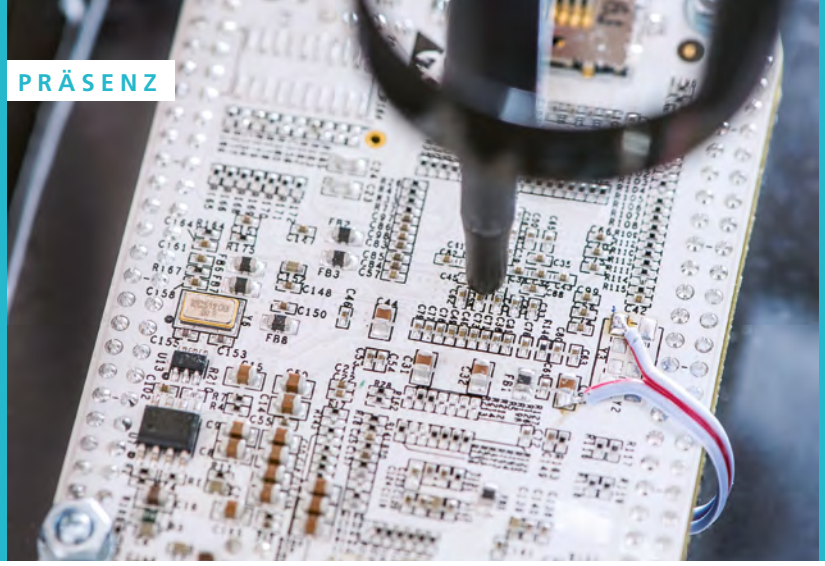
PRÄSENZ



SEITENKANALANGRIFFE VERSTEHEN UND PRAKTISCH DURCHFÜHREN

ANGRIFFE AUF KRYPTO IN IOT

Die Herausforderung: Von Seitenkanalangriffen geht ernsthafte Gefahr aus. Ohne Kryptographische Algorithmen lassen sich IoT-Geräte und eingebettete Systeme kaum entwickeln. Obwohl moderne Algorithmen wie AES gegen mathematische Angriffe abgesichert sind, geht von den Seitenkanalangriffen immer noch eine große Gefahr aus, indem beispielsweise durch Messungen am Gerät der geheime Schlüssel geknackt wird. Dieses Seminar stattet Sie mit dem wichtigen Know-how aus, um Seitenkanalangriffe zu verstehen und einzuordnen.

Inhalte des Seminars

Überblick über Angriffe gegen kryptographische Implementierungen

Einführung in wichtige Seitenkanalangriffe und Seitenkanalmessmethoden

Fokus auf den wesentlichsten Seitenkanalangriff, die Differentielle Power Analyse (DPA)

Praktische Durchführung eines DPA Angriffs auf eine AES Implementierung in einem Mikrokontroller

Schwierigkeiten für Angreifer, Strategien zum Schutz und konkrete Gegenmaßnahmen

Ihr Nutzen

- Nach dem Seminar können Sie Seitenkanalangriffe auf kryptographische Implementierungen verstehen.
- Sie können einen Seitenkanalangriff praktisch durchführen und verstehen, welche Geräte unter welchen Umständen bedroht sind.
- Sie können einschätzen, welche Maßnahmen Sie zum Schutz ergreifen müssen.

INFORMATIONEN IM ÜBERBLICK

Grundkenntnisse werden bedarfsgerecht vermittelt. Python von Vorteil

Entwickler*innen für eingebettete Elektronik für IoT-Zwecke und von IoT-Geräten

2 Tage Präsenz

1200,–

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referent:

Dr. Johann Heyszl, Abteilungsleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/seitenkanalangriffe