ETHICAL HACKING

Das Wissen über Schwachstellen und wie sie ausgenutzt werden können sind die Grundvoraussetzungen für zeitgemäße IT-Security-Konzepte. Dieses Verständnis befähigt Sicherheitsverantwortliche in Unternehmen dazu, Sicherheitslücken zu finden, Risiken zu bewerten und Maßnahmen zu ergreifen, um diese zu schließen. So können sie Lösungen entwickeln, die Angriffe von vornherein vermeiden.
Durch Hacken zu mehr Sicherheit – das ist die Idee des Themenfeldes „Ethical Hacking".
Indem man sich in die Rolle eines Angreifers versetzt, lernt man die Schwachstellen kennen. Der Fokus liegt dabei auf Schwachstellen, die vor allem im industriellen Umfeld auftreten. Diese sind im Zuge von „Industrie 4.0" und der damit wachsenden Vernetzung von besonderer Bedeutung.

Unser Weiterbildungsangebot:

- Binary Exploitation
- Angriffe auf eingebettete Systeme und Gegenmaßnahmen
- Pentesting von Systemen
- Reverse Engineering
- Seitenkanalattacken und Fehlerangriffe
- Web Exploitation
- Forensik eingebetteter und mobiler Systeme
- Absicherung von Linux-Systemen

WEITERBILDUNGSPROGRAMM

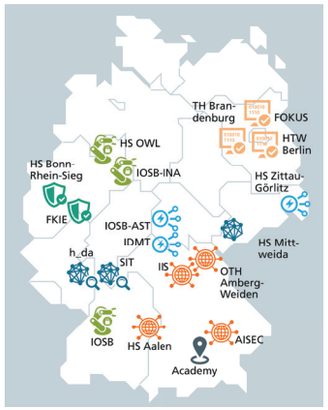
Das Weiterbildungsprogramm „Lernlabor Cybersicherheit" wird vom Bundesministerium für Bildung und Forschung gefördert. In sechs Konsortien kooperieren jeweils Fraunhofer-Institute und Hochschulen für angewandte Wissenschaften, um mit unterschiedlichen thematischen Schwerpunkten aktuelle Er-kenntnisse der Forschung auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Ziel ist es, auf diese Weise das Wissen über Sicherheitslücken, Schwachstellen, Bedrohungen und deren Abwehr in den Unternehmen zu erhöhen.
Die Fraunhofer Academy übernimmt die Koordination und Steuerung der Weiterbildungsangebote aller Konsortien.

Fraunhofer ACADEMY

Fraunhofer IIS

Hochschule Aalen

Ostbayerische Technische Hochschule Amberg-Weiden



Kontakt:

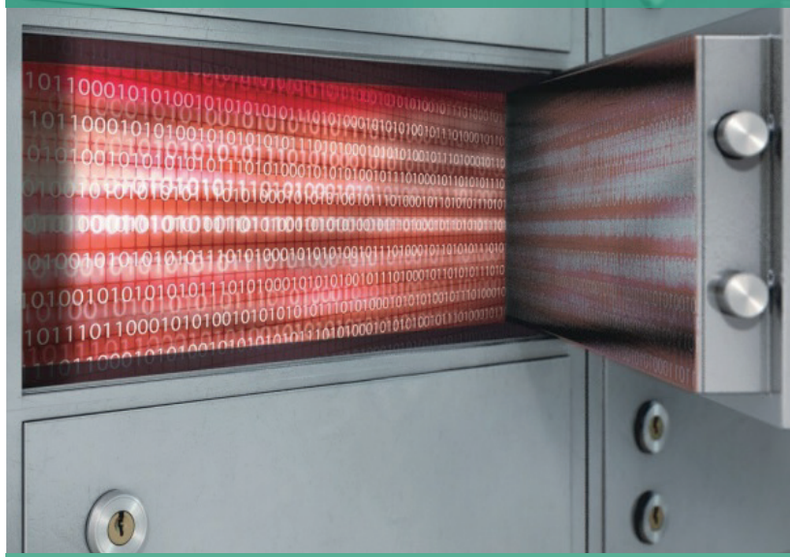
Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit (AISEC)
Parkring 4
85748 Garching bei München
Tel.: +49 89 3229986-0
E-Mail: info@aisec.fraunhofer.de

Fraunhofer AISEC

Fraunhofer AISEC

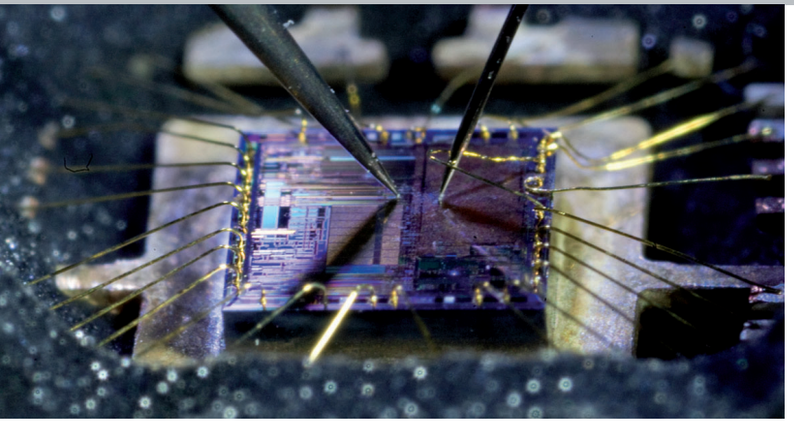
FRAUNHOFER-INSTITUT FÜR ANGEWANDTE UND INTEGRIERTE SICHERHEIT

LERNLABOR CYBERSICHERHEIT



EMBEDDED SYSTEMS
MOBILE SECURITY
INTERNET OF THINGS
ETHICAL HACKING

EMBEDDED SYSTEMS



Eingebettete Systeme (Embedded Systems), Sensoren und Aktoren sind in einer Vielzahl sicherheitskritischer Anwendungen im Einsatz. Eine hohe Verfügbarkeit der Komponenten, Reaktionszeiten, die häufig Echtzeitanforderungen besitzen, aber insbesondere auch die Gewährleistung der Manipulationssicherheit und der Schutz vor unerlaubtem Informationsabfluss (Produkt- und Know-How-Schutz) sind zentral für den sicheren Betrieb von z.B. Produktionsanlagen. Es ist deshalb essentiell, dass die verantwortlichen Fachkräfte ein Verständnis für die kritische Rolle dieser Komponenten entwickeln und Wissen darüber besitzen, wie die Qualität einzelner Komponenten sowie deren Zusammenwirken zu bewerten ist. Sie müssen aber auch in der Lage sein, erforderliche, individuell auf die Unternehmens-
bedürfnisse angepasste, eingebettete Software sicher zu
entwickeln oder entsprechende Lastenhefte für Dienstleister zu erstellen.

Unser Weiterbildungsangebot:

- Sichere Software-Entwicklung
- Embedded OS und Linux Security
- Trusted Computing und TPM 2.0
- Secure Elements als Vertrauensanker

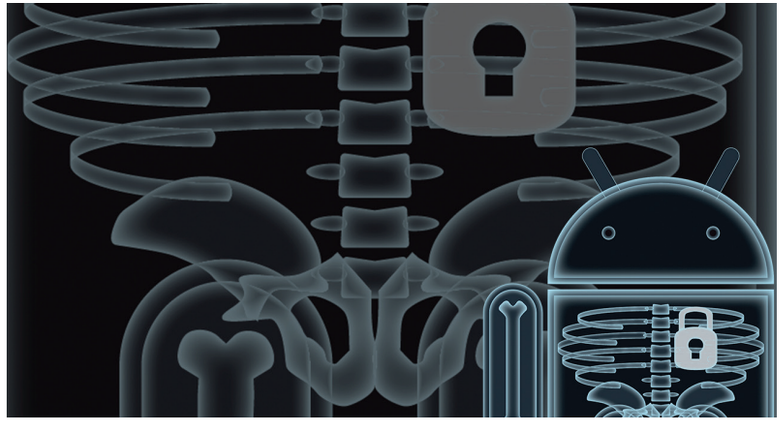
MOBILE SECURITY

Beginnend mit dem ersten iPhone 2007 über die breite Verfügbarkeit von Android-Geräten für den Massenmarkt sind mobile Endgeräte wie Smartphones oder Tablets heute fester Bestandteil des privaten und beruflichen Lebens. Viele der Millionen von Apps haben mittlerweile die Grenzen des mobilen Geräts selbst überwunden – sie greifen auf Cloud-Dienste zu oder ermöglichen die Bedienung und Steuerung anderer Geräte. Mobile Endgeräte werden außerdem dafür eingesetzt, Steuergeräte oder auch Fahrzeuge an das Internet anzubinden.
Diese Anwendungsgebiete und ihre weite Verbreitung machen mobile Geräte zu begehrten Zielen für Angreifer.

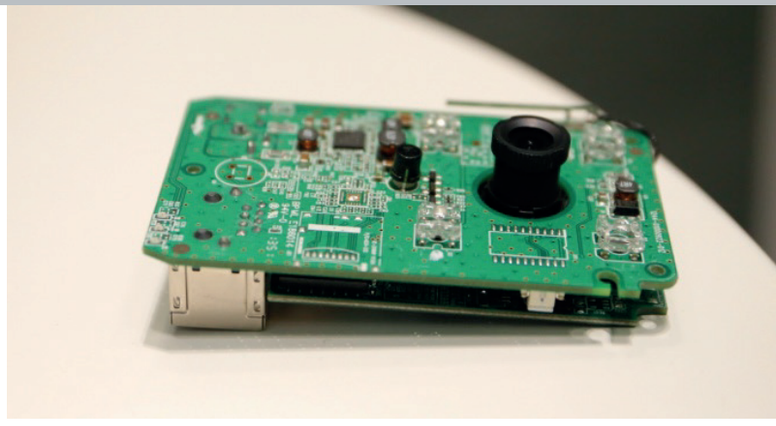
Entwickler von Apps oder Mitarbeiter von Unternehmen, deren Geschäftsmodell auf mobilen Geräten und Anwendungen basiert, sollten sich mit entsprechenden Sicherheitsfragen auseinandersetzen und Schutzmaßnahmen umsetzen können.

Unser Weiterbildungsangebot:

- Sicherheit mobiler Systeme und Anwendungen
- Android: Security und Privacy
- Sicherheit in Mobilfunknetzen
- Security im Fahrzeug



INTERNET OF THINGS



Eingebettete Systeme und mobile Kommunikation sind zwei Grundbausteine für das Internet of Things. Geräte von sehr kleiner Baugröße verfügen häufig nur über wenig Rechenleistung. Andere, die für einen besonders autarken Betrieb entworfen sind, müssen auf Energieeffizienz optimiert werden, um eine möglichst lange Lebenszeit der Geräte zu erreichen. Beschränkungen des verfügbaren Speichers oder lediglich sehr schmalbandige Kommunikationsverbindungen bringen große Herausforderungen hinsichtlich der IT-Sicherheit mit sich. Beispiele für solche Anwendungen sind autonome vernetzte Sensorsysteme, Wearables, e-Health-Systeme/Medizintechnik oder altersgerechte Assistenzsysteme. Die Gewährleistung der Schutzziele Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität für diese Systeme ist eine wichtige Aufgabe. Zudem gilt es zu verhindern, dass diese Systeme für DoS-Angriffe missbräuchlich verwendet werden.

Unser Weiterbildungsangebot:

- Hardware-Sicherheit und -Pentesting
- Sicherheit vernetzter Sensorsysteme
- Sichere schmalbandige Kommunikation
- Kryptographie für das Internet der Dinge