-REIHE IT-SICHERHEIT IM »INTERNET OF THINGS«

### DAS PROGRAMM IM ÜBERBLICK

#### IT-Sicherheit im »Internet of Things«

Die Workshops befähigen die Teilnehmer zur Betrachtung der Angriffsflächen aus Sicht der Angreifer, um die Funktionsweise der verschiedenen Sicherheitsmechanismen zu verstehen, diese unter Sicherheitsaspekten zu bewerten und in konkreten Fällen praktisch anzuwenden.

#### Ihre Vorteile auf einen Blick

- Praktische Anwendungen in Experimentallaboren
- Transfer von neuestem Forschungswissen
- Fachreferenten mit führendem Expertenwissen
- Bedarfsorientierte Trainings auf Basic-, -Advanced- und Expert-Level
- Effektives Training in kleinen Gruppen
- Bei Bedarf individuell angepasste Inhouse-Trainings

Mehr Informationen finden Sie unter  
[www.fkie.fraunhofer.de/lernlabor](http://www.fkie.fraunhofer.de/lernlabor)



### WORKSHOPREIHE: IT-SICHERHEIT IM »INTERNET OF THINGS«

Die Module sind bedarfsgerecht aufgebaut, sodass Sie in demjenigen Level und Schulungsmodul einsteigen können, welches für Ihre Vorkenntnisse und Kompetenzbedarfe geeignet ist.

Sichere und  
zuverlässige  
Protokolle

Sicherheit  
in drahtlosen  
Netzen

Fortgeschrittene  
Firmware-  
analyse

Einführung  
in die Firm-  
wareanalyse



Module in der Workshopreihe IT-Sicherheit im »Internet of Things«

## Firmware

**Einführung in die Firmwareanalyse** | Beschaffung von Firmware über Hersteller oder Geräteschnittstellen; Extraktion der Firmware vom Gerät mittels Hardware-Werkzeugen; Entpacken der Firmware-Container, um einzelne Komponenten wie Web- oder Samba-Server zu identifizieren; Analyse der Firmware-Komponenten anhand statischer und dynamischer Analysemethoden; Einführung in die Benutzung der wichtigsten Werkzeuge für Firmware-Extraktion und -Analyse

Dauer: 2 Tage Präsenz  
Ort: Bonn oder Inhouse  
Zielgruppe: Analysten, Entwickler, Reverser, IT-Sicherheitsexperten  
Preis: 1200 €

**Fortgeschrittene Firmwareanalyse** | Identifikation und Nutzung von Low-Level Hardware-Interfaces; Reverse Engineering von Firmwarekomponenten; Praktische Übungen von statischer Analyse an realer Firmware; Fuzzing auf ganzer Firmware oder auf Firmwarekomponenten; Ausnutzen von Sicherheitslücken für die Einrichtung von Firmware-Backdoors/-Rootkits

Dauer: 2 Tage Präsenz  
Ort: Bonn oder Inhouse  
Zielgruppe: Analysten, IT-Forensiker, Reverser  
Preis: 1200 €

## Internet of Things

**Sicherheit in drahtlosen Netzen** | Übersicht über die Konzepte und Funktionen der wichtigsten drahtlosen Netzzugänge im Bereich »Internet of Things«; Detaillierte Betrachtung der Sicherheitsmechanismen für WLAN, Bluetooth Low Energy, DECT und Zigbee; Erarbeitung der verschiedenen Verschlüsselungsmethoden im Bereich WLAN (WEP bis WPA3); Praktische Durchführung von Angriffen auf WLAN und Bluetooth Low Energy

Dauer: 1 Tag Präsenz  
Ort: Sankt Augustin oder Inhouse  
Zielgruppe: Administratoren, Anwender, Entwickler  
Preis: 600 €

**Sichere und zuverlässige Protokolle** | Motivation für standardisierte Übertragungsprotokolle im M2MBereich als Alternative zu »http«; Kennenlernen der wichtigsten Spezifikationen für MQTT und CoAP mit Fokus auf die Sicherheit beider Protokolle; Praktische Übung zur Absicherung einer MQTT-Verbindung mit TLS1.3; Konzepte für sichere Firmware-Updates; »Trade-off« zwischen Energieverbrauch und Sicherheit eines IoT-Geräts verstehen

Dauer: 1 Tag Präsenz  
Ort: Sankt Augustin oder Inhouse  
Zielgruppe: Anwender, Berater, Entwickler  
Preis: 600 €

Veranstaltet durch: