PRÄSENZ

VERNETZT BLEIBEN – ABER GESCHÜTZT!

# SICHERE HARDWAREGEBUNDENE IDENTITÄTEN

**Die Herausforderung: IoT-Systeme effizient schützen.** Sichere Geräte sind die Grundvoraussetzung für eine abgesicherte IT- und speziell IoT-Infrastruktur. Dies setzt eine gesicherte Authentifizierung der vernetzten Geräte voraus. Gerade in der Fertigungstechnologie gestaltet sich dieser Prozess sehr schwierig und aufwendig. Dieses Seminar zeigt Ihnen, wie Sie mit Physical Unclonable Functions (PUFs) jedes Ihrer Geräte eindeutig identifizieren können. Die Methode hat für Sie den Vorteil, dass kein sicherer Schlüsselspeicher im Gerät benötigt wird.

## Inhalte des Seminars

### Authentifizierung in eingebetteten Systemen/IoT

– Stand der Technik
– Vorteile durch Hardware Fingerprinting/PUFs

### Von der physikalischen Fertigungsschwankung zur Sicherheit

– Einführung PUF-Schaltungen
– Leichtgewichtige Authentifikation ohne Kryptographie
– Generierung Kryptographischer Schlüssel mit PUFs

### Sicherheitsanalyse

– Bewertung von PUF-Daten
– Angriffe und Gegenmaßnahmen
– Systemsicht und Einsatzszenarien

## Ihr Nutzen

» Nach dem Seminar können Sie Szenarien für den Einsatz von PUFs einordnen.
» Sie lernen, PUF-Schaltungen, Protokolle für Lightweight-Authentifizierungen, Fehlerkorrekturverfahren und Angriffe auf PUFs nachzuvollziehen.
» Sie erhalten eine Einführung in die praktische Anwendung.
» Sie haben exklusiven Zugang zu neuesten wissenschaftlichen Erkenntnissen aus der PUF-Forschung.

## INFORMATIONEN IM ÜBERBLICK

Grundlegende IT-Kenntnisse, Grundlegende IT-Sicherheitskenntnisse von Vorteil

Fachkräfte, Hardware-Architekten*innen, Management, Technische Leitung in Entwicklungsprojekten

1 Tag Präsenz

600,–

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referent:

Dr. Matthias Hiller, Gruppenleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

**www.cybersicherheit.fraunhofer.de/hardwaregebundene-identitaeten**