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 solche Systeme für Denial of Service-Angriffe missbräuchlich verwendet werden.

ETHICAL HACKING

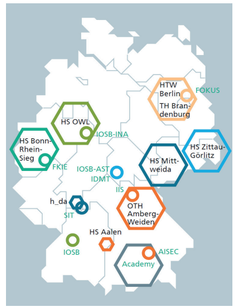
Das Wissen über Schwachstellen und wie sie ausgenutzt werden können sind die Grundvoraussetzungen für zeitgemäße IT-Sicherheitskonzepte. Dieses Verständnis befähigt Sicherheitsverantwortliche in Unternehmen dazu, Sicherheitslücken zu finden, Risiken zu bewerten und Maßnahmen zu ergreifen, um diese zu 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.

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 Erkenntnisse 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
Fraunhofer AISEC
Hochschule Aalen
Ostbayerische Technische Hochschule Amberg-Weiden

Kontakt:
Dr. Daniela Pöhn
Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC
Parkring 4, 85748 Garching bei München
Tel.: +49 89 3229986-129
E-Mail: daniela.poehn@aisec.fraunhofer.de

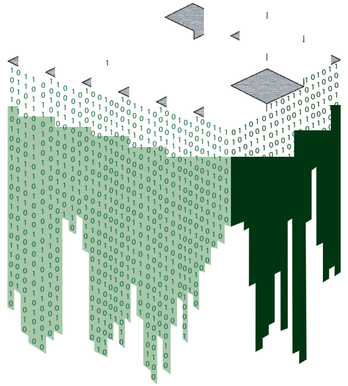


Fraunhofer AISEC

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE UND INTEGRIERTE SICHERHEIT

LERNLABOR CYBERSICHERHEIT

KURSANGEBOT MAI 2017



INTERNET OF THINGS
ETHICAL HACKING
EMBEDDED SYSTEMS
MOBILE SECURITY

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 besitzen, wie die Qualität einzelner Komponenten sowie deren Zusammenwirken zu bewerten ist. Sie müssen aber auch in der Lage sein, erforderliche, individuell auf die Unternehmensbedürfnisse angepasste, eingebettete Software sicher zu entwickeln oder entsprechende Lastenhefte für Dienstleister zu erstellen.

MOBILE SECURITY

Beginnend 2007 mit dem ersten iPhone 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 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 dafür eingesetzt, Steuergeräte oder 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.

MOBILE APPLICATION SECURITY

Erst Apps verwandeln das Smartphone vom Telefon zu einem Multifunktionsgerät. Sie erfüllen unterschiedlichste Funktionen und sind für den Nutzer wichtige Begleiter im Alltag. Doch so einfach die Entwicklung von Apps ist, so einfach ist es auch, unbeabsichtigt sicherheitsrelevante Fehler in einer App zu übersehen. Da Apps zunehmend für kritische Aufgaben (bspw. geschäftliche E-Mails) und in kritischen Bereichen innerhalb von Unternehmen eingesetzt werden, ist es wichtig, von Apps ausgehende Gefahren zu kennen und deren Risikopotential einschätzen zu können. Mit diesem Wissen lassen sich bei der Entwicklung der Apps mit geringem Aufwand Sicherheitsschwächen vermeiden. So können Applikationen mit einem höheren Sicherheitsniveau entstehen. Auch für bereits fertig entwickelte und in den gängigen App-Stores erhältliche Apps ist es wichtig, potenzielle Probleme erkennen zu können, um bspw. deren Einsatz im Unternehmen einzuschränken.

Lernziel

Dieses Modul gibt einen Überblick über das Sicherheitsmodell von Android und iOS, sowie über Analyseverfahren und Tools. Aktuelle Gefahren und Sicherheitslücken von Apps werden aufgezeigt und Hands-on Analyse von Android Apps wird vorgestellt.

Datum	03.05.2017 - 05.05.2017
Ort	Fraunhofer-Institut AISEC, Business Campus, Parkring 4, 85748 Garching bei München
Sprache	Deutsch (auf Anfrage auch Englisch)
Zielgruppe	Entwickler und Tester von Android Apps, Sicherheitsbeauftragte, die über Einsatz von Apps entscheiden
max. Teilnehmer	10
Voraussetzungen	Basiswissen Programmierung, Basiswissen Android Anwendungen
Teilnahmegebühr	1.800€

MASCHINELLES LERNEN

Bei der Analyse großer Mengen an Daten ist maschinelles Lernen in der Lage, Vorhersagen zu machen und Entscheidungen automatisch zu treffen. Im Bereich der Cybersicherheit nimmt die Datenmenge so rasant zu, dass aktuelle Sicherheitslösungen an ihre Grenzen kommen. Darüber hinaus müssen Security-Experten im Wettlauf mit den Angreifern so schnell wie möglich Gegenmaßnahmen entwickeln und einsetzen, um neuartige Angriffe abzuwehren. Dies sind Herausforderungen, denen mit statistischen Methoden wie maschinellem Lernen begegnet werden kann.
Mit maschinellem Lernen können zahlreiche Daten aus Sicherheitskomponenten entnommen und Modelle erzeugt werden. Diese beschreiben die Eingaben und erstellen Vorhersagen, wodurch auch Entscheidungen getroffen werden können. Mit zunehmender Datenmenge werden diese Modelle kontinuierlich präzisiert. So können auch unbekannte Bedrohungen erkannt werden.

Lernziel

Ziel des Kurses ist es, einen Einblick in maschinelles Lernen und Data Mining zu erhalten und diese Grundlagen bei der Modellierung von Anomalieerkennungen zu vertiefen. Vorgestellt werden Grundlagen, Modellierungsmethoden zur Anomalieerkennung und konkrete Vorgehensweisen bei der Programmierung.

Datum	09.05.2017
Ort	Fraunhofer-Institut AISEC, Business Campus, Parkring 4, 85748 Garching bei München
Sprache	Englisch
Zielgruppe	Sicherheitsingenieure, Analysten der IT-Sicherheit, Entwickler sicherer Systeme/Software
max. Teilnehmer	12
Voraussetzungen	Basiswissen Programmierung, Basiswissen IT-Sicherheit, Basiswissen maschinelles Lernen
Teilnahmegebühr	600€

SICHERE IDENTITÄTEN FÜR IoT

Eine sichere IoT-Infrastruktur setzt eine sichere Authentifizierung der verbundenen Geräte voraus. In zukünftigen vernetzten Cyber-Physischen Systemen werden Daten unternehmensübergreifend von Maschine zu Maschine ausgetauscht, wobei Maschinen oder Objekte direkt mit z.B. einem Lieferanten kommunizieren. Ein sicherer Informationsaustausch entlang des gesamten Wertschöpfungsprozesses erfordert Konzepte, um Menschen, Maschinen und Prozesse eindeutig auch über Unternehmensgrenzen hinweg zu identifizieren. Physical Unclonable Functions (PUFs) werten Fertigungsschwankungen in elektronischen Schaltungen aus, um jedem Gegenstand ein einzigartiges Verhalten zu geben. Challenge-Response Protokolle ermöglichen es, mit Hilfe von PUFs Geräte auch ohne kryptografische Algorithmen zu authentifizieren. Zudem können Schlüssel für kryptografische Algorithmen zur Laufzeit mit PUFs erzeugt werden, sodass sie nicht dauerhaft im System gespeichert werden müssen.

Lernziel

Dieses Modul gibt einen Überblick über die Funktionsweise und Anwendungen von PUFs mit Beispielen aus der aktuellen Forschung. Vorgestellt werden Szenarien für den Einsatz von PUFs, Vergleich mit anderen Technologien, PUF-Schaltungen, Protokolle für Lightweight Authentifizierung, Fehlerkorrekturverfahren und Angriffe auf PUFs.

Datum	11.05.2017
Ort	Fraunhofer-Institut AISEC, Business Campus, Parkring 4, 85748 Garching bei München
Sprache	Englisch
Zielgruppe	IT-Security Fachexperten, Hardware-Architekten, Manager oder technische (Projekt-)Leiter in Entwicklungsprojekten
max. Teilnehmer	16
Voraussetzungen	Grundlagen IT-Security. Es wird kein Vorwissen in Hardware Security oder Elektrotechnik benötigt
Teilnahmegebühr	600€

IT-SICHERHEIT IM UNTERNEHMEN

Aufgrund zahlreicher bekannt gewordener Cyberangriffe und Sicherheitsvorfällen rückt das Thema IT- bzw. Cybersicherheit immer mehr in den Fokus der Öffentlichkeit. Betroffene Unternehmen haben in der Regel nicht nur mit den unmittelbaren Konsequenzen eines solchen Angriffs zu kämpfen, sondern sehen sich möglicherweise auch juristischen Folgen und einem erheblichen Imageschaden ausgesetzt. Cybersicherheit umfasst Maßnahmen, um Systeme und einzelne Komponenten vor Manipulationen zu schützen. Man spricht hier vom Schutzziel der Integrität, um die Vertraulichkeit sensibler Informationen, aber auch um die Verfügbarkeit von Funktionen und Diensten zu gewährleisten. Mitarbeiter in allen Branchen und Sektoren brauchen ein Paket an dedizierten Kenntnissen und Fertigkeiten, die sie und ihr Unternehmen befähigt, die Sicherheitslage einzuschätzen und eigene Lösungen zu entwickeln, um Cyberangriffe zu erkennen und abzuwehren.

Lernziel

Ziel des Kurses ist es, ein Grundverständnis für die Funktionsweise von Sicherheitstechniken und -mechanismen zu entwickeln. Zudem werden die Aufgaben der Unternehmensführung im Hinblick auf die Erstellung von Sicherheitsrichtlinien und einer Sicherheitsarchitektur diskutiert.

Datum	18.05.2017
Ort	Fraunhofer-Institut AISEC, Business Campus, Parkring 4, 85748 Garching bei München
Sprache	Deutsch
Zielgruppe	Mitglieder des Vorstands, Geschäftsführer, Verantwortliche der Geschäfts-/ Unternehmensleitung
max. Teilnehmer	16
Voraussetzungen	Keine
Teilnahmegebühr	1.800€