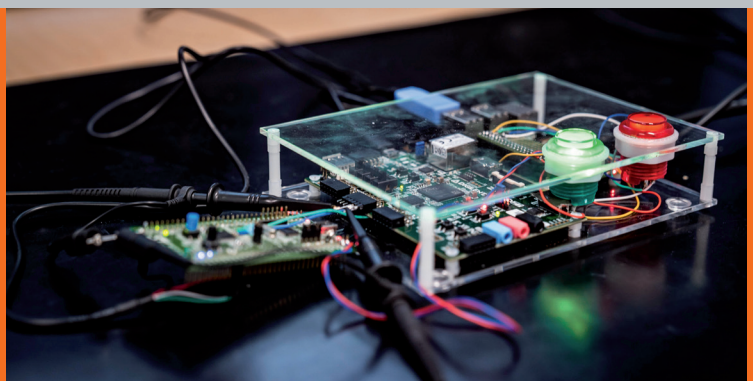
Fraunhofer
ACADEMY

SEMINAR



IHRE VORTEILE AUF EINEN BLICK

Nach dem Seminar können Sie…
…verstehen, welche Möglichkeiten hardwarenahe Analysen bieten und welches Equipment benötigt wird
…mehrere Angriffswege praktisch durchführen
…verstehen, welche Geräte bedroht sind und welche Maßnahmen Sie zum Schutz ergreifen müssen

Dieses Seminar bietet Ihnen…
…eine Einführung in hardwarenahe Analysen von eingebetteten Geräten von Fachexperten mit langjähriger Erfahrung im Bereich der Absicherung von eingebetteten Systemen
…das Wissen und erste praktische Erfahrung, um fundiert bewerten zu können, wie Sie mit dem Thema hardwarenahe Analysen umgehen müssen

Melden Sie sich gleich an!
www.cybersicherheit.fraunhofer.de/hw-analyse

HARDWARE-UNTERSTÜTZTE ANALYSE VON EINGEBETTETEN SYSTEMEN

Angewandte Hardware Angriffe auf IoT-Syteme

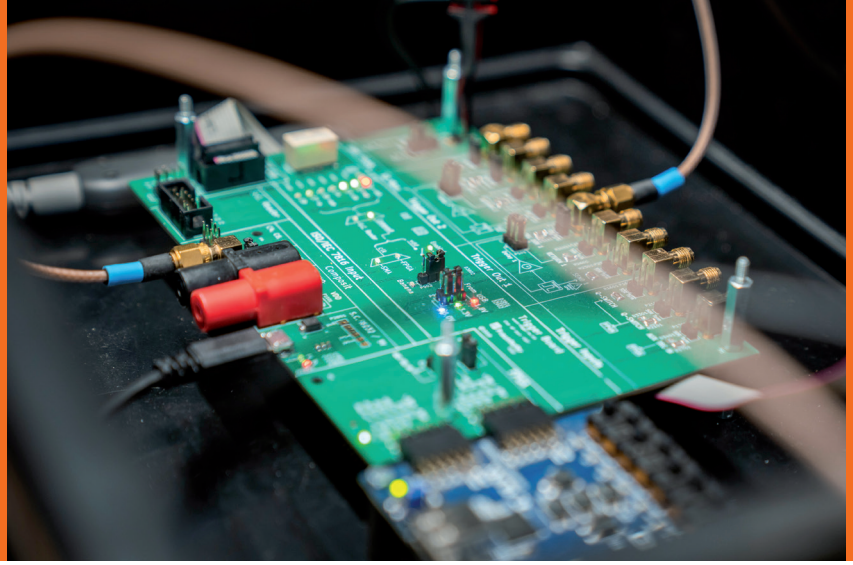
Die Herausforderung: Software ist nicht der einzige Angriffsvektor – Hardwareunterstütztes Pentesting eröffnet weitere Möglichkeiten

Sobald der Angreifer physikalisch auf das zu schützende IoT-System zugreifen kann, ergeben sich ganz neue mächtige Angriffsmöglichkeiten. Es ist notwendig, diese schon beim Design des Systems einschätzen zu können, da sonst reine softwarebasierte Schutzmechanismen wirkungslos sind. Moderne IoT-Systeme haben eine Vielzahl von Schnittstellen zur Kommunikation, aber auch zum Debuggen. Auf diese hat ein physikalischer Angreifer Zugriff und kann das System manipulieren. Daneben gibt es externe Speicherchips aus denen Firmware und kryptographische Schlüssel zur Laufzeit oder offline extrahiert und verändert werden können. Diese gilt es effektiv zu schützen.

Die Lösung: Aktuelle Tools und hardwarenahe Angriffsmethoden kennen und anwenden

Durch einen umfassenden Überblick der gängigen aktuellen hardwarebasierten Angriffsmethoden und Gegenmaßnahmen werden Teilnehmende in die Lage versetzt, die Sicherheit existierender eingebetteter Systeme besser einschätzen zu können. Außerdem ermöglicht es ihnen schon in der Design Phase, physikalische Angriffe einzubeziehen und abzuwehren.

Durch praktische Übungen in unserem Hardwarelabor sind die Teilnehmenden anschließend in der Lage die Sicherheit selbstständig zu evaluieren.



INFORMATIONEN IM ÜBERBLICK

Kurs: Hardware-unterstützte Analyse von Eingebetteten Systemen
Voraussetzungen:
Die erforderlichen Grundlagen und der Umgang mit den Tools können bedarfsgerecht vermittelt werden. Linux Kenntnisse und Erfahrung bei der Programmierung von Mikrocontrollern helfen im praktischen Teil.
Dauer: 2 Tage Präsenz
Kurssprache: Deutsch oder Englisch
Teilnehmerzahl: max. 12 Personen
Veranstaltungsort: Garching bei München oder inhouse
Kosten: 1200 €
Veranstaltet durch:

Fraunhofer AISEC

UNSERE REFERENTEN

Carsten Rolfes
Wissenschaftlicher Mitarbeiter Hardware Security am Fraunhofer AISEC

Marc Schink
Wissenschaftlicher Mitarbeiter Hardware Security am Fraunhofer AISEC

Johannes Obermaier
Wissenschaftlicher Mitarbeiter Hardware Security am Fraunhofer AISEC

Die Inhalte

- 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
- Seitenkanalanalyse

Die Zielgruppe

- Architekten und Entwickler von eingebetteten Systemen
- Pentester von eingebetteten Systemen

Die Lernziele

Teilnehmende bekommen einen Überblick aktueller Bedrohungen und Angriffstechniken auf eingebettete Systeme, speziell automotive ECUs, Gateways und Bussysteme. Sie verstehen das systematische Vorgehen beim Pentesting von eingebetteten Geräten und der möglichen Angriffsvektoren und können HW und SW Werkzeuge bei jedem Schritt anwenden.

Der Mehrwert für Ihr Unternehmen

Die Teilnehmenden erlernen in der Schulung aktuelle Angriffe auf eingebettete Systeme zu verstehen, deren Bedrohung einzuschätzen und praktisch durchzuführen.

Dieses Wissen kann direkt in die Entwicklung Ihres nächsten Produkts einfließen und somit dessen Sicherheit erhöht werden.

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.

HABEN SIE NOCH FRAGEN ZU…

… Hardware-unterstützte Analyse von Eingebetteten Systemen?
Carsten Rolfes
Fraunhofer AISEC
Telefon +49 89 3229986-128
carsten.rolfes@aisec.fraunhofer.de

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