Hardwareunterstützte Analyse eingebetteter Systeme

Dem Angreifer einen Schritt voraus

Die Herausforderung: Software ist nicht der einzige Angriffsvektor. Haben Hacker physikalischen Zugriff auf IoT-Systeme, können sie diese manipulieren, und es entstehen enorme, mächtige Angriffsmöglichkeiten. Darum sind reine softwarebasierte Schutzkonzepte obsolet! Lassen Sie die IT-Sicherheit der Hardware nicht außen vor, und schützen Sie so Ihre IoT-Systeme. Erfahren Sie, warum Sie bereits in der Designphase physikalische Angriffe einbeziehen müssen, und lernen Sie diese abzuwehren.

Inhalte des Seminars

Suche von Debug Interfaces

Auslesen/Modifizieren von Flash-Chips/ Reverse Engineering von Flash-Inhalten (Disassembly und Reversing spezieller Architekturen)

Glitching (Spannung, Clock) -HW

Reverse Engineering von Feldbussen: Analyse/Manipulation von CAN-Kommunikation

Pentesting von Netzwerkgeräten

Evaluierung von Produktschutzmaßnahmen: Überprüfung der vom Hersteller angebotenen Schutzmechanismen

Ihr Nutzen

- Nach dem Seminar verstehen Sie, welche Möglichkeiten hardwarenahe Analysen bieten, und welches Equipment benötigt wird.
- Sie können mehrere Angriffswege praktisch durchführen.
- Sie verstehen, welche Geräte bedroht sind, und welche Maßnahmen Sie zum Schutz ergreifen müssen.
- Aufgrund von praktischen Übungen im Hardwarelabor können Sie eine Sicherheitslage selbstständig evaluieren.

Informationen im Überblick

Grundkenntnisse werden bedarfsgerecht ermittelt, Kenntnisse von Linux und Mikrokontrollern von Vorteil

Architekt*innen, Entwickler*innen sowie Pentester von eingebetteten Systemen

2 Tage Präsenz

1200,–

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referent:

Dr.-Ing. Matthias Hiller, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/hw-analyse