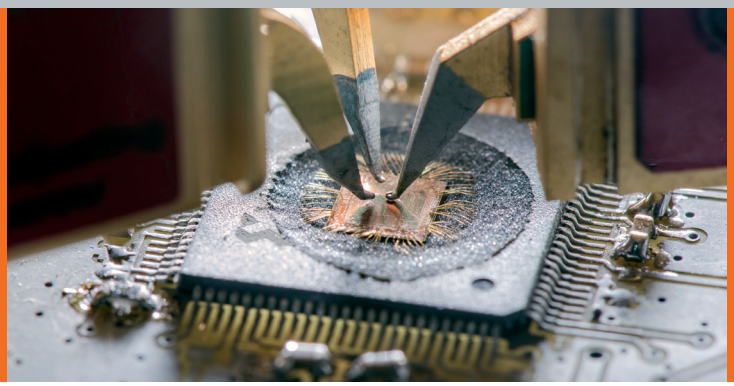
Fraunhofer
ACADEMY

SEMINAR



ANGRIFFE AUF KRYPTO IN IOT

Seitenkanalangriffe verstehen und praktisch durchführen

IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie …

…Seitenkanalangriffe auf kryptographische Implementierungen verstehen
…einen Seitenkanalangriff praktisch durchführen
…verstehen, welche Geräte unter welchen Umständen bedroht sind
…einschätzen, welche Maßnahmen Sie zum Schutz ergreifen müssen

Dieses Seminar bietet Ihnen …

…eine Einführung in Seitenkanalangriffe von Fachexperten mit mehr als 10 Jahren Erfahrung im Bereich der Hochsicherheit
…das Wissen, um fundiert bewerten zu können, wie Sie mit dem Thema Seitenkanalangriffe umgehen müssen

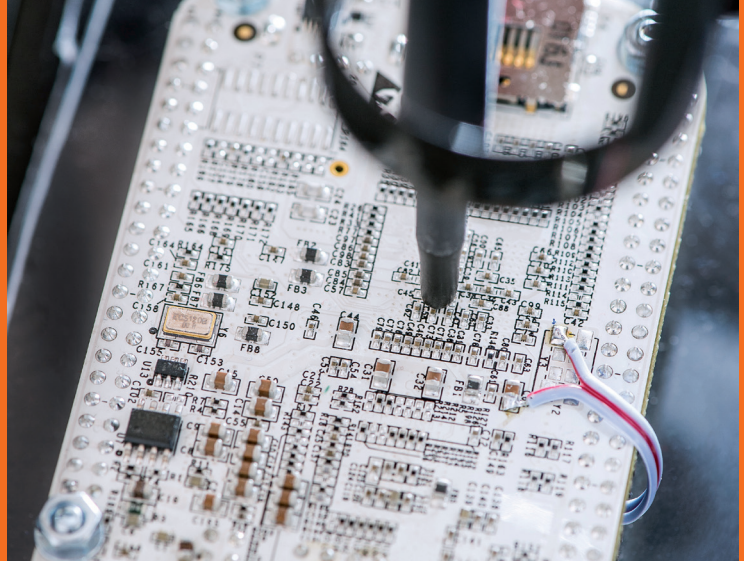
Melden Sie sich gleich an!
www.cybersicherheit.fraunhofer.de/seitenkanalangriffe

Die Herausforderung: Seitenkanalangriffe, eine ernstzunehmende Gefahr?

Kryptographische Algorithmen sind essentiell, um sichere IoT-Geräte und eingebettete Systeme zu entwickeln. Moderne Algorithmen wie AES sind sehr sicher gegen jegliche mathematische Angriffe. Trotzdem stellen Seitenkanalangriffe aber eine ernstzunehmende Gefahr dar. Ein Angreifer kann anhand von Messungen am Gerät den geheimen Schlüssel knacken. Dafür gibt es leider viele Beispiele im Bereich des IoT: Home und Builduing Automation, Drohnen, Warenverfolgung etc.

Die Lösung: Seitenkanalangriffe und deren Gefahrenpotential richtig einschätzen

Im Seminar wird das notwendige Know-How über Seitenkanalangriffe vermittelt, um die Bedrohung besser einordnen zu können. Dazu wird im praktischen Übungsteil im Hardwarelabor ein Angriff simuliert. Anschließend werden Strategien zum Schutz vor wichtigen, praxisrelevanten Seitenkanalangriffen vermittelt.



INFORMATIONEN IM ÜBERBLICK

Kurs: Angriffe auf Krypto in IoT
Voraussetzungen: Die erforderlichen Grundlagen können bedarfsgerecht vermittelt werden. Kenntnisse in Python helfen im praktischen Teil.
Dauer: 2 Tage Präsenz
Kurssprache: Deutsch oder Englisch
Teilnehmerzahl: max. 12 Personen
Veranstaltungsort: Garching bei München
Kosten: 1200 €
Veranstaltet durch:

Fraunhofer AISEC

UNSERE REFERENTEN

Dr. Johann Heyszl
Leiter der Abteilung Hardware Security am Fraunhofer AISEC

Florian Unterstein
Wissenschaftlicher Mitarbeiter Hardware Security am Fraunhofer AISEC

Die Inhalte

- 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

Die Zielgruppe: Sicherheitsexperten und Fachkräfte

- Entwickler von Eingebetteter Elektronik für IoT-Zwecke
- Entwickler von IoT-Geräten

Das Lernlabor Cybersicherheit: Weiterbildung für die IT-Sicherheitsexperten von morgen

Das Lernlabor Cybersicherheit ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen Laboren mit moderner IT-Infrastruktur.

Der Mehrwert für Ihr Unternehmen

Sie profitieren von einer Schulung zu Seitenkanalangriffen von Fachexperten mit langjähriger Erfahrung im Hochsicherheitsbereich. Dabei wird klar vermittelt, unter welchen Umständen Seitenkanalangriffe in der Praxis relevant sind und gegen welche Formen man sich daher schützen muss.

Lernziele

Die Teilnehmenden bekommen einen Überblick über vielfälltige Angriffe, die Implementierungseigenschaften von kryptographischen Algorithmen ausnutzen, wissen unter welchen Umständen diese ernstzunehmen sind, und können in der Praxis Strategien und Schutzmaßnahmen gegen diese Angriffe ergreifen. Sie entwickeln ein ausgeprägtes Verständnis und bekommen praktische Erfahrung mit dem wichtigsten bekannten Seitenkanalangriff.

HABEN SIE NOCH FRAGEN ZU…

… Angriffe auf Krypto in IoT?
Dr. Johann Heyszl
Fraunhofer AISEC
Telefon +49 89 3229986-172
johann.heyszl@aisec.fraunhofer.de

… Anmeldung, Organisation oder weiteren Angeboten?
Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de