Fraunhofer
ACADEMY

Weiterbildung im
Lernlabor Cybersicherheit

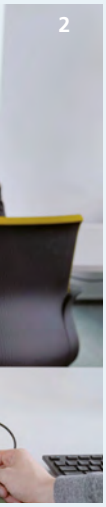
Know-how für mehr IT-Sicherheit

Embedded Security

www.cybersicherheit.fraunhofer.de

Inhalt

1



2

3

Das Lernlabor Cybersicherheit ist Teil der Weiterbildungseinrichtung Fraunhofer Academy im Bereich Information und Kommunikation. Im Zentrum des umfassenden Angebots des Lernlabors stehen alle Themen rund um die IT-Sicherheit.

Impressionen aus unseren Lernlaboren Cybersicherheit:

1 Im Lernlabor Cybersicherheit am Fraunhofer AISEC erhalten Sie Einblick in aktuelle Forschungsthemen, z.B. die Absicherung der Kommunikation in und mit Fahrzeugen. Das Automotive Labor ermöglicht praxisnahe Einblicke.

2 Das Lernlabor Cybersicherheit beim Fraunhofer SIT.

3 Lernlabor Cybersicherheit in Sankt Augustin: Techniken und Strategien für den Hochsicherheitsbereich kennenlernen, z.B. sichere biometrische Gesichtserkennung.

4 Im Lernlabor Cybersicherheit des Fraunhofer FOKUS in Berlin werden verschiedene Gefahrenszenarien simuliert und vernetzte Technologien und Lösungen für die öffentliche Sicherheit praxisnah erprobt.

Mehr Sicherheit mit unseren Weiterbildungen

5 Gründe für die Weiterbildung im Lernlabor Cybersicherheit

5

Anerkannte Expertinnen und Experten

Profitieren Sie vom langjährigen Spezialwissen unserer Expertinnen und Experten aus der Forschung und unseren Entwicklungs- und Beratungsprojekten. In Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen erhalten Sie verwertbare, neueste Erkenntnisse auf allen Gebieten der Cybersicherheit.

Bei uns bekommen Sie Wissen aus erster Hand

Unsere Kurse sind nicht nur auf dem aktuellsten Stand der Forschung, sie orientieren sich auch passgenau an praktischen Fragestellungen und weisen statt grauer Theorie einen großen Praxisanteil in den Laboren auf. Im Team trainieren und erarbeiten Sie Lösungskonzepte in den Bereichen, die für Sie tatsächlich relevant sind.

Maßgeschneiderte Inhouse-Seminare

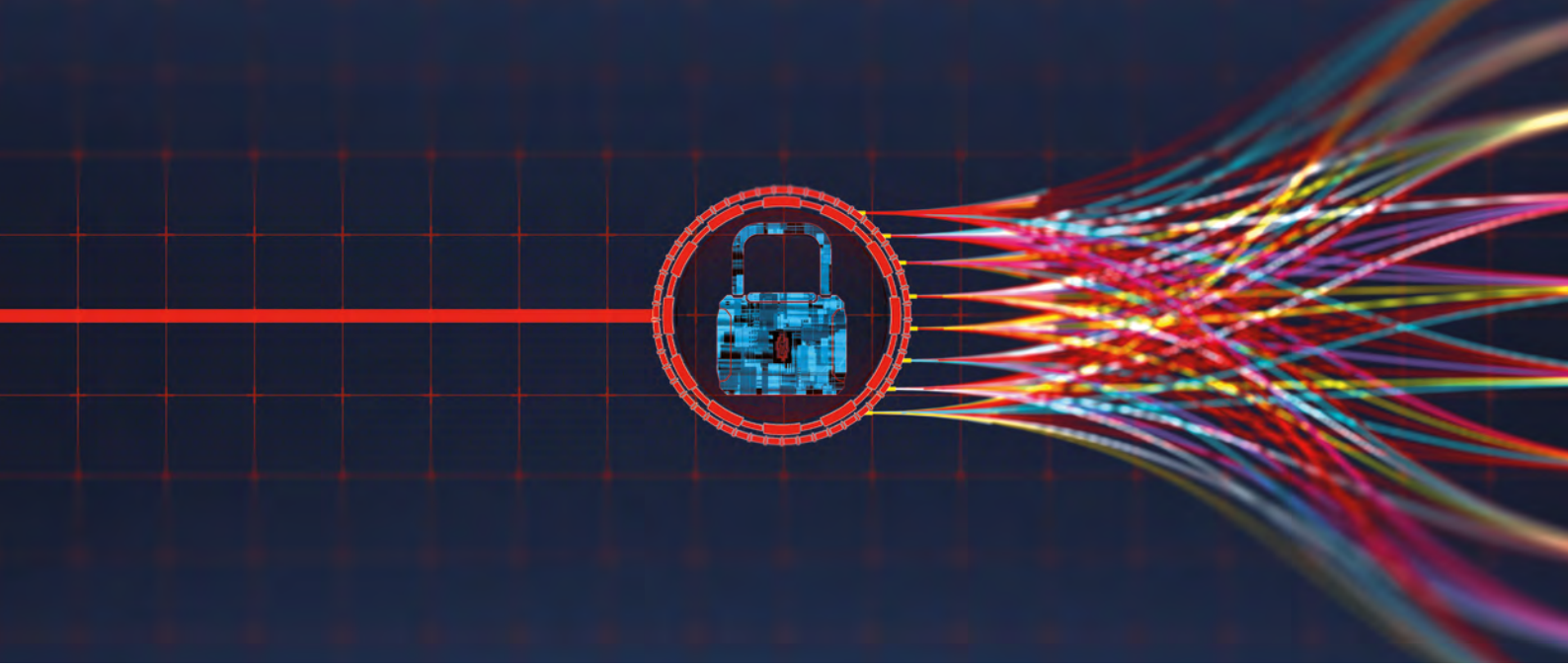
Integrieren Sie die Weiterbildung zum Thema Cybersicherheit direkt in Ihr Unternehmen, für mehrere Mitarbeitende oder Abteilungen. Dafür passen wir die Inhalte individuell auf Ihre Bedarfe an. Wir beraten Sie gerne, welche Lösung für Sie die optimale darstellt.

Für jede Situation das passende Seminar

Ein Universalkonzept bei IT-Sicherheitslösungen gibt es nicht! Die Komplexität und das Spektrum an Problemfeldern ist einfach zu groß. In unserem breiten Themenangebot finden Sie jedoch garantiert die passende Weiterbildung. Zugeschnitten auf Ihren Kenntnisstand und auf Ihr Spezialgebiet. Ob als Onlineseminar, Präsenzseminar oder Mix aus beidem.

Lernlabore

An zahlreichen Standorten in Deutschland können Sie in unseren modernen Lernlaboren mithilfe hochwertiger technischer Infrastruktur reale Bedrohungsszenarien nachstellen und durchspielen. Anhand konkreter Anwendungsfälle wird so das Gelernte für Sie erfahrbar und direkt umsetzbar.



Kompetenzaufbau auf allen Ebenen

IT-Sicherheitswissen betrifft nicht mehr nur Spezialistinnen und Spezialisten, auch entscheidungsbefugte Personen, Fachkräfte und Anwendende sollten lernen, Sicherheitsrisiken abzuschätzen und diese zu beherrschen. Hierfür benötigen die Mitarbeitenden eine Bandbreite an Qualifikationen und ein tiefes Verständnis für die Bedeutung und die Konsequenzen von IT-Sicherheitsproblemen in ihrem Verantwortungsbereich. Das Lernlabor richtet sich deshalb an folgende Zielgruppen mit jeweils spezifischen Seminaren:

Führungskräfte, die Entscheidungsprozesse verantworten müssen, benötigen einen verständlichen Überblick über aktuelle Gefahren, Sicherheitsstrategien und Methoden.

Sicherheitsexpertinnen und -experten mit einer IT-Sicherheits-ausbildung oder entsprechender Berufserfahrung können ihr Wissen auf den neuesten Stand bringen.

Fachkräfte, Spezialistinnen und Spezialisten, die Sicherheitsexpertise aufbauen müssen.

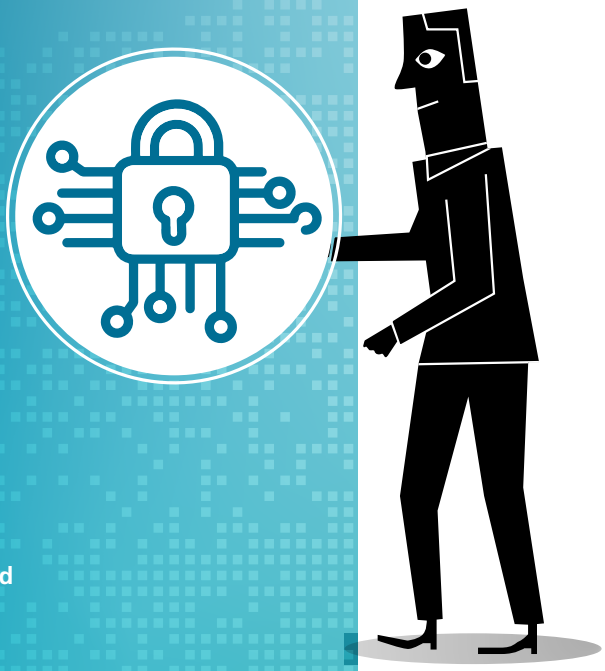
IT-Nutzerinnen und -Nutzer ohne spezifische Fachkenntnisse, von denen erwartet wird, dass sie Sicherheitsbewusstsein aufbauen und sicherheitskonformes Verhalten entwickeln.

Erklärung der Symbole auf den Seminarseiten

- Abschluss
- Voraussetzungen
- Zielgruppe
- Dauer
- Kosten
- Örtlichkeit

Embedded Systems

Kritische Systeme verstehen lernen



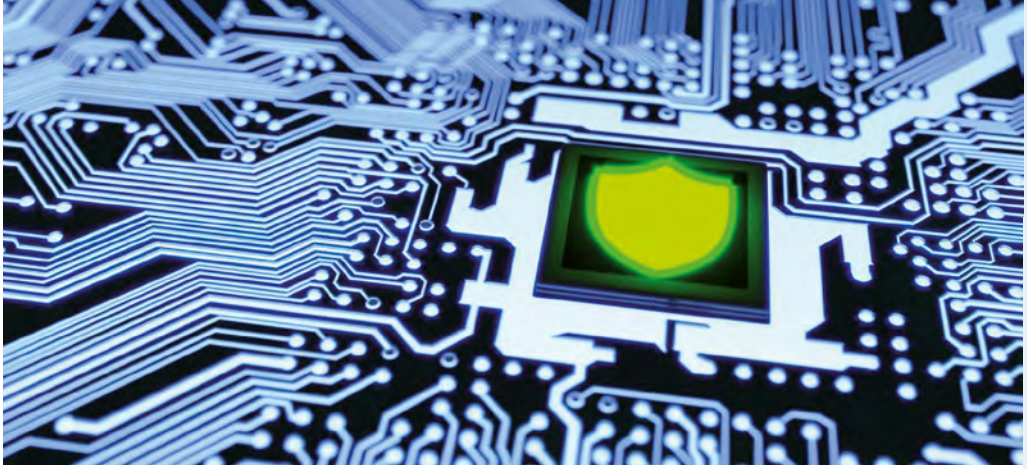
Embedded Systems nehmen im Alltag und in der Industrie eine sehr wichtige Rolle ein. Allgemein gesprochen, vereinfachen sie Prozesse in denen ein Datenaustausch stattfindet. Insbesondere im letzten Fall bieten sie deshalb einen Mehrwert für die Produktion, indem sie Abläufe gezielter durchführen und darüber hinaus effizienter gestalten.

Wie diese Abläufe funktionieren, ist für die Anwendenden aber nicht immer ersichtlich, unter anderem wegen der hohen Vernetzung der Systeme. Sicherheitsprobleme bei eingebetteten Systemen sind daher sehr sensibel und schwer einzuschätzen. Gefährdet sind mobile Geräte und Geräte des IoT. Aber auch Systeme der industriellen Produktion, Energieversorgung oder der Fahrzeugtechnik. Im schlimmsten Fall drohen Manipulationen und Produktionsausfälle.

Umso wichtiger ist es deshalb, kritisch zu bleiben und Sicherheitsaspekte mitzudenken. Schützen Sie sich vor Datenmanipulationen oder einer unerlaubten Speicherung und Verwendung Ihrer Informationen.

Das Lernlabor Cybersicherheit bietet dahingehend ausgewählte Seminare zu verschiedenen Schwerpunktthemen an. Lernen Sie darin, wie einzelne Komponenten zusammenwirken und wodurch sich daraus Sicherheitslücken ergeben können. Lernen Sie verschiedene Typen von Sicherheitsproblemen kennen, und wie diese analysiert werden. Die Seminare folgen dabei stets einem lösungsorientierten Ansatz, indem es Raum für praxisnahe Übungen und Sicherheitskonzepte gibt.

Da sich Sicherheitsprobleme der Embedded Security schnell verändern, ist eine Ausrichtung auf den Forschungs- und Entwicklungsbereich essenziell.



Embedded Systems | **Online**

Security in Embedded Systems

Informiert bleiben – gewappnet sein!

Die Herausforderung: Cybersicherheit eingebetteter Systeme umfassend und effizient prüfen. Neue Schnittstellen und Vernetzung zeigen: IT-Sicherheit von eingebetteten Systemen ist zentrales Qualitätsmerkmal. Sicherheitsprobleme sind hier unerwartet und schwer einzuschätzen. Dieses Seminar bereitet Sie auf unberechenbare, intelligent agierende Angriffe vor. Wie sieht ein ganzheitlicher Schutz sowohl bei Hard- als auch Software aus? Praxisorientiert lernen Sie wichtige Aspekte und Konzepte kennen.

Inhalte des Seminars

Einführung:
Security von Embedded Systems
- Welche spezifischen Herausforderungen zeigen sich für Embedded Systems?
- Welche Angriffsmodelle und Angriffsvektoren liegen vor?

Community Challenge
- Austausch mit anderen Teilnehmenden
- Diskussion am Beispiel aktueller Angriffe auf Embedded Systems

Hardwareangriffe auf Embedded Systems
- Wie sehen Angriffe in der Praxis aus?
- Untersuchung von invasiven und nicht invasiven Angriffen
- Wie funktionieren Seitenkanalangriffe und Laser-/EM-Impulsangriffe?
- Wie kann Hardware die Systemsicherheit unterstützen?

Case Study
- Möglichkeit, an einer Fallstudie das bisher Erlernte anzuwenden und zu vertiefen

Security für Embedded Systems Software
- Typische Bedrohungen im Bereich Software
- Wie schütze ich meine Systeme?

Case Study
- Beweisen Sie Ihren bisherigen Wissensstand an einer Fallstudie

Sicherheit im Entwicklungsprozess
- Allgemeine Probleme und Schwachstellen
- Untersuchung von Sicherheitslücken über den gesamten Lebenszyklus

Ihr Nutzen

- Nach dem Seminar können Sie Sicherheitsaspekte beim Einsatz und der Entwicklung von Embedded Systems verstehen.
- Sie lernen, mögliche Gefahren und Schwachstellen zu erkennen.
- Sie können die Schutzanforderungen von Hardware und Software nachvollziehen.
- Sie haben die Grundprinzipien sicherer Entwicklungsprozesse für Embedded Systems gelernt und können sie für Ihr Arbeitsumfeld richtig umsetzen.

Informationen im Überblick

Grundlegende IT-Kenntnisse und IT-Sicherheitskenntnisse von Vorteil

Zum Einstieg oder zur Vertiefung in eingebettete Systeme

4,5 Stunden

260,–

online

Veranstaltet durch

Fraunhofer AISEC

Fraunhofer FKIE

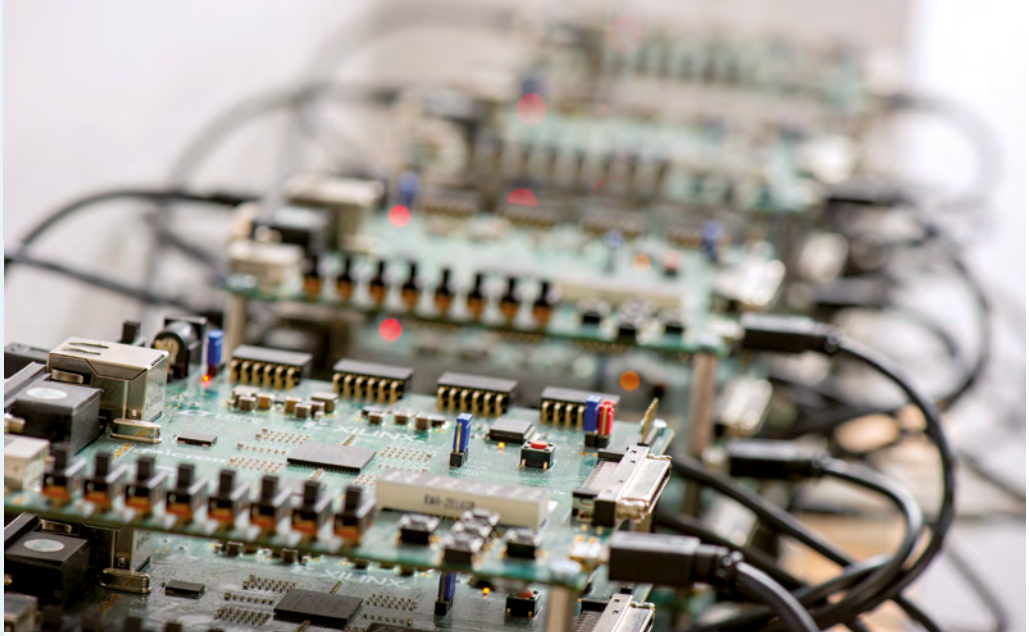
Referenten:

Andreas Seelos-Zankl, wiss. Mitarbeiter Fraunhofer AISEC

Johannes vom Dorp, Forschungsgruppenleiter Applied System Analysis Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/security-in-embedded-systems-online



Absicherung FPGA-basierter Systeme

IT-Sicherheit in komplexer Umgebung

Informationen im Überblick

- Idealerweise Grundlagen IT-Security und FPGA Design (wird optional vermittelt)
- Embedded Systems & Hardware Architekt*innen und Entwickler*innen, Technische Leitung, Fachexpert*innen
- 1 – 2 Tage Präsenz
- 600,– bzw. 1200,–
- Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referentin:

Nisha Jacob Kabakci,
wiss. Mitarbeiterin
Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/eingebettete-systeme-fpgas

Die Herausforderung: Flexible und sichere FPGA-Systeme (Field Programmable Gate Array) bauen. Rekonfigurierbare Hardware-Bausteine, sogenannte FPGAs, ermöglichen die Beschleunigung von Netzwerkfunktionen. Ihre Programmierbarkeit erlaubt neue Flexibilität. Ein Vorteil, der auch Angriffsmöglichkeiten bietet. Für die IT-Sicherheit zeigt das: Es braucht ein hohes Maß an Erfahrungswissen. Dieses Seminar stattet Sie damit aus. In einem Vorgespräch lassen sich die Inhalte des Seminars deshalb unternehmensspezifisch anpassen.

Inhalte des Seminars

Einführung in die Marktanalyse FPGA
- Einordnung mit einem unabhängigen Marktüberblick FPGA
- Angriffe auf FPGA
- Reverse Engineering
- Seitenkanalangriffe
- Fehlerangriffe

Sicherheitskonzepte für FPGAs in Embedded Systems
- Secure HDL Coding Style
- Systematische Prüfung der Sicherheit des Gesamtsystems

FPGA Auswahlkriterien
- Sicherheitsfunktionen kommerziell verfügbarer FPGAs

Ihr Nutzen

- Nach dem Seminar haben Sie einen Überblick über aktuelle Angriffe auf FPGAs und können diese verstehen.
- Sie wissen, welche Gegenmaßnahmen mit aktuellen Chips implementiert werden können.
- Sie wissen, wie Sie ein sicheres FPGA-basiertes System designen können.
- Sie sind in der Lage, anhand von relevanten Kriterien den geeigneten FPGA für die Absicherung Ihres Systems auszuwählen.

Hardwareunterstützte Analyse eingebetteter Systeme

Dem Angreifer einen Schritt voraus

Die Herausforderung: Software ist nicht der einzige Angriffsvektor. Haben Hacker physikalischen Zugriff auf IoT-Systeme, können sie diese manipulieren, und es entstehen enorme, mächtige Angriffsmöglichkeiten. Darum sind reine softwarebasierte Schutzkonzepte obsolet! Lassen Sie die IT-Sicherheit der Hardware nicht außen vor, und schützen Sie so Ihre IoT-Systeme. Erfahren Sie, warum Sie bereits in der Designphase physikalische Angriffe einbeziehen müssen, und lernen Sie diese abzuwehren.

Inhalte des Seminars

Suche von Debug Interfaces

Auslesen/Modifizieren von Flash-Chips/ Reverse Engineering von Flash-Inhalten (Disassembly und Reversing spezieller Architekturen)

Glitching (Spannung, Clock) -HW

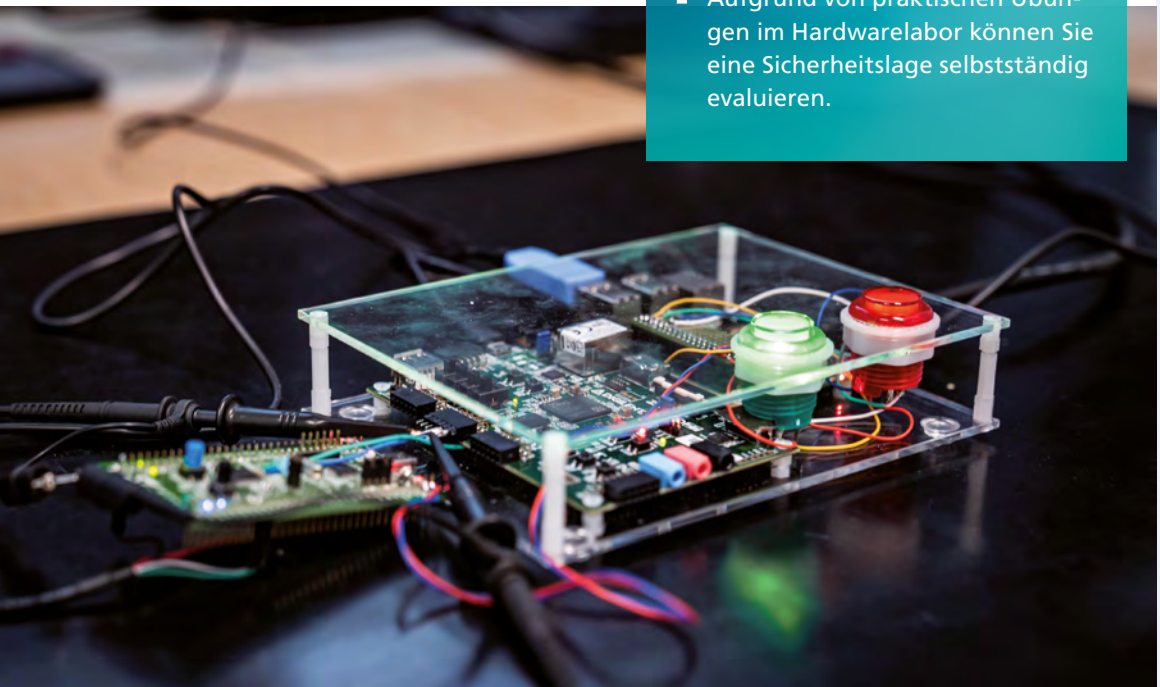
Reverse Engineering von Feldbussen: Analyse/Manipulation von CAN-Kommunikation

Pentesting von Netzwerkgeräten

Evaluierung von Produktschutzmaßnahmen: Überprüfung der vom Hersteller angebotenen Schutzmechanismen

Ihr Nutzen

- Nach dem Seminar verstehen Sie, welche Möglichkeiten hardwarenahe Analysen bieten, und welches Equipment benötigt wird.
- Sie können mehrere Angriffswege praktisch durchführen.
- Sie verstehen, welche Geräte bedroht sind, und welche Maßnahmen Sie zum Schutz ergreifen müssen.
- Aufgrund von praktischen Übungen im Hardwarelabor können Sie eine Sicherheitslage selbstständig evaluieren.



Informationen im Überblick

Grundkenntnisse werden bedarfsgerecht ermittelt, Kenntnisse von Linux und Mikrokontrollern von Vorteil

Architekt*innen, Entwickler*innen sowie Pentester von eingebetteten Systemen

2 Tage Präsenz

1200,–

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referent:

Dr.-Ing. Matthias Hiller, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/hw-analyse

Informationen im Überblick

- Basiswissen zu Programmierung, IT-Sicherheit und maschinellem Lernen
- Sicherheitsingenieur*innen, Analyst*innen Entwickler*innen sicherer Systeme/Software
- 1 Tag Präsenz bzw. online
- 600,–
- Garching bei München, inhouse oder online

Veranstaltet durch

Fraunhofer AISEC

Referent:

Nicolas Müller, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/maschinelles-lernen

Maschinelles Lernen für mehr Sicherheit

Mit ML unbekannte Angriffe erkennen!

Die Herausforderung: Sicherheitslösungen skalieren bei zunehmenden Datenmengen nicht. In der Cybersicherheit fallen, wie in vielen anderen Bereichen auch, immer mehr Daten an, die es zu analysieren gilt, z. B. Log-Dateien oder Mitschnitte von Netzwerkverkehr. Diese Daten von Menschen analysieren zu lassen, skaliert nicht. Auch signaturbasierte Analysetools lösen dieses Problem nicht, da sie sich auf Signaturen verlasssen, die wiederum von Menschen erstellt werden – was auch die Erkennung von unbekannten Angriffen (Zero-Days) einschränkt.

Die Folge: Nur, was in den Signaturen abgedeckt ist, kann (unter kostspieligem Einsatz von Experten) überhaupt erkannt werden.

Inhalte des Seminars

Überblick über die Schnittmenge von Cybersicherheit und maschinellem Lernen

Datengewinnung und Preprocessing mit Fokus auf Cyber-Security-Daten

Grundlegende Prinzipien ML: Konzepte und Algorithmen

Use Case: Anomalieerkennung

Praktische Hinweise/Tools/Hilfestellung bei der Erstellung eigener ML-Systeme

Ausblick & State of the Art, z.B. Adversarial Machine Learning

Ihr Nutzen

- Nach dem Seminar sind Sie in der Lage einzuschätzen, in welchen Bereichen sich maschinelles Lernen sinnvoll einsetzen lässt.
- Sie können Programmierungen und Modellierungen zur Anomalieerkennung vornehmen.
- Sie bekommen einen Einstieg in die Themen der Cybersicherheit, bei welchen maschinelles Lernen relevant ist.
- Sie führen praktische Übungen am Use Case Anomalieerkennung durch.
- Sie erhalten State-of-the-Art-Wissen zu maschinellem Lernen und neuen Forschungen.

Embedded Systems | **Präsenz**

Embedded Security Engineering

Mit Praxisbeispielen für Automotive und IoT

Die Herausforderung: Cybersicherheit für eingebettete Systeme methodisch entwickeln und umsetzen. Lernen Sie anhand eines konkreten Anwendungsfalls, eine systematische Entwicklungsmethodik anzuwenden, wie es z.B. im Automobilbereich in der ISO/SAE 21434 gefordert wird. Adressiert werden dabei Fragestellungen wie leichtgewichtige Kryptographie mit geeignetem Schlüsselmanagement, Hardware-Sicherheitskonzepte wie TPM 2.0 und die Entwicklung von Protokollen.

Inhalte des Seminars

Grundlagen einer systematischen Entwicklungsmethodik
- IT-Sicherheit und Kryptographie
- Entwicklungsprozesse
- Herausforderungen bei der Absicherung eingebetteter Systeme

Kryptographie für eingebettete Systeme
- Leichtgewichtige Kryptographie und Schlüsselmanagement
- Langzeitsicherheit (z.B. Migrationsstrategien, Post-Quantum-Kryptographie)
- Netzwerksicherheit und Kryptographische Protokolle (z.B. Secure Over-the-air Code Update)

Hardware-Sicherheit, Plattformintegrität und Geräteidentität
- TPM 2.0, leichtgewichtige Alternativen
- Attestierungsprotokolle
- Secure Boot

Separations- und Isolationslösungen
- z.B. Mikrokern-Betriebssysteme

Standardisierung
- ISO/SAE 21434, ISO15118

Ihr Nutzen

- Nach dem Seminar können Sie die verschiedenen Arten von Gefährdungen verstehen und bewerten.
- Sie lernen, grundlegende Begriffe der IT-Sicherheit und Kryptographie zu verstehen und einzuordnen.
- Sie können Bedrohungs- und Risikoanalysen durchführen.
- Sie lernen, Sicherheitskonzepte und -protokolle systematisch zu entwickeln, Sicherheitslösungen praktisch umzusetzen und entwickelte Sicherheitslösungen in ihrer Wirksamkeit zu bewerten.

Informationen im Überblick

Gutes Verständnis technischer Systeme, idealerweise im Bereich eingebettete Systeme

Entwickler*innen aus den Bereichen Automotive, IoT und weiteren Domänen im Embedded-Bereich, Technische Leiter*innen in Entwicklungsprojekten

2 Tage

1200,–

Darmstadt

Veranstaltet durch

Fraunhofer SIT

Referent:

Dr. Dirk Scheuermann,
wiss. Mitarbeiter
Fraunhofer SIT

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/embedded-security-engineering

Mobile Security

Sicherheitsfalle Mobilgerät?!

Mobile Endgeräte sind ein selbstverständlicher Teil unseres Alltags- und Berufslebens. Gerade deshalb dringen sie aber auch in besonders kritische Bereiche der persönlichen Sphäre und des Unternehmensnetzwerks ein. Bleiben Sie deshalb am Ball und bedenken Sie mögliche Sicherheitsaspekte jener Geräte.

Geschätzt werden mobile Geräte insbesondere aufgrund ihrer hohen Funktionalität. Zum Beispiel durch mobiles Internet oder Apps. Dieses hohe Maß an Anwendbarkeit bietet jedoch in vielerlei Hinsicht verschiedene Angriffsmöglichkeiten. Hinzu kommt der stetige Wandel der Technologie wie im Bereich Mobilfunkstandard, welcher schnell zu Verunsicherung führen kann hinsichtlich der Sicherheitsaspekte.

Anwendungen werden breiter und vernetzter genutzt, weshalb IT-Sicherheitsaspekte nicht mehr allein die Entwickelnden oder Administratorinnen und Administratoren betreffen, sondern auch die Anwendenden. Informieren Sie sich daher im Lernlabor Cybersicherheit und lernen Sie, Bedrohungen vorzubeugen, diese einzuschätzen und abzuwenden!

Lernen Sie anhand aktuellster Erkenntnisse und vieler Praxisbeispiele, welche Bereiche besonders beachtet werden müssen, und welche Sicherheitsmechanismen angewendet werden sollten. Erproben Sie die Funktionalität Ihres Geräts anhand von Praxisbeispielen.

Mobile Endgeräte bedürfen genauso wie Desktop Geräte einer zentralen Überwachung, einer Versorgung mit Updates und dem Schutz vor Sicherheitslücken.

IT-Sicherheit in der Fahrzeugkommunikation

Schutzbedarfe erkennen

Die Herausforderung: Immer mehr Vernetzung im Fahrzeug. Fahrzeugkommunikation wird immer komplexer: Das zeigen neue Funktionalitäten und die zunehmende Vernetzung von Steuergeräten. Daraus ergeben sich Angriffsmöglichkeiten auf die Sicherheit anderer Verkehrsteilnehmer, Privatsphäre und Geschäftsmodelle für Hersteller. Bereiten Sie geeignete Schutzmaßnahmen für die Fahrzeugumgebung vor. Dieses Seminar zeigt Ihnen beispielsweise, wie sich fahrzeuginterne BUS-Systeme evaluieren und verbessern lassen. Hier erfahren Sie die Chancen und Risiken.

Inhalte des Seminars

Einführung IT-Sicherheit im Automotive- Umfeld
- Vorstellung ausgewählter IT-Sicherheitsvorfälle und deren technischer Hintergrund

Kryptographische Grundlagen
- Interaktive Übungen mit Alltagsbezug
- Prinzipien der Verschlüsselung und digitaler Strukturen

IT-Sicherheit von Fahrzeug-BUS-Systemen
- Übersicht gängiger Architekturen
- IT-Sicherheitseigenschaften
- Einführung in die gängigen Betriebssysteme im Fahrzeugumfeld
- Diskussion möglicher Angriffe

Grundlagen und IT-Sicherheitsaspekte der V2X-Kommunikation
- Schutz vor manipulierten Nachrichten
- Schutz der Privatsphäre
- Security-Format der V2X-Nachrichten: ETSI TS 103 097
- Ausschluss von Teilnehmern bei Missbrauchsfällen

Einführung in Trust Assurance Levels (TAL) als Beispiel einer Lifecycle-übergreifenden IT-Sicherheitslösung

Ihr Nutzen

- Nach dem Seminar beherrschen Sie Kryptographische Grundlagen.
- Sie haben einen Überblick über gängige BUS-Systeme, sowie deren IT-Eigenschaften.
- Sie haben eine Vorstellung von der fahrzeuginternen Vernetzung und vom Security-Format der V2X-Kommunikation.
- Sie kennen das Identitätsmanagement der V2X-Kommunikation im Spannungsfeld von Sicherstellung der Authentizität sicherheitsrelevanter Nachrichten und dem Schutz der Privatsphäre.
- Sie haben die Grundprinzipien sicherer Entwicklungsprozesse für Embedded Systems gelernt und können diese für Ihr Arbeitsumfeld richtig umsetzen.

Mobile Security | **Präsenz**

Informationen im Überblick

Grundkenntnisse Fahrzeug-IT

Mitarbeitende von Automobilherstellern, und -zulieferern, die nicht über tieferes IT-Sicherheitswissen verfügen

1 Tag Präsenz

600,–

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referenten:

Daniel Angermeier, stellv. Abteilungsleiter Fraunhofer AISEC

Dr. Sven Plaga, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/fahrzeugkommunikation

Informationen im Überblick

Grundlegende IT-Kenntnisse

Systemarchitekt*innen, Anwender*innen und Betreiber*innen von 5G- Technologien

2 Tage Präsenz

max. 16 Teilnehmende

1200.–

Bonn

Veranstaltet durch

Fraunhofer FKIE

Referent:

Dr. Michael Rademacher, IT-Sicherheitsforscher am Fraunhofer FKIE

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/5g

5G, aber sicher?

Neue Architektur – neue Risiken?!

Die Herausforderung: Sicherheitslücken des neuen Standards erkennen. Neue Technologien öffnen zunächst viele Möglichkeiten. Aber Anforderungen wie Geschwindigkeit, Kostenersparnis und sparsamer Energieverbrauch bedürfen unterschiedlicher Sicherheitsstrategien. Der Kurs zeigt Ihnen potenzielle Angriffsszenarien, speziell für industrielle Anwendungen. Machen Sie sich mit der 5G-Architektur vertraut und schützen Sie Ihr System. Erfahren Sie in diesem Seminar, wie neueste Entwicklungen in mögliche Sicherheitskonzepte integriert werden können.

Inhalte des Seminars

Überblick über 5G
- Aktueller Stand der Spezifikation
- Eigenschaften des Mobilfunkstandards

Ausgewählte 5G-Technologien im Blick
- Multi Edge Computing
- Campus-Netze
- Network Function Virtualisation (Slicing)

Anwendungsbeispiele
- Direkt aus der Praxis
- Expertise der wissenschaftlichen Fraunhofer-Referenten/innen

Ihr Nutzen

- Nach dem Seminar können Sie die Eigenschaften der 5G-Technologien und deren Anwendungsbereiche beurteilen, insbesondere in 5G vorgesehene Features.
- Sie erhalten einen Einblick über 5G-Sicherheitsmaßnahmen.
- Sie können abschätzen, welche Maßnahmen zur Absicherung Ihrer 5G-basierten Anwendungen ausgewählt werden sollten.

Internet of Things – IoT

Schutzmechanismen für Kommunikationssysteme

Nicht nur im Privaten sind wir von immer mehr Geräten umgeben, die digital miteinander vernetzt sind. Auch in der Wirtschaft hat das Internet der Dinge (IoT) einen hohen Stellenwert eingenommen. Geräte des IoT gestalten unseren Alltag bequemer und verkürzen Arbeits- sowie Produktionsprozesse, indem sie untereinander intelligent kommunizieren: vorausgesetzt, diese Netzwerke funktionieren auch zuverlässig.

Die direkte Anbindung an das Internet, insbesondere in drahtlosen Netzwerken, bietet die perfekte Basis für Eindringlinge und Gefährder. Hinzu kommt, dass IT- Sicherheitsaspekte, schon bei der Herstellung der Geräte, oft in den Hintergrund rücken. Auch weil sich Endverbraucher zu sehr auf dem Nutzen von Funktionen ausruhen. Umso wichtiger ist es deshalb, schon bei der Integration der Geräte mögliche Sicherheitslücken nicht zu übersehen.

Denn in Folge könnten Fremde Einsicht in persönliche Daten erhalten, sich Zugriff auf Zugangsdaten verschaffen, Geräte manipulieren und in Konsequenz gravierende persönliche und wirtschaftliche Schäden anrichten.

Im Lernlabor Cybersicherheit lernen Sie, wie man mögliche Sicherheitsrisiken aufspürt und identifiziert. Durch die verschiedenen Kurse erfahren Sie, wie IoT- Kommunikationssysteme abgesichert werden, und so ein reibungsloser Austausch von Daten gewährleistet wird. Das Wissen, das durch intensive Forschungsarbeit der Fraunhofer Mitarbeiterinnen und Mitarbeiter generiert wurde, fließt dabei direkt mit in die Kursinhalte ein.

IoT ist höchst anfällig für Sicherheitsrisiken. Dies betrifft nicht nur mobile Geräte und Computer, sondern zunehmend auch intelligente Fertigungsanlagen.

Informationen im Überblick

Grundlegende IT-Kenntnisse, Grundlegende IT-Sicherheitskenntnisse von Vorteil

Software Architekt*innen und Entwickler*innen in IoT, Admins, Betreiber*innen

1 Tag Präsenz

600,–

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referent:

Sascha Wessel, Abteilungsleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/absicherung-iot-systeme

Absicherung von IoT-Systemen

Sicherheits-Albtraum IoT?

Die Herausforderung: Vielfältige Sicherheitslücken machen IoT zum leichten Angriffsziel. Die Problemfaktoren: Anbindung zum Internet, geringfügige Absicherung und wenig Rechenleistung. Neben all dem eröffnen sie aber in der Regel Zugang zu persönlichen Daten und vertraulichen Informationen von Unternehmen. Dieses Seminar stattet Sie mit notwendigem Wissen zu Sicherheitslücken im IoT-Bereich aus. Welche möglichen Sicherheitsrisiken gibt es in der Kommunikationsarchitektur? Lernen Sie anhand von realen Beispielen, wie Sie Ihr System schützen können.

Inhalte des Seminars

Überblick zum Angriffsziel IoT
- Sicherheitslücken bei IoT
- Vorführungen zum Google Hacking

Vertiefte Analyse der IoT-Architektur
- Risiken und Bedrohungen
- Schutzmaßnahmen

Embedded Systems & IoT
- TPM (Trusted Platform Module) und Trusting Computing
- Sicherheitsmechanismen innerhalb des Linux Kernel

Demonstration und Hands-on
- Schwachstellenscanner im direkten Einsatz
- Pentesting für IoT

Ihr Nutzen

- Nach dem Seminar können Sie nicht nur für IoT-Geräte, sondern auch für das gesamte Unternehmensnetz Bedrohungen abwehren.
- Sie wissen, wie man Sicherheitslücken aufspürt, abschätzt und beseitigt.
- Sie lernen, von außen erreichbare IoT-Geräte im Unternehmen zu identifizieren und abzusichern.

Angriffe auf Krypto in IoT

Seitenkanalangriffe verstehen und praktisch durchführen

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

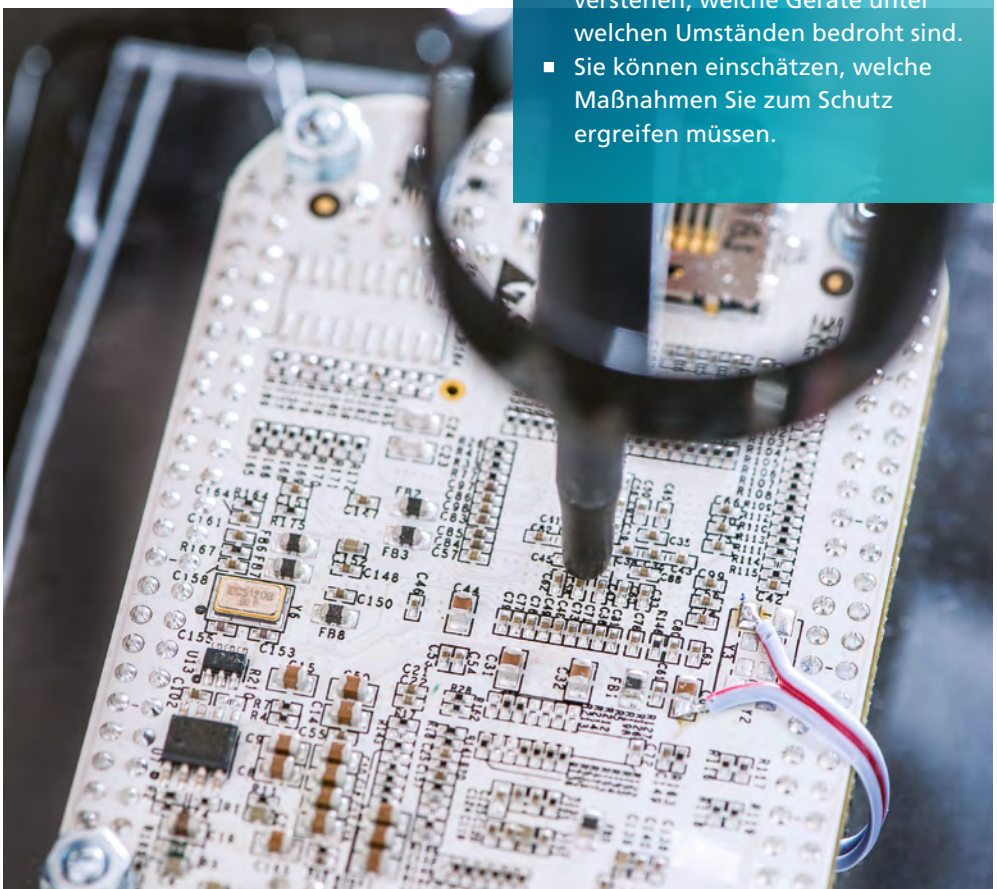
Fokus auf den wesentlichsten Seitenkanalangriff, die Differentielle Power Analyse (DPA)

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.-Ing. Matthias Hiller, Abteilungsleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/seitenkanalangriffe

Informationen im Überblick

Keine Voraussetzungen

Führungskräfte, Fachkräfte und Spezialist*innen, technische Leitung, ggf. inkl. Vertretung von Zulieferern

1-2 Tage Präsenz oder online

jeweils 1400,– pro Experte & Tag

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referent*innen:

Senior Sicherheitsanalysten des Fraunhofer AISEC mit Managementerfahrung

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/lagebewertung

Security-Lagebewertung für vernetzte IoT-Produkte

Wie sicher ist ihr IoT-Produkt?

Die Herausforderung: IT-Sicherheit in komplexen Systemen. Sie arbeiten an einem Produkt oder Service und würden gerne die Sicherheitslage einschätzen? Genügt Ihr aktuelles IT-Sicherheitskonzept den gewünschten Anforderungen, oder haben Sie Schwachstellen übersehen? Lassen Sie in diesem Workshop Ihr (geplantes) IoT-Produkt von wissenschaftlichen Sicherheitsexperten überprüfen. Gemeinsam werden relevante Teilbereiche gesichtet und diskutiert. Sie erhalten individuelle Empfehlungen, die Sie direkt umsetzen können.

Inhalte des Workshops

Mögliche Themen je nach Anforderungen im Unternehmen

- Vorgespräch zu den Inhalten des Workshops
- Systemeinschätzung von den Experten (Senior Sicherheitsanalysten)
- Gemeinsame Besprechung der priorisierten Teilbereiche an den Präsenztagen
- TPM und Trusting Computing
- Umfangreiche Bewertung zur Kritikalität einzelner Bereiche

Ihr Nutzen

- Nach dem Workshop verstehen Sie, welche Möglichkeiten hardwarenahe Analysen bieten, und welches Equipment benötigt wird.
- Sie können mehrere Angriffswege praktisch durchführen.
- Sie verstehen, welche Geräte bedroht sind, und welche Maßnahmen Sie zum Schutz ergreifen müssen.
- Aufgrund von praktischen Übungen im Hardwarelabor können Sie eine Sicherheitslage selbstständig evaluieren.

Internet of Things – IoT
Präsenz

Informationen im Überblick

-Vorteilhaft: Grundkenntnisse über Kryptographie, Computernetzwerke und Linux CLI

Admins, Anwender*innen, Berater*innen, Entwickler*innen

2 Tage Präsenz

Max. 12 Teilnehmer

1200,–

Bonn

Veranstaltet durch

Fraunhofer FKIE

Hochschule Bonn-Rhein-Sieg
University of Applied Sciences

Referent:

Dr. Michael Rademacher, IT-Sicherheitsforscher am Fraunhofer FKIE

IoT-Sicherheit

Sichere Netze und zuverlässige Protokolle

Drahtlose Netze gehören seit Jahren zum Alltag vieler Menschen. Angetrieben durch das „Internet of Things" (IoT) nimmt die Zahl der Geräte, die ständig kabellos kommunizieren, stetig zu. Durch die drahtlose Ausbreitung und die teilweise sehr hohen Reichweiten sind übertragene Daten ohne die richtige Anwendung von Sicherheitsmechanismen leicht mitlesbar oder manipulierbar. Trotz vorhandener Sicherheitsmechanismen in den jeweiligen Protokollstandards fehlt oft das Wissen darüber, welche Möglichkeiten existieren, diese nach dem aktuellen Stand der Forschung zu bewerten und auf einen konkreten Anwendungsfall praktisch anzuwenden.

Inhalte des Seminars

- Grundlagen des IoT
- Überblick (Funk-)Protokolle
- 433 MHz: Einführung und Angriffe
- Proprietäre Protokolle: Analyse und Angriffe mit SDRs
- Bluetooth Low-Energy: Einführung und Sicherheitsmechanismen
- Bluetooth Low-Energy: Praxis/Demos
- Zigbee: Einführung und Sicherheitsmechanismen
- WLAN: Einführung, Sicherheitsmechanismen und Angriffe
- WLAN: Praxis/Demos
- Transport- und Anwendungsprotokolle: MQTT/CoAP
- Absicherung der Protokolle, TLS
- IoT- Sicherheitsaspekte auf höheren Schichten
- Exkurs: Suchmaschine »Shodan«

Ihr Nutzen

- Sie lernen Sicherheitsmechanismen drahtloser Netze für das IoT kennen.
- Nach dem Seminar haben Sie sichere und zuverlässige Protokolle für das IoT kennen gelernt und können diese beurteilen.
- Sie können Sicherheitsmechanismen einschätzen und korrekt anwenden.

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sicherheit-in-drahtlosen-netzen

Security und Privacy von Bluetooth Low Energy

BLE-Applikationen – von Anfang an sicher!

Informationen im Überblick

Grundkenntnisse in Bluetooth Low Energy sowie in Linux CLI und Wireshark sind vorteilhaft

Entwickler*innen und Sicherheitsexpert*innen aus dem Bereich Bluetooth Low Energy oder Fachkräfte, die IT-Sicherheitsanalysen planen, durchführen oder beauftragen.

2 x 3 Std. online

500,–

online

Veranstaltet durch

Fraunhofer SIT

Referent:

Matthias Cäsar, wiss. Mitarbeiter am Fraunhofer SIT

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/bluetooth-low-energy

Die weitreichende Verbreitung von Bluetooth Low Energy (BLE) und die fehlende Absicherung gegen Angriffe in der Grundkonfiguration machen BLE zu einem beliebten Angriffsziel. Umso wichtiger ist es, mögliche Schwachpunkte im BLE-Protokoll zu kennen. In diesem Seminar lernen Sie, welche aktuellen Gefahren es im BLE-Protokoll gibt und wie Sie bestmögliche Sicherheit und Privatsphäre schon bei der Konzeption Ihrer BLE-Applikation berücksichtigen können.

Inhalte des Seminars

Grundlagen Bluetooth Low Energy (BLE)
- Überblick über relevante Layer des Protokolls

Versionsabhängige Sicherheitsaspekte der Pairing-Verfahren und deren Authentifizierungsmethoden
- Legacy Pairing
- LE Secure Connection Pairing
- Hands-on Training mit Wireshark und Crackle

Relevante Schwachstellen im BLE-Protokoll
- sowie Sniffing, MITM- und Hijacking-Angriffe
- Privatsphärenfreundliche Konzepte im BLE-Protokoll
- Demos zu ausgewählten Angriffen

Best-Practice für die Konzeption von BLE-Applikationen

Ihr Nutzen

- Nach dem Seminar können Sie die verschiedenen Pairing-Methoden von BLE hinsichtlich Ihrer Sicherheit einschätzen.
- Sie lernen, die Gefahren von aktuellen Schwachstellen im BLE-Protokoll einzuschätzen.
- Sie können die Auswirkungen der Privacy-Einstellungen von BLE auf die Privatsphäre der Nutzer nachvollziehen.
- Sie berücksichtigen bereits bei der Konzeption Ihrer BLE-Applikationen Sicherheit und Privatsphäre.
- Sie bekommen einen aktuellen und umfassenden Überblick über die Sicherheit und Privatsphäre des BLE-Protokolls.

Produktzertifizierung

Produkte zertifizieren? – Aber bitte!

Das breite Angebot an Produkten erschwert es Kaufenden, die richtige Wahl zu treffen. Deshalb sind verlässliche Anhaltspunkte gefragt, die den potenziellen Kundenkreis informieren und die Auswahl erleichtern.

Zertifizierungen sind mehr als nur Labels. Sie sind notwendig, um Märkte zu strukturieren und zu ordnen. Sie schaffen einheitliche Standards, die von Inhabern des Zertifikats gemeinsam getragen werden. Ziel ist es, ein hohes Maß an Qualität der Produkte zu bestätigen, Leistungsfähigkeit sicherzustellen und, daraus resultierend, einen sicheren Raum zu schaffen, der potenzieller Kundschaft Vertrauen bietet. Doch auch aufseiten der herstellenden Unternehmen können sich Türen zu geregelten Märkten öffnen.

Der Weg zur Zertifizierung ist jedoch nicht immer leicht zu bewältigen. Die Auswahl der passenden Zertifizierung sowie das Abwägen von Kosten-Nutzen-Faktoren können so einige Stolpersteine bereithalten. Schaffen Sie sich daher einen Überblick und besuchen Sie einen der angebotenen Kurse des Lernlabors Cybersicherheit!

In diesen lernen Sie nachzuvollziehen, wie einzelne Zertifizierungen aufgebaut sind, und was Sie beachten sollten. Erfahren Sie, welchen Nutzen, aber auch welche Risiken hinter einer Zertifizierung stehen können. Im Lernlabor können Sie von der wissenschaftlichen Expertise der Mitarbeitenden profitieren und so ihre Produkte zukunftssicher machen.

Zertifikate sind mehr als nur Labels. Sie schaffen Vertrauen und Vergleichbarkeit durch einheitliche Standards bzgl. Funktionalität, Qualität und Sicherheit zertifizierter Produkte.

Produktzertifizierung
Präsenz | Online

Informationen im Überblick

Kenntnisse des Referenzarchitekturmodells IDS, idealerweise Mitglied im IDSA

Unternehmen: Herstellende von IDS-Komponenten; Teilnehmende: Techniker*innen, Entwickler*innen, Product Owner

3–5 Tage (abhängig vom Produkt), Präsenz oder online

nach Vereinbarung

Berlin od. Garching bei München, inhouse oder online

Veranstaltet durch

Fraunhofer FOKUS

Referent*innen:

Nadja Menz, Gruppenleiterin Fraunhofer FOKUS

Sascha Wessel, Abteilungsleiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/ids-komponentenzertifizierung

International Data Space Komponentenzertifizierung

Ist mein Produkt IDS-Ready?

Um Daten als Wirtschaftsgut nutzen zu können, ist ein geregelter und sicherer unternehmensübergreifender Datenaustausch notwendig. Die Initiative International Data Space (IDS) zielt darauf ab, einen sicheren Datenraum zu schaffen, der Unternehmen verschiedener Branchen und aller Größen die souveräne Bewirtschaftung ihrer Datengüter ermöglicht. Im IDS sollen Daten sicher ausgetauscht und mit Nutzungsrestriktionen versehen werden. Die Akzeptanz des IDS im Kontext des Austauschs unternehmenskritischer Daten ist zu gewährleisten. Um dieses Ziel zu erreichen, fällt dem Prozess der Zertifizierung eine zentrale Rolle zu.

Inhalte des Seminars

Modul 0 (2 Stunden als vorbereitende Websession)
- Klärung der Komplexität und der Reife des Produkts
- Ziel: Inhalt und Umfang des Workshops festlegen

Modul I (1 Tag)
- Vorstellung des IDS-Zertifizierungsschemas
- Gemeinsamkeiten und Unterschiede IDS-Zertifizierung und 62443-4-2
- Übersicht Kriterienkatalog
- Produktvorstellung (Kunde)

Modul II (1–3 Tage, nach Bedarf)
- Besprechung der Kriterien
- IDS-spezifische Kriterien
- 62443-4-2-Kriterien
- Entwicklungsspezifische Kriterien

Modul III
- Zusammenfassung der Ergebnisse
- Next Steps für die IDS-Zertifizierung

Ihr Nutzen

- Nach dem Workshop besitzen Sie ein Verständnis von den Komponenten im IDS auf technischer Ebene.
- Sie können die Zertifizierbarkeit des eigenen Produkts beurteilen.
- Sie können Vorteile, Nutzen und Risiken einer IDS-Zertifizierung bewerten.
- Sie können den Aufwand einer IDS-Zertifizierung für das eigene Produkt einschätzen.
- Der Workshop bietet Ihnen eine Entscheidungsgrundlage für die IDS-Zertifizierung Ihres Produkts und eine Einschätzung des Abdeckungsgrades der bereits vorhandenen Kriterien.
- Sie erarbeiten eine konkrete Roadmap mit den noch nötigen Schritten zur IDS-Zertifizierung Ihres Produkts.

Sicherheitszertifizierung von Produkten

Ist eine Common Criteria Zertifizierung für Sie das richtige Mittel der Wahl?

Die Auswahl der passenden Zertifizierung ist nicht immer einfach. Risiken und Vorteilen müssen gegeneinander abgewägt werden. Wenn Sie mit dem Gedanken spielen, eine Common-Criteria-Zertifizierung (CC) zu erwerben, dann bietet dieses Seminar die geeignete Grundlage. Sie lernen die Kernkonzepte kennen und erfahren, wie CC auf Ihrem Produktportfolio anwendbar wäre. Profitieren Sie von den (Wettbewerbs-)Vorteilen, die eine CC-Zertifizierung Ihrem Produkt bietet.

Inhalte des Seminars

Überblick zur Produktzertifizierung
- Prinzip der Zertifizierung: unabhängige Evaluierung, zweite Prüfebene
- Nutzen: Produktqualität, Vertrauenswürdigkeit, Zugang zu regulierten Märkten, Imagevorteile
- Zertifizierungskriterien als dokumentierte Best Practices zum Qualitätsmanagement in der Produktentwicklung

Sicherheitszertifizierung nach Common Criteria
- Fokussierung auf Sicherheitseigenschaften als essenzielles Qualitätsmerkmal
- Vorgeschichte, internationale Standardisierung
- Nationale Schemata und internationale Anerkennung
- Akteure und Arbeitsverteilung in der CC-Zertifizierung
- Konkreter Ablauf des Zertifizierungsverfahrens
- CC-Standarddokumente und Basiskonzepte

Ihr Nutzen

- Nach dem Seminar können Sie das deutsche Zertifizierungsschema des BSI nachvollziehen.
- Sie können die zentralen Konzepte der Common Criteria anwenden.
- Sie lernen, wie man notwendige Aktivitäten auf Herstellerseite abschätzen kann.
- Sie verstehen, die Anwendbarkeit von CC bzgl. Ihres Portfolios abzuschätzen, und können eigens eine CC-Zertifizierung initiieren.

Produktzertifizierung
Präsenz

Informationen im Überblick

Keine Voraussetzungen

Produktmanager*innen, Projektleiter*innen, Produktentwickler*innen, technische Einkäufer*innen für Sicherheitsprodukte

1 Tag Präsenz

600,–

Berlin

Veranstaltet durch

Fraunhofer FOKUS

Referent*innen:

Nadja Menz,
Gruppenleiterin
Fraunhofer FOKUS

Thilo Ernst,
wiss. Mitarbeiter
Fraunhofer FOKUS

Jaroslav Svacina,
wiss. Mitarbeiter
Fraunhofer FOKUS

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/sicherheitszertifizierung-produkte


Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
Sicherheit in Software-Entwicklung & Netzwerken
www.cybersicherheit.fraunhofer.de
Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
IT-Forensik
Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
Organisatorische IT-Sicherheit & Datenschutz
www.cybersicherheit.fraunhofer.de
Fraunhofer ACADEMY
Weiterbildung im Lernlabor Cybersicherheit
Know-how für mehr IT-Sicherheit
Energie- & Wasserversorgung und Public Safety

Möchten Sie Informationen zu einem anderen Themengebiet?

Hier finden Sie alle Broschüren rund um die Weiterbildungen im Lernlabor Cybersicherheit: www.cybersicherheit.fraunhofer.de/downloads

Inhouse- oder Firmen- und Behördenschulungen

Inhouse-Schulungen individuell auf Sie zugeschnitten

Wollen Sie Inhalte aus unserem Kursangebot individuell zusammenstellen, oder finden Sie in unserem Angebot keinen passenden Termin oder Ort? Kein Problem: Stellen Sie Ihre ganz persönlichen Bedürfnisse in den Vordergrund.

Sie haben die Wahl, so geht's:

- Wählen Sie ein Wunschseminar aus unseren vielfältigen Themen aus und bestimmen Sie den Zeitraum und Schulungsort.
- Nennen Sie uns Inhalte aus unseren Kursangeboten, die geschult werden sollen, und wir konzipieren ein passendes Seminar.
- Sie sagen uns, welches spezielle Wissen geschult werden soll, und wir entwickeln eine individuelle Schulung für Sie.

Bei einem individuellen Inhouse-Seminar erhalten Sie genau auf Ihre Bedürfnisse abgestimmtes Wissen – für Ihr Unternehmen, Abteilungen Ihres Unternehmens, für Ihre Behörde, Fachreferate oder einzelne Mitarbeiterinnen und Mitarbeiter. Dabei stehen wir Ihnen sehr gerne beratend zur Verfügung, wenn es um für Sie maßgeschneiderte, inhaltliche Zusammenstellung der vielfältigen Kombinationsmöglichkeiten unserer Themen geht.

Wir als Lernlabor Cybersicherheit bieten Ihnen alle relevanten Elemente aus einer Hand: Die didaktische, mediale sowie technische Umsetzung der Inhalte, aber auch Konzept und Umsetzung.

Fragen Sie uns an!

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne

telefonisch unter +49 89 1205-1555

e-mail: cybersicherheit@fraunhofer.de

www.cybersicherheit.fraunhofer.de

Hier erhalten Sie aktuelles Wissen!

Aktuelle Informationen zu unseren Seminarangeboten, Veranstaltungen und Themen im Bereich Cybersicherheit finden Sie hier:

www.cybersicherheit.fraunhofer.de

Stöbern Sie in unserem Blog und erfahren Sie, was unsere Fachexpertinnen und -experten über aktuelle Themen im Bereich Cybersicherheit berichten:

www.cybersicherheit.fraunhofer.de/de/blog

Abonnieren Sie unseren Newsletter und bleiben Sie so auf dem Laufenden:

www.cybersicherheit.fraunhofer.de/newsletter

Weitere Informationen rund um das Thema Weiterbildung bei der Fraunhofer Academy erhalten Sie hier:

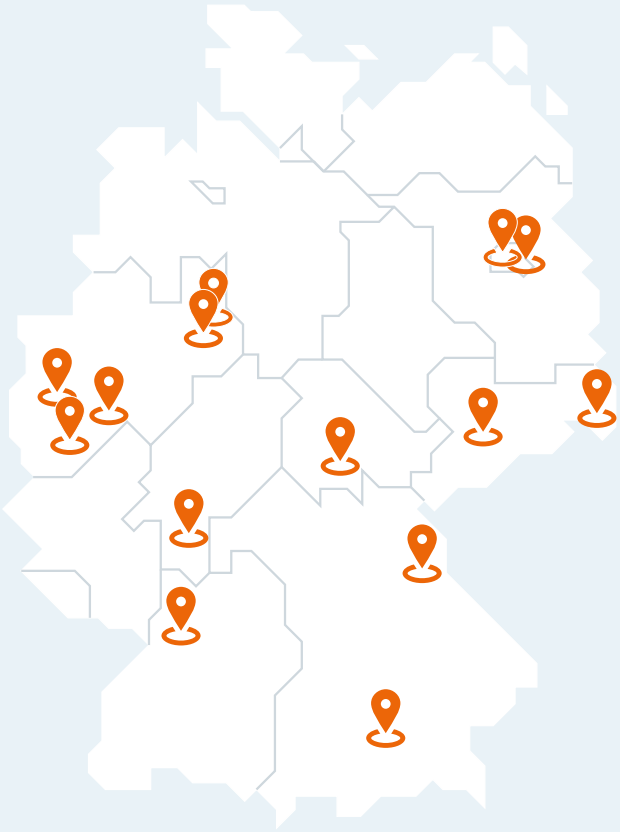
Aktuelle Qualifizierung aus der angewandten Forschung

Das Lernlabor Cybersicherheit ist ein Weiterbildungsprogramm, in dem Expertinnen und Experten von Fraunhofer und ausgewählten Fachhochschulen aktuellste Erkenntnisse auf dem Gebiet der Cybersicherheit vermitteln. Die Lehrmodule werden von den beteiligten Fraunhofer-Instituten und Fachhochschulen entwickelt und weitergegeben. Die Fraunhofer Academy ist die Geschäftsstelle und Plattform der Initiative, die Entwicklung, Vermarktung, Teilnehmermanagement und Qualitätssicherung koordiniert. Das Programm wird durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert.

Die beteiligten Partnerhochschulen

- Ostbayerische Technische Hochschule Amberg-Weiden
- Hochschule für Technik und Wirtschaft Berlin
- Hochschule Bonn-Rhein-Sieg
- Hochschule Mittweida
- Hochschule Niederrhein
- Technische Hochschule Ostwestfalen-Lippe
- Hochschule Zittau/Görlitz

Standorte der Lern- und Forschungslabore der beteiligten Fraunhofer-Institute und Fachhochschulen



Die beteiligten Fraunhofer-Institute

- Fraunhofer AISEC
- Fraunhofer FKIE
- Fraunhofer FOKUS
- Fraunhofer IEM
- Fraunhofer IOSB
- Fraunhofer IOSB-AST
- Fraunhofer IOSB-INA
- Fraunhofer SIT

Know-how schafft Sicherheit! Seit 5 Jahren unterstützen wir deshalb Unternehmen auf dem Weg zu mehr IT-Sicherheit.«

Dr. Raphaela Schätz,
Qualitäts- und Programm Management
im Lernlabor Cybersicherheit

Herausgeber

Fraunhofer Academy
Hansastraße 27c
80686 München

Telefon +49 89 1205-1555
Fax +49 89 1205-77-1599

cybersicherheit@fraunhofer.de
www.cybersicherheit.fraunhofer.de

Redaktion: Elly Leimenstoll

Layout und Satz, Illustrationen:
Vierthaler & Braun

Sie haben Fragen zum Angebot oder möchten sich zu Seminaren beraten lassen?

Melden Sie sich gerne
- telefonisch unter + 49 89 1205-1555
- per E-Mail: cybersicherheit@fraunhofer.de
- auf unserer Website unter

www.cybersicherheit.fraunhofer.de

Wir beraten Sie gerne, welche Weiterbildungen und Inhalte für Sie hilfreich sind.

Sie suchen nach Angeboten für Ihr Team?

Für Unternehmen bieten wir Inhouse-Schulungen und unternehmensspezifische Programme zur Qualifizierung und Kompetenzentwicklung. Wir erheben gemeinsam mit Ihnen den Kompetenzbedarf in Ihrer Abteilung oder Firma und beraten Sie, die richtigen Fähigkeiten in Ihrer Organisation aufzubauen.

Adem Salgin

Ihr Ansprechpartner im Lernlabor Cybersicherheit

Seminarberatung
und Anmeldung

Stand Juli 2022

Sie erreichen uns

– telefonisch unter +49 89 1205-1555
– per E-Mail: cybersicherheit@fraunhofer.de
– auf unserer Website unter

www.cybersicherheit.fraunhofer.de