Fraunhofer
AISEC

FRAUNHOFER-INSTITUT FÜR ANGEWANDTE UND INTEGRIERTE SICHERHEIT AISEC

JAHRESBERICHT
2018/2019

Aktuelle Informationen über das Fraunhofer AISEC finden Sie auf unserer Website **www.aisec.fraunhofer.de** oder auf unseren Social-Media-Kanälen:

Twitter www.twitter.com/FraunhoferAISEC

LinkedIn www.linkedin.com/company/fraunhoferAISEC

YouTube www.youtube.com/user/FraunhoferAISEC

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC

JAHRESBERICHT
2018/2019

Fraunhofer
AISEC

Sehr geehrte Damen und Herren,

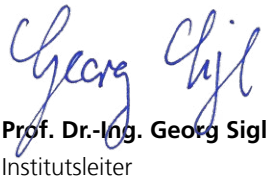
mit diesem Jahresbericht blicken wir nicht nur auf sehr erfolgreiche zwölf Monate zurück. 2018 konnten wir auch unser zehnjähriges Jubiläum als AISEC feiern.
Unsere Geschichte begann im Dezember 2008 als Projektgruppe des Fraunhofer SIT in Darmstadt – mit einem Fokus auf Kompetenzen, die weder unser damaliges Mutterhaus noch die Fraunhofer-Welt insgesamt abdeckte, für die aber ein großer Bedarf seitens der Industrie bestand: Embedded Security und Hardware-Sicherheit. Dieses Fundament haben wir im Laufe der Jahre stetig erweitert, nach den Bedürfnissen unserer Kunden, und technologische Entwicklungen vorwegnehmend. Einige der Themen, die die Sicherheitsdebatten von heute bestimmen, haben wir dabei besonders früh auf unsere Agenda gesetzt: Bereits 2009 forschte das AISEC intensiv im eigenen Cloud-Labor, seit 2014 beschäftigen wir uns mit dem Bereich Sicherheit für und durch Maschinelles Lernen, und auch im Themenfeld der Post-Quantum-Kryptografie gibt es schon seit einiger Zeit laufende Projekte.

Heute deckt das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit die gesamte Bandbreite der IT-Sicherheitsforschung ab – über den kompletten Technologiestack und mit einem breiten Spektrum an Methoden, das von Risikoanalysen über automatisierte Codeanalysen bis zu maschinellen Lernverfahren zur Verbesserung des Sicherheitsniveaus reicht. Domänen-Knowhow haben wir dabei vor allem in den technologiegetriebenen Schlüsselbranchen aufgebaut, wie zum Beispiel in der produzierenden Industrie, in der Automobilbranche und im Energiesektor.
Digitalisierung braucht Sicherheit. »Integrierte« Sicherheit bedeutet für uns, den Aspekt der Daten- und Informationssicherheit, der Cybersicherheit, nahtlos in die Konzeption von neuen Systemen und Anwendungen einzubringen und auch Bestandssysteme methodisch abzusichern. Deshalb suchen wir aktiv den Schulterschluss mit anderen Forschungsdisziplinen und -instituten. Hier haben wir im zurückliegenden Jahr viele wichtige Initiativen gestartet und mitgestaltet: Das Fraunhofer AISEC ist nicht nur Sprecherinstitut des Leistungszentrums Sichere Intelligente Systeme (LZSiS) in München, sondern hat auch die Sprecherrolle des zum 1. Januar 2018 neugeschaffenen Fraunhofer Clusters of Excellence Cognitive Internet Technologies (CCIT) inne.

»Mit Sicherheit innovativ« – so lautet unser Motto seit jeher. Dass unsere Ansätze hier die richtigen sind, zeigt die Auszeichnung »Innovator des Jahres«, die wir 2019 bereits zum zweiten Mal in Folge erhalten haben. Nicht nur unsere Erfolge aus 2018/2019, sondern der erfolgreiche Auf- und Ausbau des AISEC über die letzten zehn Jahre war und ist nur möglich dank des großartigen Engagements aller unserer Mitarbeiterinnen und Mitarbeiter und ihrer hohen Identifikation mit unseren Zielen. Dafür möchten wir uns als Institutsleiter an dieser Stelle herzlichst bedanken – und schließen hier unsere Alumni ausdrücklich mit ein. Bedanken möchten wir uns auch bei all unseren Partnern und Kunden, die im Laufe der Jahre großartige Projekte mit uns vorangetrieben haben. Ihr anhaltendes Vertrauen ist uns wichtig und verdeutlicht die hohe Relevanz unserer Forschung und unserer Vorentwicklungen. Auch weiterhin werden wir die Digitalisierung aktiv mitgestalten – zum Nutzen von Industrie und Wirtschaft und zum Wohle der Gesellschaft. Mit unserem Neubau, den wir im Herbst 2019 beziehen, wird uns dafür eine Infrastruktur zur Verfügung stehen, die unseren Handlungsraum signifikant erweitert.

Wir wünschen Ihnen eine angenehme Lektüre dieses Jahresberichts und freuen uns, wenn Sie unsere Aktivitäten auch in Zukunft mit Interesse begleiten.

Prof. Dr. Claudia Eckert
geschäftsführende Institutsleiterin



Prof. Dr.-Ing. Georg Sigl
Institutsleiter

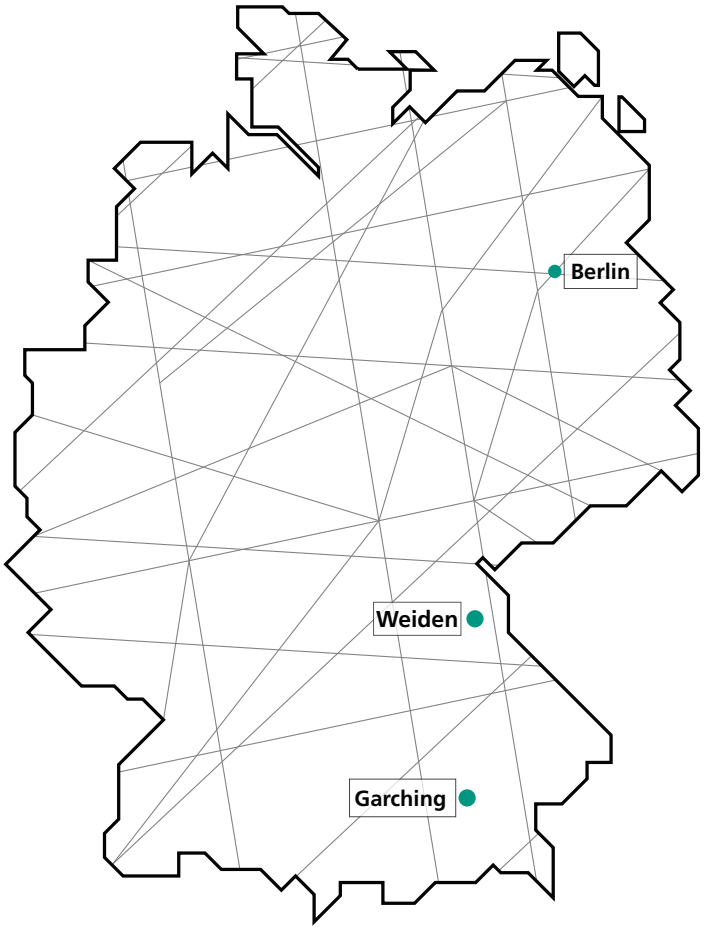
INHALTSVERZEICHNIS

Forschung und Innovation im Schulterschluss

Wissenschaftliche Beiträge und Outreach

Rund um das AISEC

STANDORTE UND ORGANISATIONSSTRUKTUR



Berlin

seit 2013, Kooperation mit der Freien Universität Berlin. Projekte zur Risikoanalyse und sicheren Software-Entwicklung.

Weiden in der Oberpfalz

seit 2016, Kooperation mit der Ostbayerischen Technischen Hochschule Amberg-Weiden. Lernlabor Cybersicherheit.

Garching bei München

seit 2009, Hauptstandort, Kooperation mit der Technischen Universität München. Umzug in den Neubau mit erweiterten Labor- und Testräumen im September 2019.

Spin-offs

SSE Secure Systems Engineering GmbH

Softwareengineering, Forschung und Beratung für ganzheitliche Informationssicherheit und Datenschutz
www.securesystems.de

Breakpoint GmbH

Hybride Analysetechniken: Vollautomatische, statische und/oder dynamische Analysen von mobilen Anwendungen (Apps) durch das Produkt App-Ray.
www.app-ray.co

Institutsleitung

Geschäftsführende Institutsleiterin	Prof. Dr. rer. nat. Dr. habil. Claudia Eckert
Institutsleiter	Prof. Dr.-Ing. Georg Sigl

Forschungsbereiche

Cognitive Security Technologies	Dr. rer. nat. Konstantin Böttinger
Hardware Security	Dr.-Ing. Johann Heyszl
Product Protection & Industrial Security	Bartol Filipovic
Service & Application Security	Dr. rer. nat. Julian Schütte
	Christian Banse
Secure Operating Systems	Sascha Wessel
Secure System Engineering	Prof. Dr. rer. nat. Marian Margraf

Innovationsgruppen

Physical Security Technologies	Dr.-Ing. Matthias Hiller
Secure Infrastructure	Prof. Dr. rer. nat. Daniel Loebenberger

Stabsbereiche

Administration	Ines Lenz
Public Relations und Marketing	Dr. phil. Barbara Eschlberger
Geschäftsstelle Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT	Margarete Hälker-Küsters
Infrastruktur und IT-Servicemanagement	Ingmar Schön
Gebäudemanagement	Christian Rasch

KOMPETENZEN UND KOOPERATIONSMÖGLICHKEITEN

Das Fraunhofer AISEC unterstützt Unternehmen aller Branchen und Dienstleistungssektoren darin, ihre Infrastrukturen, Produktionsanlagen, Geschäftsprozesse und Vertriebsnetze abzusichern und verlässlich zu betreiben. Im Spannungsfeld zwischen wirtschaftlichen Erfordernissen, Benutzerfreundlichkeit und Sicherheitsanforderungen verfolgen wir mit über 100 Mitarbeiterinnen und Mitarbeitern das Ziel, die Wettbewerbsfähigkeit unserer Kunden zu verbessern, indem wir in enger Zusammenarbeit innovative Produkte und Dienstleistungen konzipieren, gemeinsam umsetzen und das bestehende Portfolio unserer Kunden weiterentwickeln.

Unser Kompetenzfeld erstreckt sich von der integrierten Sicherheit eigebetteter Systeme und Hardware-Komponenten über Betriebssysteme, Applikationen (Apps) und Cloud-basierte Services bis hin zu Lösungen zur sicheren Software- und System-Entwicklung sowie zur Nutzung maschineller Lerntechniken für die Cybersicherheit. Dabei greifen wir auf ein umfassendes Knowhow im gesamten Spektrum des Technologie-Stacks zurück. Intensiv beschäftigen sich die Wissenschaftlerinnen und Wissenschaftler mit der Sicherheit von Industrieanlagen und Automotive-Systemen und den Herausforderungen unterschiedlichster Branchen wie im Energiebereich oder im öffentlichen Sektor.

UNSERE KOOPERATIONSMÖGLICHKEITEN IM ÜBERBLICK

- Im Rahmen von **industriellen Forschungsaufträgen** entwickeln unsere Expertinnen und Experten in enger Zusammenarbeit mit unseren Kunden Technologien, die exakt auf die Bedürfnisse des jeweiligen Kunden zugeschnitten sind – von Hardware und eingebetteten Softwaresystemen bis hin zu Services und Anwendungen.

- Das Fachwissen aus Wissenschaft und Technik sowie die herstellerneutrale Expertise machen das Fraunhofer AISEC zu einem idealen Partner im Bereich Sicherheit. Unsere **Sicherheits-Labors** sind mit modernster Technik ausgestattet, um im Auftrag unserer Kunden **technische Sicherheitsanalysen, Risiko-Assessments und Sicherheits-Test** durchzuführen und so die Sicherheit von Produkten, Hardware-Komponenten und Software zu bewerten und Systeme und Daten umfassend abzusichern.

- Mit der Durchführung von **Machbarkeitsstudien** unterstützen wir Unternehmen bei der Absicherung ihrer Investitionen und entwickeln gemeinsam individuelle Lösungen zum Schutz vor Wirtschaftskriminalität, Wirtschaftsspionage und Datenverlust.

- Die **Technologie- und Compliance-Beratung** am Fraunhofer AISEC erstreckt sich über alle Bereiche der IT-Sicherheit, vom ersten Orientierungsgespräch hin zum prozessoptimierten Technologietransfer.

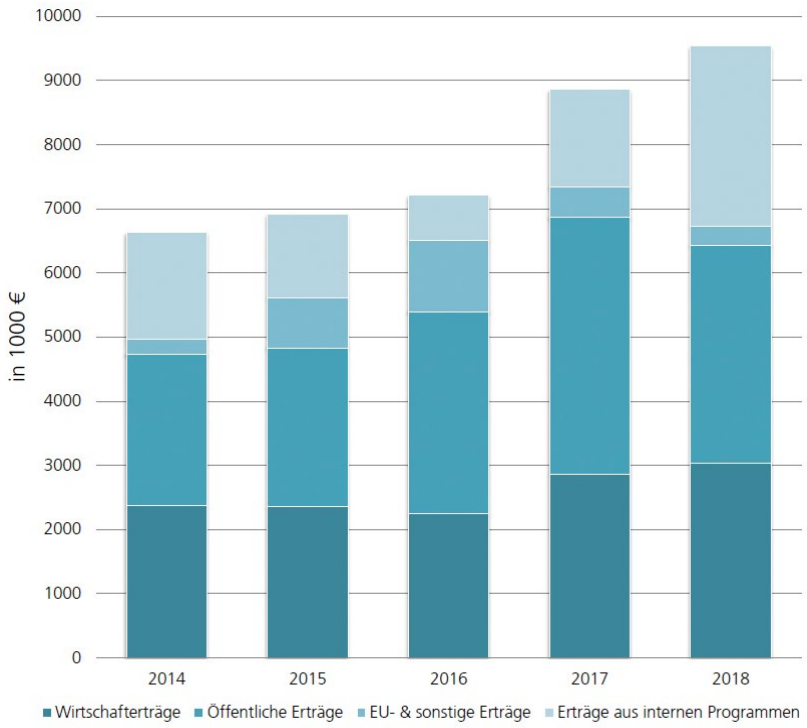
- Die industrienahe Ausrichtung unserer Forschung ermöglicht es uns, Fragestellungen mit gesellschaftlicher und gesamtwirtschaftlicher Relevanz schnell zu identifizieren und unsere Kunden bei der Durchführung von **Studien und Untersuchungen** zu aktuellen Themen zielgerichtet zu unterstützen.

- Häufig arbeiten wir mit unseren Kunden in **öffentlich geförderten Vorlaufprojekten** zusammen. In diesen nationalen und internationalen Forschungsvorhaben erarbeiten wir gemeinsam mit Unternehmen und anderen Forschungseinrichtungen Lösungen für aktuelle Herausforderungen in den verschiedensten Wirtschaftszweigen. Durch die **interdisziplinäre Zusammenarbeit** können die Kooperationspartner vom fachspezifischen Expertenwissen des Fraunhofer AISEC profitieren.

- Um die gewonnenen Erkenntnisse weiterzugeben, bietet das Fraunhofer AISEC im Rahmen des **Lernlabors Cybersicherheit** Schulungen mit den Schwerpunkten Embedded Systems, Mobile Security, Internet oft Things und weiteren Themen an. Der Fokus liegt auf der anwendungsorientierten Weiterbildung durch modulare und bedarfsorientierte Konzepte auf neuestem Stand der Forschung und in modernen Laborumgebungen.

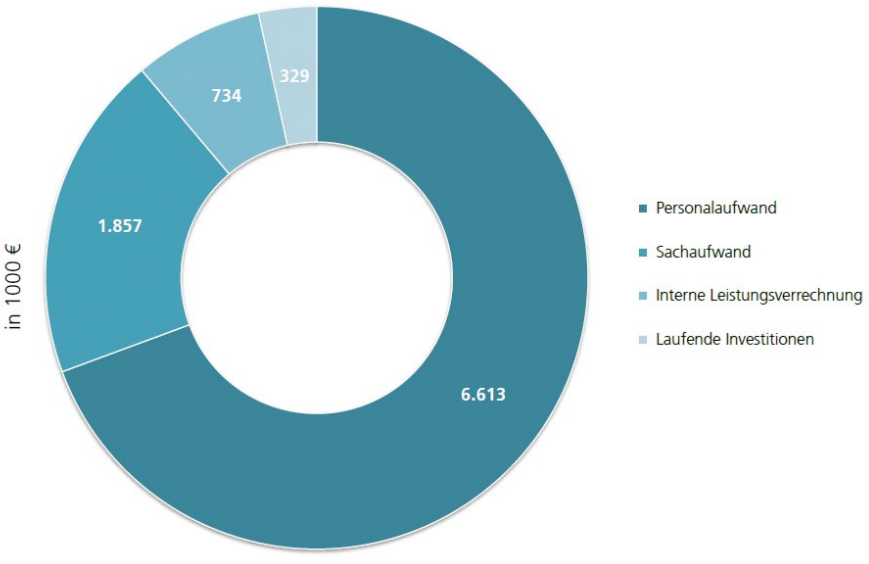
AUFWAND UND ERTRÄGE

NACHHALTIGES WIRTSCHAFTLICHES WACHSTUM



Das Fraunhofer AISEC verzeichnet eine steigend hohe Nachfrage seitens der Industrie. Im Jahr 2018 wurden Wirtschaftserträge in Höhe von rund 3 Mio € erzielt, was eine Fortsetzung der positiven Entwicklung der Vorjahre (rund 2,3 Mio € in 2016, 2,8 Mio € in 2017) bedeutet. In allen Bilanzen unserer Geschichte als eigenständiges Institut belaufen sich die Wirtschaftserträge auf über 30 Prozent des gesamten Betriebsaufwandes. 2019 werden sie bei über 36 Prozent liegen.
Zu einem gesunden nachhaltigen Wachstum gehört auch die intensive marktorientierte Vorlaufforschung. Diese spiegelt sich in den öffentlichen Erträgen wider. Der hohe Anstieg der Erträge aus internen Programmen auf 2,8 Mio € in 2018 ist das Ergebnis unserer intensiven Beteiligung an institutsübergreifenden Initiativen wie dem Leistungszentrum Sichere intelligente Systeme und dem Cluster of Excellence Cognitive Internet Technologies.

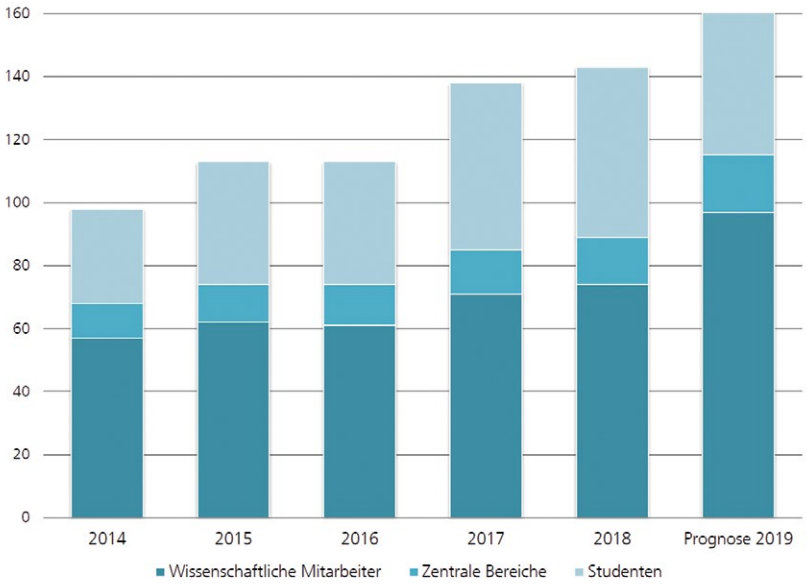
GESAMTAUSGABEN 2018



Summe Gesamtausgaben: 9,533 Mio €

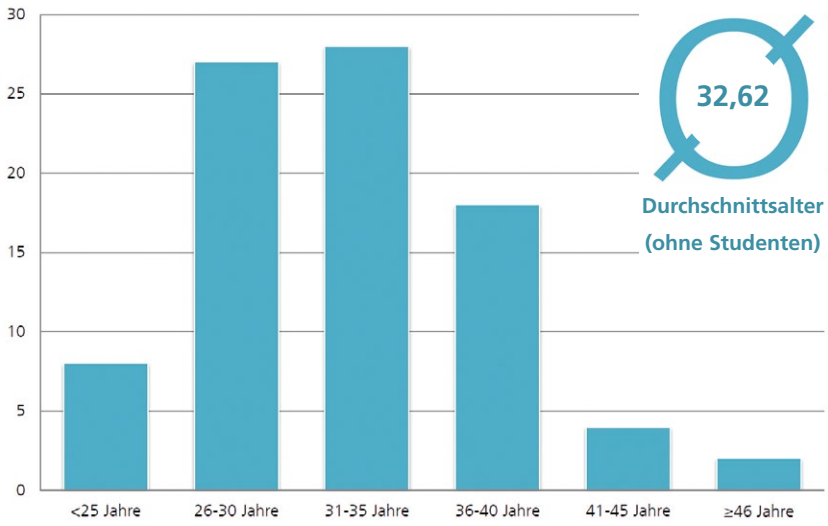
PERSONAL

GESUNDER ORGANISCHER AUFWUCHS TROTZ FACHKRÄFTEMANGEL

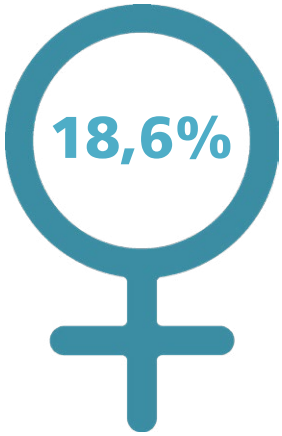


Ende des Jahres 2018 konnte das AISEC insgesamt 143 Mitarbeitende verzeichnen, wobei knapp 10 Prozent dem technischen und administrativen Bereichen zuzuordnen sind. Im wissenschaftlichen Bereich kommen zu 74 fest angestellten Wissenschaftlern 54 Studenten. Vor allem im wissenschaftlichen Bereich kündigt sich für 2019 ein signifikantes Wachstum an, obwohl die Personalgewinnung in der IT-Branche allgemein als neuralgisches Thema beschrieben wird.
Die AISEC-Belegschaft ist ein junges Team: Das Durchschnittsalter betrug im Jahr 2018 ohne Studenten 32,9 Jahre. Die Mehrheit der Forschenden ist damit deutlich unter 40 Jahre alt. 18,6 Prozent der Mitarbeitenden sind weiblich, damit liegt der Frauenanteil am AISEC über dem branchenspezifischen Durchschnitt.

EIN JUNGES TEAM: ALTERSVERTEILUNG 2018



HOHER FRAUENANTEIL



UNSER KURATORIUM

Das Kuratorium berät das Fraunhofer AISEC in Fragen der inhaltlichen Ausrichtung und strategischen Weiterentwicklung. Die Mitglieder werden vom Vorstand der Fraunhofer-Gesellschaft im Einvernehmen mit der Institutsleitung berufen. Dem Kuratorium des Fraunhofer AISEC gehören Persönlichkeiten aus Wirtschaft, Wissenschaft und Öffentlicher Hand an. Ihnen ist gemeinsam, dass sie sich in ihrer täglichen Arbeit auf unterschiedliche Art und Weise mit dem Thema IT-Sicherheit beschäftigen. Sie sind nah am Geschehen – politisch wie wirtschaftlich. Dies macht ihren Rat so wertvoll.

Derzeit besteht das Kuratorium des Fraunhofer AISEC aus:

Prof. Dr. Udo Helmbrecht (Vorsitzender)

Geschäftsführer der »European Union Agency for Cybersecurity (ENISA)«, seit 2010 Honorarprofessor der Universität der Bundeswehr München

Prof. Dr.-Ing. Georg Carle

Lehrstuhl für Netzarchitekturen und Netzdienste, Fakultät für Informatik der Technischen Universität München

Abdou Naby Diaw

Chief Information Security Officer und Vice President der Deutsche Lufthansa AG

Horst Flätgen

Ministerialdirigent des Bundesministeriums der Finanzen (IT-Steuerung in der Bundesfinanzverwaltung; Dienstleistungen)

Dr.-Ing. Stefan Hofschen

Vorsitzender der Geschäftsführung der Bundesdruckerei GmbH

Prof. Dipl.-Kfm. Dieter Kempf

Präsident des Bundesverbands der Deutschen Industrie (BDI)

Andreas Könen

Abteilungsleiter CI »Cyber- und IT-Sicherheit« im Bundesministerium des Inneren, für Bau und Heimat

Dr. Manfred Paeschke

Chief Visionary Officer der Bundesdruckerei GmbH

Dr.-Ing. Heike Prasse

Leiterin des Referats »Kommunikation und Sicherheit digitaler Systeme« im Bundesministerium für Bildung und Forschung

Thomas Rosteck

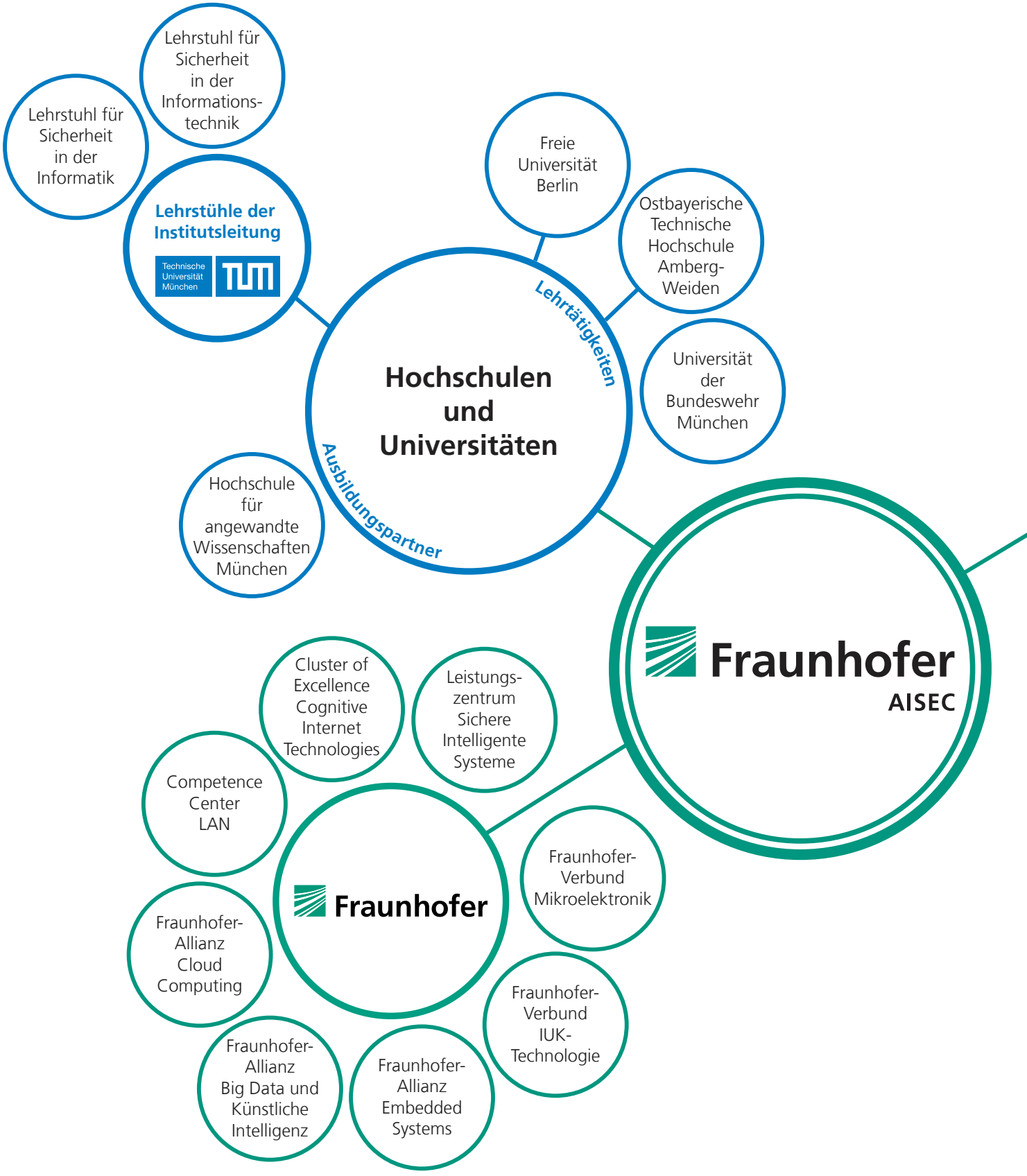
Division President Chip Card & Security bei Infineon Technologies AG

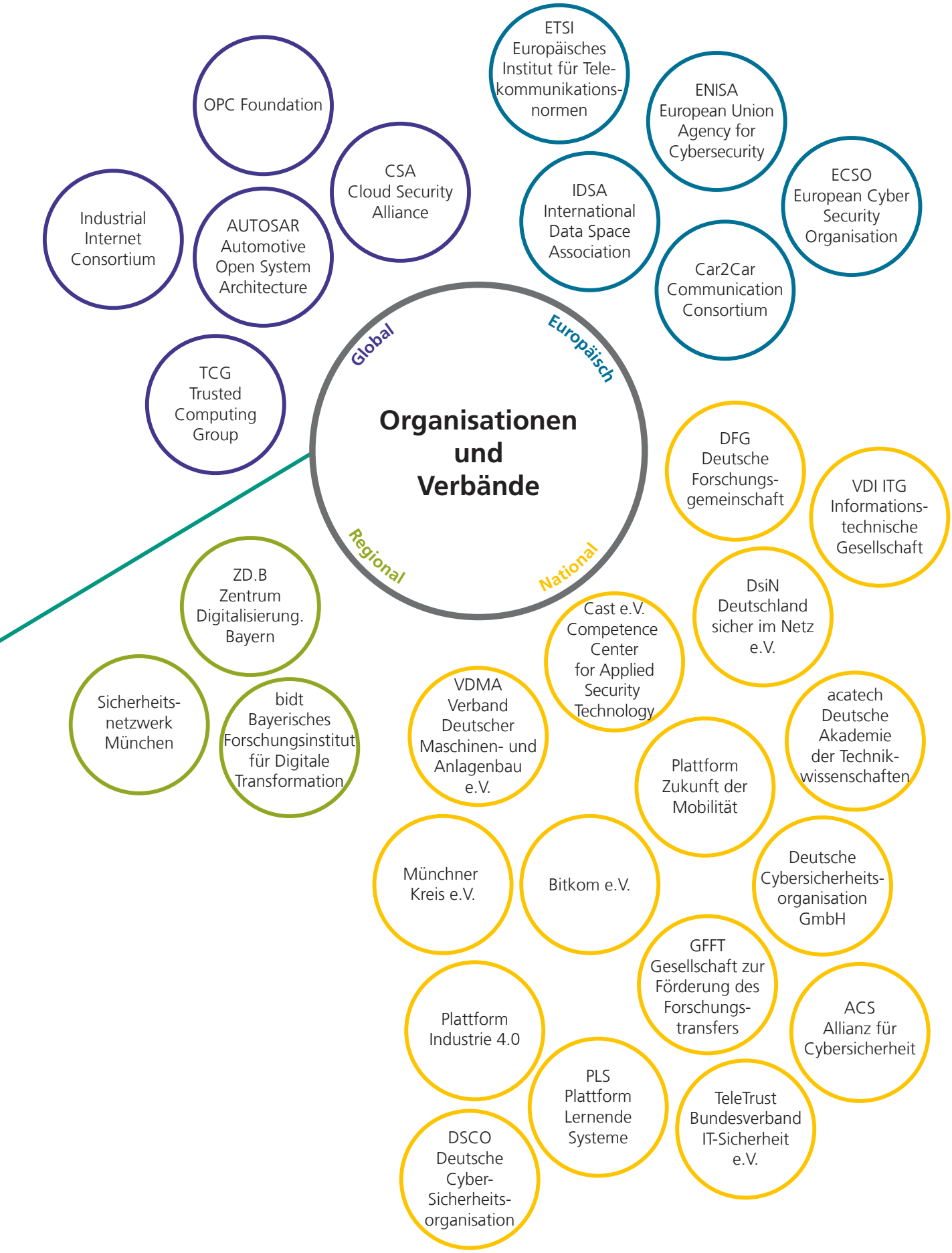
Dr. Stefan Wimbauer

Referatsleiter »Angewandte Forschung, Cluster-Politik« im Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie

BEI ALLEN EHEMALIGEN UND DERZEITIGEN KURATOREN MÖCHTEN WIR UNS HERZLICH FÜR DIE WERTVOLLE BEGLEITUNG UND DIE KONSTRUKTIVE UNTERSTÜTZUNG BEDANKEN.

UNSER NETZWERK




Organisationen und Verbände
Global
Europäisch
National
Regional
OPC Foundation
ETSI Europäisches Institut für Telekommunikationsnormen
ENISA European Union Agency for Cybersecurity
ECSO European Cyber Security Organisation
CSA Cloud Security Alliance
IDSA International Data Space Association
Car2Car Communication Consortium
Industrial Internet Consortium
AUTOSAR Automotive Open System Architecture
TCG Trusted Computing Group
DFG Deutsche Forschungsgemeinschaft
VDI ITG Informationstechnische Gesellschaft
DsiN Deutschland sicher im Netz e.V.
Cast e.V. Competence Center for Applied Security Technology
ZD.B Zentrum Digitalisierung. Bayern
Sicherheitsnetzwerk München
bidt Bayerisches Forschungsinstitut für Digitale Transformation
VDMA Verband Deutscher Maschinen- und Anlagenbau e.V.
acatech Deutsche Akademie der Technikwissenschaften
Plattform Zukunft der Mobilität
Münchner Kreis e.V.
Bitkom e.V.
Deutsche Cybersicherheitsorganisation GmbH
GFFT Gesellschaft zur Förderung des Forschungstransfers
Plattform Industrie 4.0
ACS Allianz für Cybersicherheit
PLS Plattform Lernende Systeme
TeleTrust Bundesverband IT-Sicherheit e.V.
DSCO Deutsche Cyber-Sicherheitsorganisation

… Digitalisierung

Unter »Digitalisierung« versteht man gemeinhin den Prozess der Umwandlung analoger Werte in digital verarbeitbare Formate. Die Digitalisierung ist nichts Neues, jedoch ist durch die rasante Entwicklung der digitalen Technologien in den letzten Jahren ein umfassender wirtschaftlicher und gesellschaftlicher Prozess in Gang gekommen: die Digitale Transformation. Treiber dieses Prozesses sind digitale Technologien, wie die drahtlose und mobile Vernetzung bis hin zum neuen Mobilfunkstandard 5G, das Internet der Dinge (IoT), das auf dieser Basis entstanden ist, das Vordringen mobiler Anwendungen (Apps) und mobiler Endgeräte in alle Bereichen des beruflichen und privaten Alltags, oder auch neue Verarbeitungsinfrastrukturen, wie Cloud- und Edge-Computing. Die mit der digitalen Transformation verbundene durchgehende Vernetzung von Maschinen und Produkten, aber auch von Logistikabläufen, Bestell-, Lager- und Rechnungswesen führt zu Systemen von nur schwer beherrschbarer Komplexität. Cybersicherheit stellt hier eine große Herausforderung dar, weil einerseits neue Lösungen und Komponenten Einzug in Produktion und Automatisierungsprozesse halten und gleichzeitig eine Vielzahl neuer Verwundbarkeiten entstehen, deren Schadenspotenzial mit dem Vernetzungsgrad zunimmt. In den komplexen Systemen von heute und morgen werden dringend neue und verbesserte Lösungen zur Gewährleistung der Daten- und Informationssicherheit benötigt. Ganz gleich, was die digitale Transformation mit sich bringt: Ohne Cybersicherheit wird sie nicht gelingen.

… Cybersicherheit

»Cybersicherheit« klingt nach einem trendigen Marketingwort, setzt sich allerdings mehr und mehr auch im deutschen Sprachgebrauch als Begriff durch. Dieser steht für die Konvergenz von realer und virtueller, IT-getriebener Welt und den damit einhergehenden Herausforderungen an die IT-Sicherheit. Das übergeordnete Ziel aller Maßnahmen zur Herstellung von Cybersicherheit (Security) ist es, Systeme, Komponenten und Daten zu schützen. Die drei zentralen Schutzziele sind die Gewährleistung der Daten- und Systemintegrität, also der Schutz vor unbefugter Manipulation, die Gewährleistung der Vertraulichkeit und die Gewährleistung der Verfügbarkeit von Funktionen und Diensten. Diese Ziele werden bereits in der klassischen IT-Sicherheit verfolgt, gewinnen aber durch die Verbindung von digitaler und physischer Welt zunehmend an Bedeutung. Dass Cybersicherheit eine physische, also eine der echten Welt angehörende Komponente besitzt, ist ein wichtiger Aspekt, der in Zukunft für das Sicherheitsbewusstsein eine große Rolle spielen wird.

… Kognitive Internettechnologien

Nicht nur die Cybersicherheit ist entscheidend für das Gelingen der digitalen Transformation. Weitere grundlegende Voraussetzungen müssen erfüllt sein, um das volle Potenzial von Vernetzung, Industrie 4.0 und Internet of Things auszuschöpfen. Dabei geht es nicht nur um Bandbreite, auch wenn das in manchen Regionen noch höchste Priorität hat. Darüber steht die Frage, ob die Industrie mit dem heutigen, webbasierten Internet den Weg in eine neue digitalisierte Zukunft antreten und dabei gleichzeitig wettbewerbsfähig bleiben kann. Für die Anforderungen des globalen Wettbewerbs an zuverlässige, flexible, industriell gefertigte Produkte, Dienstleistungen und Anlagen ist das »herkömmliche Internet« als Basis unzureichend. Die Industrie braucht neue Internet-Technologien – Schlüsseltechnologien von einer neuen Sensorgeneration mit integrierten KI-Verfahren zur Datenverarbeitung »at the Edge« bis hin zu vertrauenswürdigen, intelligenten Datenräumen – um neue Geschäftsmodelle und Wertschöpfungsprozesse zu entwickeln. Nur wenn diese kognitiven Technologien vertrauenswürdig sind und in nicht manipulierbaren Umgebungen ausgeführt werden, können sie die Basis für die Erbringung hochintelligenter, lernender Prozesse und Dienstleistungen, ein »kognitives Internet» bilden, das auf die Bedarfe und Anforderungen der Industrie der Zukunft zugeschnitten ist. Das damit verbundene Werteversprechen der integrierten Sicherheit ist ein Schlüsselthema für die Zukunft.

… Digitale Identitäten

Die Grenzen zwischen digitaler und physikalischer Welt werden durch die Digitale Transformation und die zunehmende Vernetzung immer weiter verschwimmen.

PROF. DR. CLAUDIA ECKERT ÜBER

IT-Sicherheit im Wandel

Um Systeme und Komponenten dennoch vor Manipulationen zu schützen, gewinnt die eindeutige Identifizierbarkeit mittels digitaler Identitäten weiter an Bedeutung. Insbesondere bei der Vernetzung von Cyber-physischen Systemen, bei denen Daten unternehmensübergreifend ausgetauscht werden, ist es immer wichtiger, Menschen, Maschinen und Prozesse auch über Unternehmensgrenzen hinweg eindeutig zu kennzeichnen. Damit gewinnt auch die digitale Abbildung von rechtlich relevanten Transaktionen zunehmend an Bedeutung, beispielsweise bei Bestellprozessen, bei denen die Zuordnung von Aktionen eine ebenso wichtige Rolle spielt wie die Frage der Rechtzeitigkeit, Vollständigkeit und Korrektheit.
Digitale Identitäten sind die Basis für digitale Souveränität. Für eine kontrollierte Weitergabe von Daten und deren Nutzung brauchen wir zusätzliche technologische Lösungen, um jederzeit Nachweise zur Compliance führen zu können, und vertrauenswürdige Plattformen wie den Industrial Data Space für datenschutzkonforme, datensouveräne Kollaboration.

… Sicherheitsforschung

Die digitale Transformation fordert neue Technologien für die Schutzziele Integrität, Vertraulichkeit und Verfügbarkeit. Nicht zu unterschätzen sind jedoch auch die Gefährdungen, die mit neuer Informationstechnologie einhergehen. Ob man nun Alexa zu sich ins Wohnzimmer einlädt oder Produktionsabläufe automatisiert – immer werden damit Cyber-Kriminellen Tür und Tor geöffnet. Deswegen ist es im Bereich der Sicherheitsforschung wichtig, sowohl ganzheitliche Sicherheitskonzepte zu untersuchen, als auch dedizierte Lösungen für einzelne Komponenten zu entwickeln – sei es eine Hardware-Komponente abzusichern, eine App zu härten oder die Integrität eines vernetzten IT-Systems beim Einsatz in der Produktion zu gewährleisten. Nur durch die Kombination von Schutzmaßnahmen, die auf unterschiedliche Anforderungen zugeschnitten sind und durch die differenziert kontrollierbare Schutzzonen errichtet werden, kann die Ausbreitung von Schäden eingedämmt werden. Auch unsichere Systembestandteile können durch eine Einbettung in einen Sicher- heitskontext kompensiert werden. Dadurch lassen sich mögliche Einfallstore schnell entdecken und beheben. Eine systematische Integration von Sicherheitsmaßnahmen in alle Phasen eines Systemlebenszyklus, also vom Design über die Inbetriebnahme, den laufenden Betrieb mit u. a. sicheren Update-Mechanismen bis hin zum sicheren Löschen und Entsorgen von Komponenten, kann künftige IT-Systeme absichern – sowohl proaktiv und vorausschauend durch intelligente Analysen, als auch reaktiv durch agile Sicherheitsarchitekturen, die sich automatisch der dynamischen Bedrohungslage anpassen. Es ist eine zentrale Aufgabe der IT-Sicherheitsforschung, die mit neuen Technologien, wie z. B. Quanten-Computern, einhergehenden möglichen neuen Bedrohungen frühzeitig zu identifizieren, dafür geeignete Sicherheitslösungen zu entwickeln und agile und beherrschbare Sicherheits-Architekturen bereitzustellen. Im Voraus-Denken liegt der Wert der Forschung. Sie schafft die Grundlage für eine aktive Gestaltung der Zukunft.

PROF. DR.-ING. GEORG SIGL ÜBER

Herausforderungen 2018/2019

… Verschmelzung von Hardware- und Software

Maßnahmen zum Hard- und Software-Schutz zur Erhöhung der Sicherheit elektronischer und digitaler Geräte und Komponenten gehören seit Jahren zum Lösungsangebot des Fraunhofer AISEC. Entwickelt werden individualisierte und maßgeschneiderte Lösungen für unterschiedliche Branchen und Produkte. Dabei handelt es sich beispielweise um eingebettete Systeme im industriellen Maschinen- und Anlagenbau, um eingebettete Hard- und Software-Komponenten in industriellen Steuerungen, im Automobil oder Avionics-Bereich, aber auch um IoT-Komponenten in der Heimautomatisierung oder im Gesundheitssektor. Gerade bei eingebetteten Systemen ist die Kombination aus Hardware und Software Security der Schlüssel für ein hohes Sicherheitslevel. Die leicht zugänglichen Komponenten wie Chips oder interne Schnittstellen sind für Angreifer mit dem richtigen Wissen und Kowhow oft leichte Ziele. Aus diesem Grund ist es unerlässlich, von Beginn an einen hohen Grad an Hardware-Sicherheit solcher Systeme anzustreben. Schwerpunkte am AISEC liegen in der Entwicklung von sicheren System-on-Chip-Lösungen, der Absicherung von eingebetteter Software gegen Manipulationen oder aber auch der Gewährleistung.

Das Fraunhofer AISEC entwickelt gehärtete eingebettete Systeme, in denen Software-Sicherheitsmechanismen durch geeignete Hardwarefunktionen ergänzt werden. Dabei bieten wir eine enge Abstimmung von Hardware- und Softwareentwicklung, wie auch die notwendige Verlagerung von wichtigen Funktionen in die Hardware. Für eingebettete Systeme konzeptioniert, entwickelt und bewertet das Fraunhofer AISEC Lösungen nach maßgeschneiderten Kriterien wie Energieaufwand, Rechenleistung und Datenübertragungsaufwand. Diese maßgeschneiderten Lösungen reichen von der sicheren Integration und Anbindung von zusätzlichen Hardware-Sicherheitsbausteinen (Secure Elements) bis zur Entwicklung von maßgeschneiderten Sicherheitslösungen in Hard- und Software, die spezifische Anforderungen unserer Kunden umsetzen. Dabei arbeiten die Bereiche Embedded Security und Hardware Security eng zusammen.

… Meltdown und Spectre

»Spectre« bezeichnet als Begriff nicht nur die Sicherheitslücke in Mikroprozessen, sondern erinnert den einen oder anderen Comic-Fan an das Schreckensgespenst aus dem DC Universum. Nicht zu vergessen natürlich die gegnerische Terrororganisation von James Bond im gleichnamigen 007-Film. Der Begriff »Meltdown« bezeichnet eigentlich eine Kernschmelze und ist außerdem der Titel eines US-amerikanischen Katastrophenfilms aus dem Jahr 2006.

Man merkt also schnell: Die Namen der Sicherheitslücken, die im Januar 2018 bekannt wurden und Milliarden verbauter Prozessoren betrafen, wurden nicht zufällig gewählt, sondern verdeutlichen das Ausmaß der Auswirkungen.
Was ist passiert? Um Prozessoren schneller arbeiten zu lassen, entwickelten Ingenieure die »Speculative Execution«, also die vorausschauende Berechnung und Speicherung von Daten, bevor diese von installierten Programmen benötigt werden.

Und genau diesen Zwischenspeicherzustand konnten Cyberkriminelle missbrauchen, um Daten abzuschöpfen.

Beunruhigend war vor allem die Zahl der betroffenen Prozessoren in Smartphones, Tablets und Computern, und zwar unabhängig vom jeweiligen Betriebssystem: Hunderte Millionen Nutzer waren betroffen. Dies zeigt deutlich, dass kein System vor Sicherheitslücken verschont bleibt. Umso wichtiger ist es, dass sich Unternehmen mit aktuellen Bedrohungen auseinandersetzen und ihre Systeme auf den Worst-Case vorbereiten, denn Cyber-Kriminelle werden immer neue Lücken suchen, um Unternehmen und Privatpersonen Schaden zuzufügen.

… Physical Unclonable Functions

Fertigungsschwankungen sind eigentlich ein unerwünschter, aber unvermeidlicher Effekt in industriellen Prozessen. »Physical Unclonable Functions« (PUFs) nutzen genau diese Schwankungen, um einzigartige Muster für jedes Gerät abzuleiten – ganz ähnlich einem menschlichen Fingerabdruck. In einem nächsten Schritt wird dieser einzigartige, aber verrauschte Fingerabdruck durch Nachbearbeitungs- und Fehlerkorrekturcodes in einen stabilen kryptographischen Schlüssel verwandelt. Am Fraunhofer AISEC untersuchen wir verschiedene Aspekte von PUFs, angefangen bei den Grundfunktionen von PUFs in integrierten Schaltungen und FPGAs bis hin zu kundenspezifischen Folien und deren Messschaltungen zur Herstellung von manipulationssicheren Hüllen.

Die Algorithmen der Schlüsselgenerierung werden für den jeweiligen Anwendungsfall individuell angepasst, außerdem integrieren wir verschiedene Faktoren, um PUF-basierte Schlüsselspeicher und Manipulationsschutz für komplette eingebettete Systeme zu entwickeln. Zusätzlich werden entsprechende Testwerkzeuge entwickelt, um die Qualität der PUFs zu beurteilen. Unsere Testeinrichtungen und das großflächige FPGA-Array ermöglichen es beispielsweise, PUFs verschiedenen Temperaturbedingungen auszusetzen, um ihre praktische Zuverlässigkeit zu bewerten.

… Quantenkryptografie

Quantenkommunikation, Quanteninternet – das sind alles sehr große Worte, doch basieren sie auf dem gleichen Prinzip: Quantenkryptografie oder auch Quantenschlüsselaustausch nutzt physikalische Prinzipen der Quantenmechanik, anstatt auf mathematischen Annahmen zu beruhen. Warum wir Quantenkryptografie als so sicher empfinden? Das liegt in der Natur der Sache – Security by Nature sozusagen. Botschaften werden in einer Abfolge von einzelnen Lichtquanten codiert. Danach garantiert Heisenbergs Unschärferelation Sicherheit, denn jeder Versuch, Quanten zu messen und abzufangen, ändert ihr Verhalten. Und diese Veränderung wäre für Sender und Empfänger sofort sichtbar.

Am Fraunhofer AISEC gehen wir noch einen Schritt weiter und befassen uns derzeit mit der Post-Quantenkryptografie. Also mit Sicherheitsaspekten, die sich aus der zukünftigen Interaktion von klassischen und quantenbasierten Systemen befasst. Immerhin ist es vorstellbar, dass in naher Zukunft Quantencomputer gebaut werden, die tatsächlich zum Einsatz kommen. Deswegen erforschen wir kryptografische Verfahren, die auch vor Angriffen mit Quantencomputern sicher sind.

THEMA HARDWARE SECURITY

Hardware-Komponenten sind physisch leicht zugänglich, dennoch werden sie in der IT-Sicherheit häufig vernachlässigt. Dabei können sich Angreifer, die über die entsprechenden Kompetenzen in den Bereichen Elektronik, Nachrichtentechnik und Hardware-Angriffen verfügen, durch interne Schnittstellen relativ leicht direkten Zugang zu integrierten Speicherchips verschaffen und Daten auslesen. Aus diesem Grund ist es besonders wichtig, Hardware-Sicherheit von Anfang an einen hohen Stellenwert einzuräumen und sich mit der Absicherung elektronischer Hardware wie Chips und eingebetteten Systemen auseinanderzusetzen. Das Fraunhofer AISEC entwickelt Lösungen, die Komponenten und Systeme gegen Angriffe schützen, die Schwachstellen in der Hardware ausnutzen.

Neue Wege zum Schutz vor Seitenkanalangriffen

Sogenannte Seitenkanalangriffe nutzen Informationen zur Laufzeit, zum Stromverbrauch oder zur elektromagnetischen Emission, um kryptografische Systeme zu untergraben. In modernen Prozessoren sind es vor allem die vielen Geschwindigkeitsoptimierungen, die zu angreifbaren Laufzeitunterschieden führen.

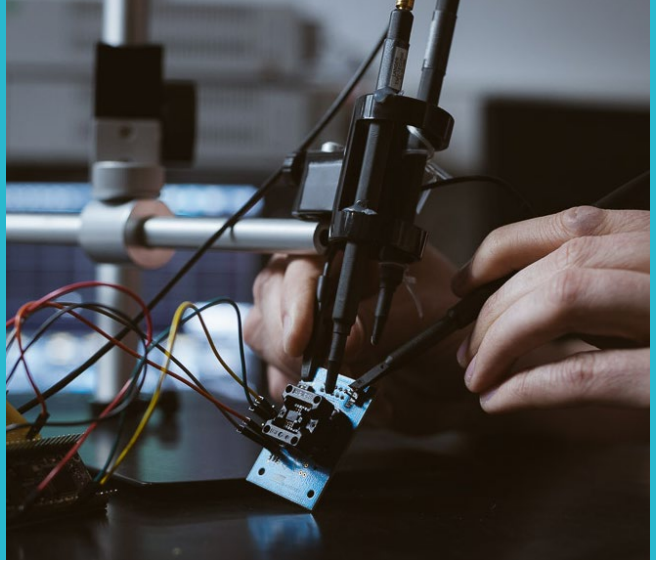
Forscherinnen und Forscher am Fraunhofer AISEC und der TU Graz konnten im August 2018 auf dem USENIX Security Symposium in Baltimore ein neues Werkzeug präsentieren, das im Rahmen des Projekts Bayern Digital entwickelt wurde: »DATA« (Differential Address Trace Analysis) ist ein differentielles Framework, das automatisiert Schwachstellen in kryptografischen Software-Libriaries findet, die geheime Informationen über Prozessorseitenkanäle offenbaren. Dafür arbeitet DATA in drei Phasen. In einem ersten Schritt wird das zu prüfende Programm ausgeführt, um mehrere Zugriffssequenzen von Speicheradressen aufzuzeichnen. Diese Spuren werden mit einem neuartigen Algorithmus analysiert, der sie dynamisch neu ausrichtet, um die Erkennungsgenauigkeit zu erhöhen. Anschließend filtert ein generischer Leakage-Test Unterschiede, die durch statistisch unabhängiges Programmverhalten, wie beispielsweise Randomisierung, verursacht werden, und deckt konkrete Informationslecks auf. Die dritte Phase klassifiziert diese Lecks nach den Informationen, die aus ihnen gewonnen werden können. Damit können Entwickler – auch ohne fundiertes Expertenwissen – zielgerichtete Bedrohungsanalysen ihrer Programme durchführen und somit die Codequalität verbessern.

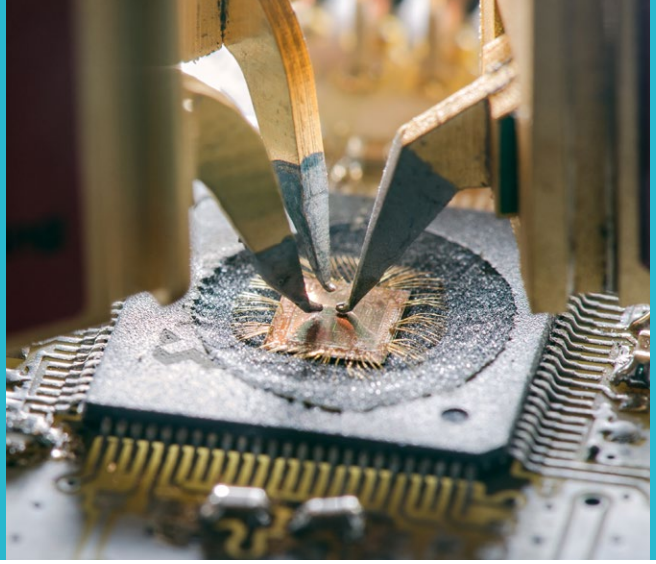
In einem Fraunhofer-MAVO-Projekt arbeitet das Fraunhofer AISEC gemeinsam mit den Partnerinstituten Fraunhofer IPMS, Fraunhofer FHR und Fraunhofer IMS an einem RFID-Chip, der in dem bisher undenkbaren Frequenzbereich von 66 GHz arbeitet und über eine hoch-effiziente kryptografische Implementierung fortschrittliche kryptografische Konzepte zur Härtung gegen Seitenkanalangriffe enthält. Eine erste Version des Readers inklusive Transceiver-Chip konnte bereits realisiert werden, eine Demonstration des Gesamtsystems ist für Ende 2019 geplant.

Unkomplizierter Schutz für Sensornetzwerke

Sensoren, wie sie in der Landwirtschaft, im Healthcare-Bereich oder im industriellen Umfeld eingesetzt werden, sind häufig leicht zugänglich und durch ihre geringe Rechenleistung oft auch nicht umfassend geschützt. Die »FunkeyBox« des Fraunhofer AISEC bietet die Möglichkeit, Firmware einfach und schnell auf viele Sensorknoten zu übertragen – und ist damit eine Alternative zu kabelgebundenen, administrativ aufwändigen Übertragungsverfahren. Hierfür werden im Backend die Firmware und eine Reihe von Schlüsseln erzeugt und über eine Kabelverbindung an die FunkeyBox übertragen. Im Inneren der Box wird jede Firmware mit einem eigenen Schlüssel versehen und via Funkkanal an die Sensorknoten übertragen. Somit erhält jeder Sensorknoten einen eigenen Schlüssel – Messwerte können fortan verschlüsselt an das Backend gesendet werden. Die Vorteile zeigen sich insbesondere im Einsatz vieler Sensorknoten: die Firmware- und Schlüsselverteilung erfolgt ohne zusätzliche Hardware auf beliebig viele Sensorknoten gleichzeitig.

Ein weiteres Projekt, das die Überwachung von Sensor-Netzwerken ohne umfassende Security-Expertise ermöglicht, ist





das Monitoring-Tool »EyeSec«, mit dem Wireless Sensor Networks (WSNs) überwacht, und Datenströme und Fehlfunktionen im System visualisiert werden können. EyeSec basiert auf drei zentralen Bestandteilen: Via Software-Defined Radio (SDR) werden die Informationen, die von den Sensoren über Funkverbindungen an das Backend übermittelt werden, mitgeschnitten. Der Vorteil dieser passiven Beobachtung liegt darin, dass das WSN in seiner Funktion nicht beeinflusst wird. Die erhobenen Datenströme und Informationen werden im EyeSec-Backend gesammelt und nach vorher definierten Mustern ausgewertet. Im Anschluss werden die Daten an die EyeSec-App übermittelt. Sie visualisiert die Datenströme mit Augmented Reality – und ermöglicht es dem Systemtechniker so, die Funktionsfähigkeit der einzelnen Sensoren zu überprüfen und entsprechende Maßnahmen einzuleiten. Der zentrale Vorteil liegt darin, dass der Techniker selbst kein fundiertes Fachwissen mehr braucht, um die Datenströme zu interpretieren und selbst Anomalien zu erkennen. EyeSec wurde 2019 auf der International Conference on Embedded Wireless Systems and Networks (EWSN) in Peking vorgestellt.

Das AISEC Hardware Labor – Angriff ist die beste Verteidigung

Die Sicherheit jedes entwickelten Verfahrens wird vor seinem Einsatz durch gezielte Angriffszenarien auf Herz und Nieren geprüft – vor allem über Seitenkanalangriffe und Fehlerangriffe durch Magnetfeld-Seitenkanalmessung oder Laser-Fehlerinjektion. Im Bereich der Fehlerangriffe auf Sicherheitschips werden an einem eigens entwickelten Laser-Messplatz Angriffe mit zwei getrennten Laserstrahlen durchgeführt. Diese Analysen sind notwendig, um sowohl Implementierungen und Chips für Hochsicherheit als auch allgemeinere eingebettete Anwendungen zu untersuchen sowie deren Sicherheit zu bewerten und zu verbessern.

Das Möglichkeitsspektrum, das das Hardware Labor bietet, wurde über viele Jahre im Rahmen von verschiedenen Förderungen und herausfordernden Projekten aufgebaut. So wurden beispielsweise für einen öffentlichen Auftraggeber erfolgreich hochkomplexe Seitenkanalangriffe auf kryptografische Funktionen eines Sicherheitschips durchgeführt. Durch die Förderung der Initiative BAYERN DIGITAL konnte das Analysewerkzeug maßgeblich vorangetrieben werden.

Im Rahmen des vom BMBF geförderten Projekts ALESSIO wurden neue Ergebnisse bei der höchst präzisen Messung von Magnetfeld-Seitenkanalinformationen zu kryptografischen Implementierungen auf Chips erzielt. Diese wurden im Rahmen einer Veröffentlichung auf der CT-RSA 2018 in San Francisco präsentiert. Als wesentlicher Beitrag des AISEC stand die Entwicklung von gehärteten kryptografischen Implementierungen gegen solche Angriffe im Vordergrund. Dazu wurden bestehende Forschungsergebnisse aus der Vorlaufforschung erweitert und erfolgreich auf FPGA-Chip-Anwendungen übertragen. Im gleichen Förderprojekt wurde auch höchst präzise Fehlerangriffe mit Laserstrahlen von nur wenigen µm Durchmesser unternommen. Es wurden Untersuchungen der erreichbaren Präzision auf Mikrokontroller-Beispielen durchgeführt, wie sie unter anderem in IoT-Geräten zu finden sind.

2018/2019 wurde außerdem intensiv an Sicherheitsanalysen im Bereich Eingebettete Systeme gearbeitet. Hier haben die Forschenden des Fraunhofer AISEC ein Hardware-Tool weiterentwickelt, das sogenannte Fehlerangriffe mittels Glitching automatisch durchführt. Solche Angriffe sind beispielsweise für Steuergeräte im Automobilbereich besonders relevant. Im Rahmen einer Industriekooperation wurden am Beispiel eines erfolgreichen Angriffs gemeinsam mit dem betroffenen Hersteller grundlegende Schutzmaßnahmen erarbeitet.

Im Neubau des Fraunhofer AISEC wird das Hardware-Labor um neueste Technologien und Verfahren erweitert.

THEMA COGNITIVE SECURITY TECHNOLOGIES

Maschinelle Lernverfahren (ML) und Systeme der Künstlichen Intelligenz (KI) werden bereits heute in zahlreichen IT-Infrastrukturen und vernetzten Endgeräten als zentrale Bausteine zur Analyse, Prognose und Steuerung eingesetzt. Autonomes Fahren, Gesundheitsversorgung, Energieversorgung oder auch Produktion der Zukunft sind ohne KI nicht mehr denkbar, bzw. nicht mehr zukunftsfähig. KI-Systemen wird deshalb neben den Daten, die sie verarbeiten, künftig eine zentrale Bedeutung zukommen. Deshalb ist die Vertrauenswürdigkeit derartiger Systeme für Unternehmen aller Branchen, aber auch für staatliche Institutionen von höchster Wichtigkeit.

Bereits seit 2009 arbeiten Forscherinnen und Forscher in der AISEC-Abteilung für kognitive Sicherheitstechnologien an der Schnittstelle zwischen Künstlicher Intelligenz und IT-Sicherheit. Damit ist das Fraunhofer AISEC eines der ersten Forschungsinstitute weltweit, das auf dem Feld tätig ist. Auch als Sprecherinstitut im institutsübergreifenden Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT (vgl. S. 34-35) treibt das AISEC das Thema voran. Seine Kompetenzen im Bereich kognitiver Sicherheitstechnologien bringt das AISEC auch in die KI-Initiative des Bundes ein. Auf der Landesebene beteiligt es sich am Aufbau eines neuen Kompetenznetzwerks für Künstliche Intelligenz, den die Bayerische Staatsregierung im Juni 2018 beschlossen hat.

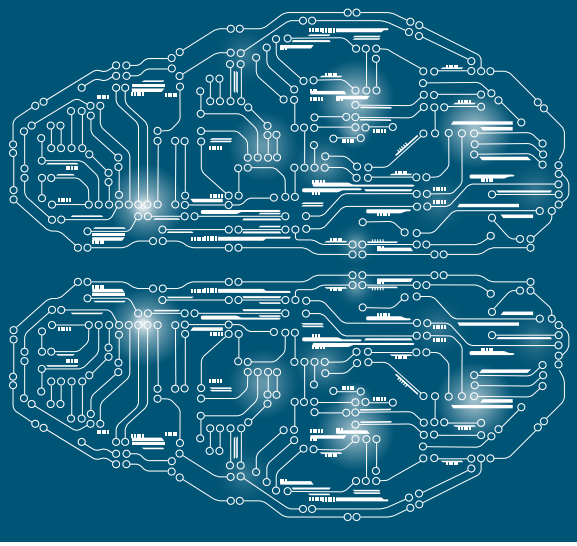
Die Themenbereiche Künstliche Intelligenz und Sicherheit sind dabei in zweierlei Hinsicht miteinander verbunden: Einerseits gilt es, mit wissenschaftlich fundierten Methoden KI-Modelle sicher zu machen, umgekehrt bedeuten kognitive Methoden einen Paradigmenwechsel für die IT-Sicherheit: Mittels KI lassen sich heterogene Datenquellen miteinander verknüpfen und frühzeitig belastbare Aussagen über bevorstehende Angriffe (threat analytics, predivtive security) herleiten. Am AISEC werden in verschiedenen Projekten neue Techniken zur Verbesserung der Angriffsresilienz von Maschinellen Lernverfahren und zur Nutzung von ML zur Angriffsfrüherkennung und -abwehr erarbeitet.

Sicherheit für die KI in der Fabrik der Zukunft

Angetrieben durch die rasante Ausbreitung von IoT und die zunehmende Vernetzung hat die praktische Anwendung der Künstlichen Intelligenz signifikante Fortschritte gemacht. Für die Industrie liegt der Vorteil vor allem in der fortschreitenden Automatisierung und der damit einhergehenden Optimierung von Abläufen. Die stetig wachsenden Datenmengen ermöglichen es, mit datengetriebenen Machine-Learning-Verfahren neue Lösungswege zu ermitteln oder Prozesse effizienter zu gestalten – sofern diese Lernverfahren sicher und zuverlässig sind.

Hier setzt beispielsweise das vom Bundesministerium für Bildung und Forschung geförderte Projekt »CyberFactory#1« innerhalb des Europäischen Gesamtvorhabens »ITEA3« an, in dem Schlüsselfähigkeiten für die Fabrik der Zukunft entwickelt werden. Diese soll sich kontinuierlich an wechselnde Randbedingungen anpassen und sich stetig optimieren können sowie in der Lage sein, ihre Widerstandsfähigkeit gegenüber physischen und IT-technischen Gefährdungen weiterzuentwickeln. Die Erfordernisse von Anwendungspartnern aus der Transportindustrie, der Elektronikfertigung und des Maschinenbaus werden dabei anhand konkreter Anwendungsfälle adressiert und die Eignung der Lösungen in Demonstratoren validiert, die sich an diesen Anwendungsfällen orientieren.

Als Forschungspartner im deutschen Konsortium vertritt das AISEC hier die Wissenschaftsthemen Datenwissenschaft und Künstliche Intelligenz. Systeme, die auf Künstlicher Intelligenz basieren, sind in höchstem Maße anfällig für Manipulationen und Störungen. Das AISEC-Knowhow soll in der Fabrik der Zukunft die Sicherheit und Zuverlässigkeit KI-basierter Steuerungsalgorithmen gewährleisten. Entscheidend sind hier Methoden der Erklärbarkeit und der Transparenz. Im Rahmen des Projektes Cyberfactory#1 werden auch robuste Machine-Learning-Verfahren erforscht, die die Zusammenarbeit von Menschen und Maschinen optimieren:



Ziel ist es, das »Anlernen« durch menschliche Bediener zu erleichtern und das sichere autonome »Hinzulernen« sich selbständig bewegender Maschinen zu ermöglichen.

Auf das Thema Sicherheit zahlt zusätzlich ein, dass das AISEC die in der verteilten Fertigung erfassten großen Datenmengen aus der Fabrik der Zukunft unter Nutzung von sicheren KI-Methoden so modelliert und rekonfiguriert, dass nur kontext- und zielrelevante Daten zur Entscheidungsunterstützung in Echtzeit herangezogen werden – nachdem in der Sicherheit bekannten Need-to-know-Prinzip.

Transparenz, Stabilität und Kontrolle sind das übergeordnete Ziel aller Projekte am AISEC, die sich der Sicherheit für die KI widmen. Der nächste Meilenstein in diesem Kontext wird die Zertifizierbarkeit von sicheren KI-Systemen sein. In einem interdisziplinären Ansatz arbeiten Experten aus den Bereichen KI und Sicherheit an auf unterschiedliche Branchen angepassten Lösungen.

Cognitive Security: die Zukunft der IT-Sicherheit

Technologien wie Machine Learning, Deep Learning und Cognitive Computing sind nicht nur für den industriellen Bereich von signifikanter Bedeutung, sondern spielen auch in der innovativen Sicherheitsforschung eine immer wichtigere Rolle. Durch die zunehmende Qualität und Quantität von Cyber-Attacken müssen zukunftsweisende kognitive Sicherheitstechnologien entwickelt werden, damit potenzielle Bedrohungen schnellstmöglich erkannt, bösartige Angriffe aktiv vorhergesehen und mit entsprechenden Schutzmechanismen verhindert werden können.

Insbesondere Anwendungen zur Erkennung von Mustern und Veränderungen in Datenströmen spielen für die Cybersicherheit eine große Rolle. Angesichts der stetig steigenden Datenmengen in Unternehmen und Produktionsabläufen als Folge der digitalen Transformation und der Umsetzung der Konzepte zur Industrie 4.0 wächst der Bedarf an KI-basierten Technologien, die Sicherheitsexperten dabei unterstützen können, Datenströme zu kontrollieren und den Netzwerkverkehr zu überwachen. So lässt sich KI beispielsweise als Filter einsetzen, der Anomalien im Netzwerk erkennt und gegebenenfalls Alarm schlägt. Derzeit entwickelt die Abteilung »Cognitve Security Technologies« beispielsweise Methoden, die es ermöglichen, auch kleinste Sensoren mit geringer Rechenleistung durch Machine-Learning-Verfahren mit Künstlicher Intelligenz auszustatten, um Anomalien erkennen und entsprechende Warnungen an das System schicken zu können.

Cyber-Sicherheitssysteme können sich mit dem Einsatz modernster Algorithmen für maschinelles Lernen und neuronaler Netze auf Basis der gesammelten Daten kontinuierlich weiterentwickeln. KI-Forensik, Human-Machine-Interface-Security und Predictive Security werden nicht nur dem Mangel an Sicherheits-Fachkräften entgegenwirken. Cognitive Security ist vielmehr die Zukunft der IT-Sicherheit.

Natural Language Processing im Dienste des Datenschutzes

Darüber hinaus forscht das Fraunhofer AISEC auch an Technologien im Bereich Natural Language Processing (NLP) – beispielsweise im Zusammenhang mit der DSGVO. NLP-Technologien ermöglichen es, natürlichsprachliche Dokumente zu analysieren. Dabei verbindet NLP Erkenntnisse aus der Linguistik mithilfe modernster Algorithmen mit Methoden der Künstlichen Intelligenz. Hier werden Modelle entwickelt, die die semantische Struktur verschiedener Datenschutzerklärungen widerspiegeln und so Rückschlüsse auf die Vollständigkeit und Rechtssicherheit der Erklärungen erlauben. So steht Künstliche Intelligenz am Fraunhofer AISEC auch im Dienste des Datenschutzes.

THEMA INDUSTRIAL AND AUTOMOTIVE SECURITY

In Zeiten von IoT und digitalen Fabriken müssen Anlagenbetreiber umfassend in Sicherheit investieren, wenn sie den Herausforderungen der Digitalisierung begegnen wollen. Viele Anlagen und Komponenten sind nur unzureichend auf diese Herausforderungen vorbereitet – bei der Inbetriebnahme hat oft die Betriebssicherheit (Safety) Vorrang, integrierte Sicherheitsmaßnahmen im Sinne der (IT-)Security spielten in der Vergangenheit bislang, wenn überhaupt, nur eine untergeordnete Rolle. Inzwischen hat sich die Erkenntnis durchgesetzt, dass Angriffe auf Industrieanlagen oder teilautonom agierende Systeme nicht nur zu hohen finanziellen Schäden oder Reputationsverlust führen, sondern auch ganz erhebliche Bedrohungen der Betriebssicherheit nach sich ziehen können. Security und Safety hängen vor allem in der Industrie sehr eng zusammen. Gerade im industriellen Bereich kann zudem der Schutz von geistigem Eigentum mitunter über die Existenz eines Unternehmens entscheiden.

Modellbasierte Risikoanalysen und Offensive Security

Um angemessene Sicherheitsmaßnahmen einleiten zu können, müssen Risiken und Bedrohungen früh identifiziert, untersucht und bewertet werden. Die häufig angebotenen One-size-fits-all-Ansätze stoßen besonders im industriellen Bereich schnell an ihre Grenzen und liefern angesichts der komplexen Funktionen, Systeme und Prozesse nur oberflächliche Ergebnisse. Seit 2018 gehört deswegen die »Modular aufgebaute modellbasierte Risikoanalyse MoRA«, die bereits in einer Vielzahl von Projekten, insbesondere im Automotive-Umfeld, eingesetzt wird, zum Portfolio des Fraunhofer AISEC. Die zugrundeliegende Methodik erlaubt eine systematische Erfassung und Bewertung von Schutzzielen, Bedrohungen und Gegenmaßnahmen. Der entscheidende Unterschied zu herkömmlichen Analysemethoden: MoRA ermöglicht es, auch spezielle Aspekte von eingebetteten Systemen zu berücksichtigen. Die Methode unterstützt außerdem eine hierarchische Zerlegung des Evaluierungsziels und erlaubt so eine bessere Skalierbarkeit sowie eine Kosten-Nutzen-Abwägung.

Anhand der modellbasierten Risikoanalyse untersuchen die Wissenschaftlerinnen und Wissenschaftler des Fraunhofer AISEC auch im Rahmen von Forschungsprojekten die Sicherheit von Systemen. Ein aktuelles Beispiel hierfür ist die Zusammenarbeit im Forschungsprojekt »DigitalTWIN«, das digitale Werkzeuge im Bauwesen erforscht. Hier entwickelt ein Konsortium aus Industrie und Forschung digitale Werkzeuge und Techniken für die Baustelle von morgen. Das Fraunhofer AISEC unterstützt hier in den Bereichen Datenschutz und Datensicherheit sowie Authentizität und Verschlüsselungstechniken und hat im Rahmen des Projekts bereits umfassende modellbasierte Risikoanalysen für vorher festgelegte Anwendungsfälle durchgeführt.

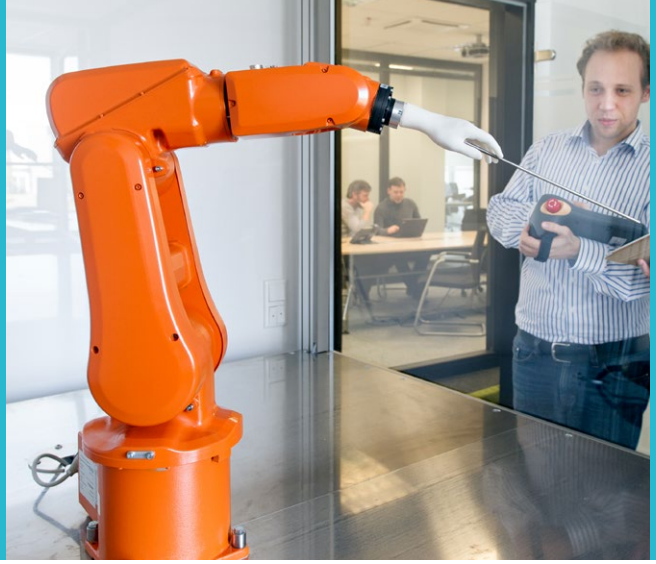
IUNO und IUNO Insec – enger Austausch zwischen Industrie und Forschung

Seine Expertise im Bereich Industrial Security gibt das Fraunhofer AISEC als Mitglied in zahlreichen Projekten an Unternehmen weiter und nutzt die Mitarbeit in Industrieverbänden, um Standardisierungen und die Fachkräfteausbildung in diesem Bereich aktiv mit voranzutreiben.

So war das Fraunhofer AISEC maßgeblich am BMBF-geförderten »Nationalen Referenzprojekt für IT-Sicherheit in der Industrie 4.0 IUNO« mit 20 Partnern aus Wirtschaft und Forschung beteiligt, das im September 2018 erfolgreich abgeschlossen wurde. Im Oktober 2018 ging IUNO nahtlos in das Folgeprojekt IUNO Insec über, bei dem das Fraunhofer AISEC als Verbundkoordinator tätig ist und das Lösungen aus IUNO zur Verbesserung des Sicherheitsniveaus insbesondere für kleine und mittelständische Unternehmen zugänglich machen wird.

Schutz vor Produktpiraterie als wachsender Geschäftsbereich

Neben der Sicherheit der Systeme hat auch der Schutz vor Produktpiraterie im industriellen Umfeld einen immer höheren Stellenwert.



Im Jahr 2018 sind 71 Prozent der Maschinen- und Anlagenbauer große Schäden durch unlautere Nachahmung von Produkten und Komponenten entstanden – so das Ergebnis der »Studie Produktpiraterie 2018«, die durch das Fraunhofer AISEC auf Basis einer Umfrage unter den Mitgliedern des Verbandes Deutscher Maschinen- und Anlagenbau e.V. VDMA erstellt worden ist. Im Vergleich zu den vorangegangen Studien ist das Bedrohungsniveau auf einem konstant hohen Level. Der geschätzte Schaden im Umsatzjahr 2017 beträgt 7,3 Milliarden Euro, was rund 33.000 Arbeitsplätzen entspricht.

Gerade bei High-Tech-Produkten, bei denen der Softwareentwicklungsanteil dominiert, oder deren Geschäftsbasis auf wenigen Algorithmen basiert, ist Produktpiraterie existenzbedrohend. Aus diesem Grund benötigen Unternehmen umfassende Abwehrstrategien, die eine Anpassung an die jeweilige Unternehmenssituation ermöglichen. Das Fraunhofer AISEC unterstützt hier in vielfältiger Weise: Durch Sicherheitskonzepte und Risikoanalysen werden bereits beim Entwurf neuer Produkte Schutzmaßnahmen in die Architektur eingearbeitet. Bei existierenden Produkten wird durch Penetrationstests überprüft, wo mögliche Schwachstellen liegen und wie diese nachträglich, beispielsweise bei einer neueren Version, geschlossen werden können. Dies beschränkt sich nicht nur auf einzelne Teilaspekte, sondern deckt alle wichtigen Bereiche ab – von Web Applications, über Betriebssysteme bis hin zur Hardware Security.

SecForCARs – Sicher vernetzt: Besondere Erfordernisse in der Automobilindustrie

Dass die zunehmende Vernetzung einen stärkeren Fokus auf das Thema IT-Sicherheit erfordert, gilt in besonderem Maße für die Automobilindustrie. Einerseits werden Produktionsprozesse stetig weiter digitalisiert und automatisiert, wodurch sich die Angriffsfläche für Cyberkriminelle vergrößert. Andererseits bestehen heutige Automotive-Systeme selbst aus komplexen Strukturen, die unter Umständen mehr als 100 elektronische Steuergeräte miteinander verbinden – Tendenz steigend.

Um sowohl die interne als auch externe Fahrzeugkommunikation abzusichern, bedarf es Automotive-tauglicher Sicherheitsmechanismen und -protokolle, die auch für lange Produktlebenszyklen geeignet sind.

Für das (teil-)autonome Fahren gilt all dies natürlich umso mehr. Im Rahmen des Projekts »Security For Connected, Autonomous Cars« (SecForCARs) erarbeitet das Fraunhofer AISEC aktuell bereits gemeinsam mit 14 weiteren Partnern aus Industrie und Wissenschaft neue Ansätze für die IT-Sicherheit im autonom fahrenden Auto. Im Fokus steht dabei die Analyse von Sicherheitsfunktionen in vernetzten und (teil-)autonom agierenden Fahrzeugen. Dafür müssen neue Modelle und Methoden entwickelt werden, die eine Bewertung der Sicherheitsfunktionen auch schon in einem frühen Konzeptstadium erlauben.

Das Fraunhofer AISEC unterstützt Unternehmen bei der Entwicklung und Integration von eigenen Methoden zur Aufdeckung von Security-Schwachstellen und führt praxisbezogene Tests von Sicherheitsmaßnahmen durch. Für die Erstellung und Etablierung von Risikobewertungsmethoden oder auch die Integration von Security Engineering in die Entwicklungs- und Qualitätssicherungsprozesse gibt es langjährige Kooperationen und Rahmenverträge mit langen Laufzeiten mit Automobilherstellern und deren Zulieferern.

Im neuen Automotive Lab, das aktuell im Neubau des Fraunhofer AISEC entsteht, wird es mit deutlich erweiterten Technologien möglich sein, die Sicherheitseigenschaften von Soft- und Hardware-Komponenten im und um das Automobil zu analysieren, Lösungen für deren Absicherung zu erarbeiten und deren Wirksamkeit zu demonstrieren.

THEMA APPLICATION AND DATA SECURITY

Angesichts der zunehmenden Vernetzung zielen Angreifer heute auf Kaskaden-Effekte: Schwachstellen in nur einem Teilsystem öffnen in sehr kurzer Zeit die Tür zu vielen anderen. Moderne Applikationen beruhen auf komplexen verteilten Systemen, die die Frage der Sicherheit in ein neues Licht stellen. Fragen des Datenschutzes werden zusätzlich dadurch erschwert, dass Daten heute nicht mehr statisch erfasst und an einem Ort genutzt werden – vielmehr befinden sie sich ständig in Bewegung, sie fließen von diversen mobilen Endgeräten oder Sensoren in die Cloud weiter zu verarbeiten Systemen und zurück.

Labels für den Datenschutz im Internet of Things

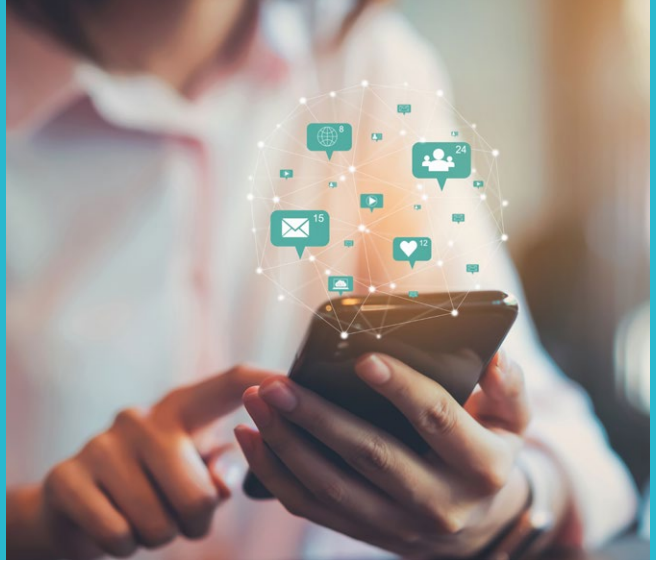
Dies gilt beispielsweise für die Datenflüsse in IoT-Systemen. Um hier mehr Kontrolle und Datensicherheit zu erreichen, wurde am Fraunhofer AISEC das Framework »LUCON« (Label-based Usage Control) entwickelt: Datensätze erhalten in diesem Konzept schon zum Zeitpunkt ihrer Erfassung Labels, die sie klassifizieren. Damit können während der Datenverarbeitung im Vorfeld definierte Nutzungsregelungen, die für unterschiedliche Klassen von Daten festgelegt sind, angewendet werden. Auch Anforderungen an den Datenschutz können so direkt umgesetzt werden. Ein Beispiel hierzu sind Anonymisierungsanforderungen: Daten dürfen erst herausgegeben werden, wenn sie über einen längeren Zeitraum aggregiert worden sind. So können sie nicht mehr einzelnen Personen zugeordnet werden. Einen besonderen Stellenwert hat eine solche Datenflusskontrolle beispielsweise im Bereich Connected Cars. Die hier anfallenden Daten sind häufig personenbezogen und müssen entsprechend geschützt werden. Deswegen ist LUCON ein zentraler Bestandteil des Projekts »car-bits.de«: Gemeinsam mit Uniscon, der Continental Automotive GmbH und der Hochschule Bonn-Rhein-Sieg arbeitet das Fraunhofer AISEC seit 2018 an einer Dienste-Plattform, die es ermöglicht, die Datenberge im vernetzten Auto auszuwerten, ohne dass Datenschutzrechte verletzt werden. LUCON ist bereits seit 2018 im Einsatz und wird hinsichtlich des Paradigmenwechsels im Internet der Dinge stetig weiterentwickelt.

Neue Methoden für die Applikationssicherheit

Im Sinne der Applikationssicherheit spielt das Testen auf Verwundbarkeiten und Schwachstellen eine immer größere Rolle. Aus diesem Grund liegt ein Fokus unserer Wissenschaftlerinnen und Wissenschaftler in der Entwicklung neuer Testmethoden. Seit 2018 wird am Fraunhofer AISEC im Rahmen der Strategie »BAYERN DIGITAL« des Bayerischen Wirtschaftsministeriums intensiv an der Methode »Code Property Graphs« gearbeitet: Die im Quelltext eines Programms verwendeten Variablen und Funktionen werden in eine grafische Darstellung übertragen. Abfragen an den Grafen können validieren, ob Konzepte im Sinne der Sicherheit richtig implementiert wurden. Die Methode kann auch dann angewendet werden, wenn nur Teile eines Quellcodes bekannt sind oder Quellcode nur partiell zur Verfügung gestellt werden darf.
Insbesondere bei kritischen Anwendungen, beispielsweise beim Mobile Payment oder bei anderen Banking-Apps, muss die Sicherheit zwingend noch im Entwicklungsprozess oder zum Abschluss desselben kritischen Tests unterzogen werden, zumal sich auch die Methoden der Angreifer weiterentwickeln. Aus diesem Grund hat sich beispielsweise das »Certificate Pinning« als Standard etabliert und ist im Überprüfungsprozess stärker in den Fokus gerückt. Die hohen Sicherheitsanforderungen, die Applikationen im Banking- und Finanzsektor erfüllen müssen, werden am Fraunhofer AISEC im eigens dafür eingerichteten und hochspezialisierten Payment-Labor untersucht. Die Überprüfung der Sicherheitsfeatures von Apps erfolgt einerseits durch die Evaluierung des Quellcodes durch Fachexperten, außerdem werden am Fraunhofer AISEC Technologien entwickelt, die Schwachstellen durch semi-automatische Werkzeuge aufdecken.

Selbstbestimmung für digitale Identitäten

Eine wichtige Säule im Umgang mit digitalen Anwendungen ist ein vertrauenswürdiges Identitätsmanagement, das die Verwaltung der eigenen persönlichen Daten und die Verteilung von Zugriffsberechtigungen ermöglicht. Unter dem Schlagwort



»Self Sovereign Identity« reagiert das Fraunhofer AISEC auf das wachsende Bedürfnis der Endverbraucher, ihre digitale Identität selbstbestimmt zu verwalten und persönliche Daten zu schützen. Die Wissenschaftlerinnen und Wissenschaftler arbeiten daran, Unternehmen im Sinne ihrer Kunden Alternativen zu zentralen Identitätsprovidern wie Facebook und Google anzubieten.

Ein Ansatz hierzu ist »re:claimID«. Im Gegensatz zu traditionellen zentralisierten Identitätsdiensten werden Identitäten in einem sicheren dezentralen Verzeichnisdienst verwaltet. Als solcher dient das Peer-to-Peer Namenssystem GNS (GNU Name System). Der Nutzer kann persönliche Daten wie zum Beispiel E-Mail-Adresse oder Geburtsdatum in diesem Verzeichnis ablegen. Diese Daten werden dort nicht im Klartext – also für jeden lesbar – gespeichert, sondern verschlüsselt. Auf Anfrage kann der Nutzer den Zugriff auf eine Teilmenge seiner Daten autorisieren, indem er dem Anfragenden einen individuellen Schlüssel ausstellt. Der Nutzer kann diesen Zugriff jederzeit widerrufen oder einschränken.
Aktuell arbeitet das re:claimID-Forschungsteam am Fraunhofer AISEC an einer Weiterentwicklung des Werkzeugs, um den Einsatz auf industrielle Anwendungsfälle zu erweitern und damit den Herausforderungen der zunehmenden Vernetzung im IoT zu begegnen.

Kontrolle in der Cloud

Nicht nur auf der Ebene der Anwendungen selbst und im Bereich Identity- und Access-Management nehmen die Herausforderungen an die IT-Sicherheit zu, auch durch die steigende Nutzung von Cloud-Diensten entstehen immer neue Angriffsflächen und Sicherheitslücken.

Im Spannungsfeld zwischen Cloud-Computing und Datensicherheit forscht das Fraunhofer AISEC an Methoden und Techniken, mit denen sich Sicherheitslücken schnell auffinden und beheben lassen. Im Juni 2019 hat das Fraunhofer AISEC die Community-Edition des »Clouditors« veröffentlicht.

Der Clouditor ist ein Assurance-Werkzeug, das die sichere Konfiguration von Cloud-Services überprüft und Schwachstellen detektiert. Er nimmt über die APIs von Cloud-Providern wie zum Beispiel Amazon Web Services oder Microsoft Azure kontinuierliche und automatisiert durchgeführte Überprüfungen von Sicherheits- und Compliance-Anforderungen vor, basierend auf Konfigurationskatalogen, die Best Practices für die Security beschreiben und benutzerdefiniert angepasst werden können. Insbesondere kleine und mittelständische Unternehmen bekommen damit die Möglichkeit, die Chancen der Cloud zu nutzen, die Konfigurationen ihre Cloud-Dienste zu auditieren und sich gleichzeitig auf einfache Weise über die Einhaltung wichtiger Sicherheitseigenschaften zu vergewissern.

Unterstützt wurde das Projekt im Rahmen von »NGCert« durch das Bundesministerium für Bildung und Forschung sowie im Rahmen von »EU-SEC« durch die Europäische Union. Für 2020 ist der Einsatz des Clouditors in der »Bayern.Cloud« geplant: die digitale Plattform, die vom Bayerischen Landesinstitut fortiss betrieben wird, bietet Hilfestellung für kleine und mittelständische Unternehmen, die weder das erforderliche Know-how noch die Ressourcen haben, um Cloud-Lösungen sicher und datenschutzkonform zu nutzen.

KOMPETENZAUFBAU SICHER IN DIE 5G-WELT

Vernetzte Baustellen, die Steuerung vernetzter Medizinroboter und autonome Autos – die umfassende Digitalisierung aller Lebensbereiche und die Manifestierung der Industrie 4.0 erfordern neue Datenübertragungswege. Unter Hochdruck wird deshalb an der Etablierung von 5G gearbeitet: mit Datenraten bis zu 10.000 Mbits/s wird das 5G-Netz bis um 100 Mal schneller sein als heutige LTE-Netze.

Damit 5G jedoch zum echten Innovationstreiber werden kann, bedarf es dedizierter Sicherheitstechnologien. Die neue Struktur des »Netzwerks aus Netzwerken« birgt hier ganz neue Anforderungen: Die hohe Dynamik der Netze und die neu entstehenden Angriffsflächen erfordern einen umfassenden Schutz vor unerlaubten Datenzugriffen und eine hohe Resistenz gegenüber Störungen. In diesem Zusammenhang bereitet auch das Fraunhofer AISEC Schlüsseltechnologien für das Netz der Zukunft vor.

Vertrauenswürdige Containertechnologien

Durch den Einsatz vertrauenswürdiger Containertechnologien ist es möglich, einzelne Funktionen und Datenpakete separiert zu verwalten und sie flexibel an die entsprechenden Edge-Knoten oder in die Cloud zu leiten – und damit auf das feingranulare Netzwerk in der 5G-Welt zu reagieren. Diese Isolierung der Datenpakete und Funktionen in Container erhöht das Sicherheitsniveau signifikant.

Ein Projekt, in dem das Fraunhofer AISEC den Einsatz von Containertechnologien zur Erhöhung der Sicherheit in 5G-Netzen auf den Prüfstand stellt, ist das Projekt »SENDATE« (Secure Networking for a Data Centre Cloud in Europe), das im Rahmen des »EUREKA«-Programms vom BMBF gefördert wurden und im März 2019 erfolgreich abgeschlossen worden ist: Im Projekt wurden Lösungen entwickelt, die es durch eine enge Verbindung von Telekommunikationsnetzen und IT-Systemen ermöglichen, Daten nicht nur zu erfassen und zu transportieren, sondern dabei gleichzeitig für die notwendige Sicherheit und Flexibilität zu sorgen. Die Expertise des AISEC auf den Gebieten SDN und Virtualisierung haben das Design der SDN/NFV-Anwendungen maßgeblich beeinflusst: Auf Basis von Container-Technologien können einzelne Anwendungen isoliert voneinander laufen.

Neue Prüfwerkzeuge und Open-Source-Hardware in komplexeren Netzwerken

Der Einsatz von sicheren Open-Source-Hardware-Komponenten wie beispielsweise RISC-V-Prozessoren ist aktuell auf dem Vormarsch und schafft Vertrauen in die verbaute Hardware neuer Netzwerke. Im eigenen Hardware-Labor untersucht das Fraunhofer AISEC beispielsweise die Sicherheit dieser spezialisierten Hardware-Module: Open-Source-Komponenten werden auf mögliche Schwachstellen überprüft, um sie beispielsweise für einen Einsatz im 5G-Kontext zu rüsten.

Das Fraunhofer AISEC bereitet sich mit dem Ausbau des bereits bestehenden 4G-Labors zu einem 5G-Labor auf das neue Zeitalter vor. Die Forschenden entwickeln Verfahren, um Systeme und Netze auf die Einhaltung der Mindeststandards zu überprüfen und Guidelines zu erstellen, die Netzbetreiber bei der Instandhaltung unterstützen.

Die Komplexität und Dynamik in 5G-Netzen erfordert zusätzlich neue Methoden, um Schwachstellen systematisch aufzuspüren. Durch automatisierte Prüfwerkzeuge können verteilte Third-Party-Komponenten umfassend analysiert werden. Dies garantiert Vertrauenswürdigkeit und Integrität, insbesondere der Software-Komponenten, in der gesamten Software Supply Chain.

KOMPETENZAUFBAU SICHER IN DIE POST-QUANTEN-ÄRA

Schneller als die Forschung zur Rechenleistung des Quantencomputers muss diejenige für neue defensive Cyber-Sicherheitsarchitekturen vorangetrieben werden. Denn die meisten aktuell verwendeten kryptografisch abgesicherten Internetverbindungen, die Verschlüsselungsverfahren selbst sowie deren Implementierungen auf der Hardware-Ebene stehen in der Post-Quanten-Ära auf dem Prüfstand. In all diesen Bereichen gibt es jedoch am Fraunhofer AISEC laufende Forschungsvorhaben.

Post-Quanten-VPN

Im BMBF-geförderten Projekt »Quantensichere VPN-Module und Operationsmodi« beschäftigt sich die AISEC-Abteilung »Sichere Infrastruktur« zusammen mit Partnern aus der Industrie mit der Erforschung und Umsetzung einer quantensicheren VPN-Lösung. Im Mittelpunkt steht die Frage, welche kryptografischen Primitive und Verfahren für den Einsatz auf den unterschiedlichen Schichten des ISO/OSI Referenzmodells der Netzwerktechnik geeignet sind. Etablierte Kommunikationsprotokolle sollen untersucht und Anpassungen vorschlagen werden, die auch im Post-Quanten-Zeitalter eine einfache Austauschbarkeit kryptografischer Verfahren (die vom Bundesamt für Sicherheit in der Informationstechnik BSI für die Post-Quanten-Ära empfohlene, sog. Krypto-Agilität) ermöglichen. Im Sinne der Interoperabilität zwischen verschiedenen Protokollimplementierungen und deren Praxistauglichkeit sollen ferner die für die Quantenresistenz relevanten Aspekte einer Standardisierung zugeführt werden.

Post-Quanten-PKIs und Kryptobibliotheken

Zu den Empfehlungen des BSI gehört auch der Entwurf abwärtskompatibler Pubic Key Instrastructures (PKIs). Eine PKI erstellt und verwaltet vertrauenswürdige elektronische Identitäten für Personen, Dienste und Dinge, die eine starke Authentifizierung, Datenverschlüsselung und digitale Signaturen über Zertifikate ermöglichen. Zurzeit werden Zertifikate mit klassischen Verfahren gesichert, die aber, sobald es Quantencomputer gibt, gebrochen werden können. Damit können Angreifer gültig erscheinende Zertifikate selbst erstellen.

Die AISEC-Abteilung »Secure Systems Engineering« (SSE) forscht unter anderem zum Thema abwärtskompatible, quantencomputerresistente PKIs. Dabei werden sowohl Lösungen betrachtet, die auf hybriden X.509 Zertifikaten basieren, als auch Lösungen, die den Parallelbetrieb von konventionellen und Post-Quantum-PKIs ermöglichen. Verschiedene Anwendungsgebiete, zum Beispiel PKIs für Signaturen, Authentisierung und Schlüsselaustausch werden in den Blick genommen. Es ist geplant, dass Industriepartner aus den Bereichen Automotive, Industrie 4.0 und Finanzinfrastruktur neu entwickelte Lösungen in Demonstratoren überführen.

Ein weiterer Schwerpunkt der Abteilung SSE auf dem Gebiet der Post-Quantenkryptografie ist das Vorhaben, die »Kryptobibliothek Botan« so zu erweitern und zu verbessern, dass Entwicklerinnen und Entwickler auf Basis der hier zur Verfügung gestellten Funktionen Lösungen finden können, die langlebige Sicherheit umsetzen. Hierzu gehören neben der Aufnahme quantencomputerresistenter Kryptoalgorythmen auch die Unterstützung des Schlüsselmanagements, die Wahrung der Kryptoagilität und vor allem die einfache Benutzbarkeit der Bibliothek.

Implementierungssicherheit als neuralgischer Punkt

Bei allen vorhandenen Ansätzen darf der Aspekt der sicheren Implementierung in der Post-Quanten-Ära nicht aus den Augen verloren werden. Vor allem Eingebettete Systeme und Chipkarten-basierte Sicherheitsanwendungen, die einerseits komplexe Anforderungen erfüllen, aber mit wenig Speicherplatz arbeiten müssen, stellen hier Herausforderungen dar. Ziel des im Rahmen der Hightech-Strategie 2025 vom BMBF geförderten Verbundprojektes »Aquorypt« ist es, die Anwendbarkeit quantencomputerresistenter kryptografischer Verfahren vom Implementierungsaspekt her zu untersuchen.

KURZMELDUNGEN I:

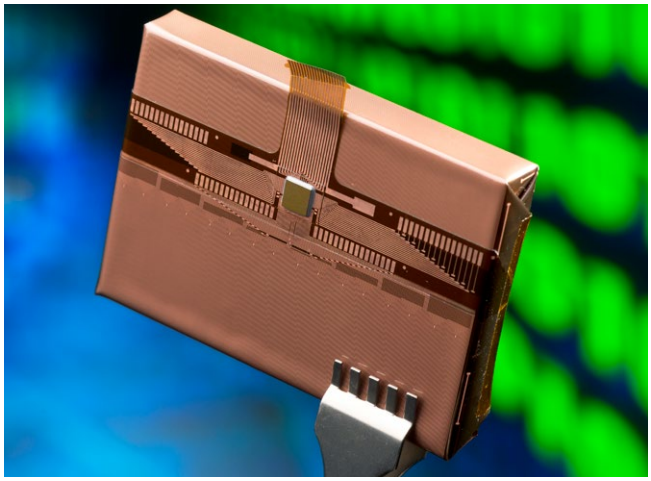
AUSZEICHNUNGEN UND ZERTIFIKATE

Zweimal in Folge: Innovator des Jahres

Bereits zum zweiten Mal in Folge wurde das Fraunhofer AISEC im Jahr 2019 vom Wirtschaftsmagazin brand eins Wissen und dem Statistik-Portal Statista als »Innovator des Jahres« ausgezeichnet. In der Kategorie »Technologie & Telekommunikation« (kleinere und mittelständische Unternehmen) erhielt das Fraunhofer AISEC in der repräsentativen Umfrage wie bereits 2018 die meisten Empfehlungen und damit die bestmögliche Bewertung.

Zu den ebenfalls mit der Höchstbewertung ausgezeichneten Organisationen gehören das Fraunhofer IIS, das Deutsche Forschungszentrum für Künstliche Intelligenz oder IBM.

Seit 2016 wird die Auszeichnung an die renommiertesten Innovatoren aus zwanzig Branchen verliehen und basiert auf der Auswertung dreier Expertenbefragungen: 2.500 Vertreter führender innovationsprämierter Unternehmen, 400 Experten des Instituts für Innovation und Technik (iit) in Berlin und 20.000 Führungskräfte des Statista Panels »Expert Circle« geben für die Umfrage jeweils ihre Stimme ab.



Ausgezeichnet: Best Paper Award auf der HOST 2018

Das »IEEE International Symposium Hardware-Oriented Security and Trust« (Host) ist eine der wichtigsten Konferenzen im Bereich Hardware Security. Auf der elften HOST 2018 in Washington, D.C. (USA) wurde die Studie »B-TREPID: Batteryless Tamper-Resistant Envelope with a PUF and Integrity Detection« mit dem Best Paper Award ausgezeichnet.

Die Arbeit ist eine institutsübergreifende Teamleistung von Vincent Immler (AISEC), Johannes Obermaier (AISEC), Martin König (EMFT), Matthias Hiller (AISEC) und Georg Sigl (AISEC). Sie stellt grundlegende Konzepte und Prinzipien für eine Schutzfolie gegen Hardware-Manipulationen an Platinen vor: Der Schutzmantel mit einer elektrisch leitfähigen Gitterstruktur, der um ein Elektronikgehäuse gewickelt wird, prüft vor jedem Systemneustart von innen heraus, ob er unversehrt ist. Sie nutzt dabei den einzigartigen Materialfingerabdruck, der bei ihrer Herstellung als Physical Unclonable Function (PUF) entsteht. Nur bei einer intakten PUF kann auf verschlüsselte Daten zugegriffen werden. Im Vergleich zu älteren Systeme ist die hier vorgestellte Hochsicherheitslösung nicht batteriegepuffert und bietet dadurch eine bessere Benutzbarkeit und mehr Einsatzmöglichkeiten.

Prof. Dr. Claudia Eckert erhält Staatsmedaille für besondere Dienste um die bayerische Wirtschaft

Im April 2018 wurde Prof. Dr. Claudia Eckert mit der Staatsmedaille für besondere Verdienste um die bayerische Wirtschaft ausgezeichnet. Als eine von 15 herausragenden Persönlichkeiten wurde sie von Bayerns Wirtschaftsminister Franz Josef Pschierer für ihre herausragenden Leistungen im Bereich IT-Sicherheit geehrt:

Claudia Eckert ist seit 2009 Professorin der Technischen Universität München, wo sie den Lehrstuhl für Sicherheit in der Informatik an der Fakultät für Informatik innehat, und Leiterin des von ihr gegründeten Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit AISEC. Durch die Entwicklung des Lehrstuhls und die Gründung des Fraunhofer AISEC ist es Claudia Eckert gelungen, ein international geachtetes Kompetenzzentrum aufzubauen, das auch für die bayerische Wirtschaft hohe strategische Bedeutung hat, so Wirtschaftsminister Franz Josef Pschierer in seiner Laudation. Die Staatsmedaille für besondere Verdienste um die bayerische Wirtschaft wird seit 1974 an jährlich höchstens 25 Personen verliehen.

TISAX® RESULT AVAILABLE

ISO 9001 Zertifiziertes Qualitätsmanagementsystem TÜV SÜD ISO 9001 www.tuev-sued.de/ms-zert

Zertifiziertes Qualitätsmanagement am Fraunhofer AISEC

Das Fraunhofer AISEC entwickelt im Auftrag von Kunden und Partnern qualitativ hochwertige Sicherheitstechnologien und Dienstleistungen. In diesem Zusammenhang ist es entscheidend, Prozessabläufe kontinuierlich zu verbessern, um auf die Bedürfnisse und Anforderungen von Auftraggebern adäquat reagieren zu können. Das Fraunhofer AISEC hat im Jahr 2018 gleich zwei Zertifizierungsaudits erfolgreich durchlaufen.

Der TISAX (Trusted Information Security Assessment Exchange) ist ein einheitlicher Prüf- und Austauschmechanismus, der kosten- und zeitintensive Mehrfachprüfungen in der Automobilindustrie vermeiden soll. TISAX wurde vom Verband der Automobilindustrie (VDA) entwickelt und ist Teil des Information-Security-Assessment (ISA). Das Fraunhofer AISEC ist Teilnehmer der Plattform und wurde 2018 von der TÜV Rheinland i-sec GmbH erfolgreich auditiert.

Seit Dezember 2018 ist das Fraunhofer AISEC außerdem nach DIN EN ISO 9001:2015 zertifiziert. Der internationale Qualitätsmanagement-Standard garantiert Partnern und Kunden im In- und Ausland Leistungsfähigkeit, Effizienz und Serviceorientierung. Nicht nur die sehr guten Ergebnisse in der Zertifizierung durch die TÜV SÜD Management Service GmbH, sondern auch das Vertrauen von Partnern und Kunden sind ein Beweis für die hohen Qualitätsstandards am Fraunhofer AISEC.

KURZMELDUNGEN II:

AUS UNSEREM NETZWERK

Initiative »Bayern online – aber sicher!« erfolgreich gestartet

Mit der Initiative »Bayern online – aber sicher!« hat das bayerische Kabinett unter der Federführung von Bayerns Digitalministerin Judith Gerlach erneut stark in das Thema IT-Sicherheit und den Ausbau der Digitalen Verwaltung investiert. Im Zentrum der Initiative steht die Weiterentwicklung und Stärkung der Cybersicherheit – insbesondere auch für kleine und mittelständische Unternehmen. Außerdem sollen alle wichtigen Behördenangelegenheiten bis Ende 2020 online möglich sein.
Schwerpunkt der Initiative ist es, Bürger, Unternehmen und Kommunen beim Schutz ihrer Daten zu unterstützen. Das Fraunhofer AISEC nimmt hier insbesondere im Bereich Cybersicherheit für Mittelständler eine führende Rolle ein: Durch Kooperationen und spezielle Förderprogramme soll die Entwicklung von IT-Sicherheitslösungen weiter gestärkt werden. Ein besonderer Fokus liegt dabei auf der Früherkennung von Gefährdungslagen. Zur zielgerichteten Reaktion auf Bedrohungen soll weiterhin ein Security Operation Center entstehen, das es bayerischen Unternehmen ermöglichen soll, sich mit Anbietern von Sicherheitstechnologien zu vernetzen und in IT-Notfällen schneller mit den zuständigen Stellen in Kontakt zu treten.

Deutsch-Französische Initiative

Am 19. Juni 2018 unterzeichneten das Ministerium für Hochschulen, Forschung und Innovation der Französischen Republik und das Bundesministerium für Bildung und Forschung der Bundesrepublik Deutschland (BMBF) anlässlich des Forums zur deutsch-französischen Forschungskooperation in Berlin eine gemeinsame Absichtserklärung. Eines der hier formulierten Vorhaben ist die gemeinsame Sicherheitsforschung im Sinne der digitalen Souveränität Europas und ihre Umsetzung mit Industriepartnern aus beiden Ländern. Für die Formulierung dieser Ziele und möglicher Ausgestaltungen der Forschungskooperation haben sich führende europäische Institutionen im Bereich der IT-Sicherheitsforschung zusammengeschlossen, darunter das Fraunhofer AISEC, das Karlsruher Institut für Technologie KIT mit seinem mit seinem Kompetenzzentrum KASTEL, und das Helmholtz Center for Information Security CISPA. Als Sprecherin und Koordinatorin der deutschen Aktivitäten hat das BMBF Prof. Dr. Claudia Eckert benannt.

IUNO wird IUNO Insec

Im September 2018 wurde in Berlin der erfolgreiche Abschluss des »Nationalen Referenzprojekts zur IT-Sicherheit in der Industrie 4.0 IUNO« gefeiert. Der Forschungsverbund, bestehend aus 21 Partnern aus Forschung und Wirtschaft, hat sich in den letzten drei Jahren den Herausforderungen der zunehmenden Digitalisierung in der Industrie gewidmet, Bedrohungen und Risiken für die intelligente Fabrik identifiziert und entsprechende Schutzmaßnahmen entwickelt. Übergeordnetes Ziel von IUNO war es, Lösungen zu entwickeln, die möglichst allgemein und damit für unterschiedlichste Unternehmen verwendbar sind. Im Folgeprojekt IUNO InSec werden nun ausgewählte Lösungen aus dem IUNO-Projekt weiterentwickelt und zur Produktreife gebracht. Im Fokus steht die systematische Verbesserung des Sicherheitsniveaus für kleine und mittelständische Unternehmen, die häufig nicht über das notwendige Expertenwissen oder die finanziellen Mittel verfügen, um selbstständig passende Sicherheitsstrategien zu entwickeln.

secUnity: Meilensteine in der IT-Sicherheitsforschung

Angesichts der fundamentalen Risiken, die durch die Digitalisierung ganzer Industriezweige entstehen, wächst der Bedarf an einem interdisziplinären Netzwerk von Experten der zivilen Cybersicherheitsforschung auf EU-Ebene. »secUnity«, ein vom Bundesministerium für Bildung und Forschung (BMBF) gefördertes Projekt zur Stärkung der IT-Sicherheitsforschung in Deutschland und Europa, hat die Herausforderungen, denen die europäische Cybersicherheitsforschung in Zukunft gegenübersteht, in der Roadmap »Cybersecurity Resarch: Challenges and Course of Action« zusammengefasst und am 5. Februar 2019 an die Europäische Agentur für Cybersicherheit ENISA übergeben. Die Roadmap wurde von über 30 namhaften europäischen IT-Sicherheitsexperten erarbeitet, darunter Forscherinnen und Forscher des Fraunhofer AISEC. Sie soll ein Grundstein sowohl für den politischen als auch für den wissenschaftlichen Diskurs sein und repräsentiert die Vision einer interdisziplinären und gemeinschaftlichen Erschließung innovativer Forschungsfragen im Bereich Cybersicherheit.

Ein weiterer Meilenstein von secUnity war die Veröffentlichung der europäischen IT-Sicherheitslandkarte im Dezember 2018, die einen umfassenden Überblick über die Akteure in der aktuellen europäischen IT-Sicherheitsforschung ermöglicht. Das Fraunhofer AISEC war an der Entwicklung der Karte maßgeblich beteiligt. Die deutschlandweite Karte, die bereits seit Februar 2017 verfügbar ist, wurde dafür sukzessive erweitert und bietet jetzt einen Überblick über alle Akteure in verschiedenen Bereichen der IT-Sicherheit – von Universitäten und Forschungsreinrichtungen bis hin zu kleinen und mittelständischen Unternehmen.

Fraunhofer AISEC ist Teil des Infineon Security Partner Networks

Die digitale Welt treibt die Vernetzung immer weiter voran und ebnet den Weg für neue Geschäftsfelder und Services. Doch durch die fortschreitende Vernetzung steigt auch das Risikopotenzial für Cyberattacken. Einige Sicherheitsexperten vertreten sogar die Meinung, dass unsere Abhängigkeit von Internet-basierten, vernetzten Technologien größer ist als die Fähigkeit, Netzwerke und Geräte umfassend abzusichern.

Um den wachsenden Bedrohungen zu begegnen, schenken immer mehr Unternehmen dem Thema Sicherheit mehr Bedeutung. Der einfachste und zugleich sicherste Weg für Unternehmen, sich dem Thema anzunehmen, ist eine Kooperation mit einem erfahrenen Sicherheitspartner – denn häufig fehlen intern die Ressourcen und das technische Know-how, um Systeme selbst abzusichern. Aus diesem Grund hat Infineon das Infineon Security Partner Network ISPN gegründet. Das ISPN fungiert als Schnittstelle für Unternehmen und Sicherheitsexperten und bringt sie zusammen, um End-to-End-Sicherheitslösungen bereitzustellen. Auch das Fraunhofer AISEC ist Partner und unterstützt das Netzwerk mit seiner umfassenden Expertise im Bereich Embedded Security. Die Anwendungsbereiche reichen von der Home Automation über Industrial Security bis hin zur Automobiltechnik und dem IoT im Allgemeinen.

FRAUNHOFER CLUSTER OF COGNITIVE INTERNET TECHNOLOGIES

Die vierte industrielle Revolution birgt viele Herausforderungen, denen sich die Industrie stellen muss. Die Orientierung an klassischen, webbasierten, digitalen Prozessen greift entscheidend zu kurz. Um ihre Digitalisierungsvorhaben umzusetzen, benötigt die Industrie neue, kognitive, also mit KI-Fähigkeiten angereicherte, Technologien, um neue, digitale Geschäftsmodelle entwickeln und damit im globalen Wettbewerb bestehen zu können. Anwendungen, Produkte und Dienstleistungen müssen nicht mehr nur innovativ sein, vielmehr erfordern sie für kognitive Anwendungen auch die vertrauenswürdige Nutzung vielfältiger Sensordaten des Internet of Things, ihre unternehmensübergreifende semantische Integration und die Erbringung hochintelligenter, lernender Dienstleistungen. Die Daten, die durch die durchgehende Vernetzung von Maschinen, Produkten und Prozessen im IoT entstehen, bieten ein enormes Potenzial, gleichzeitig führen sie aber auch zu einer hohen Komplexität. Für viele Unternehmen stellt die zunehmende Komplexität eine kaum zu beherrschende Herausforderung dar. Hier setzt der Fraunhofer Cluster of Exellence »Cognitive Internet Technologies« (CCIT) an und arbeitet an zentralen Schlüsseltechnologien für ein kognitives industrielles Internet mit dem Ziel, eine zentrale Komponente für eine agile, flexible und wettbewerbsfähige Industrie bereitzustellen.

Exzellente Forschung durch gebündelte Kompetenz

Die Fraunhofer-Gesellschaft hat mit der Neugründung des Clusters of Excellence Cognitive Internet Technologies (CCIT) frühzeitig auf den Bedarf aus der Industrie reagiert. Seit seiner Gründung im Frühjahr 2018 bündelt der Forschungscluster die Kompetenzen von dreizehn Fraunhofer-Instituten aus Mikroelektronik, Informations- und Kommunikationstechnik und Produktion. Die erstklassigen Forschungs- und Entwicklungskompetenzen aus den einzelnen Instituten werden im CCIT zusammengeführt und auf das Ziel ausgerichtet, digitale Souveränität für Unternehmen zu unterstützen und vertrauenswürdige Technologien für innovative Formen der industriellen Datenökonomie bereitzustellen. Drei Forschungszentren (IoT-COMMs, Data Spaces und Machine Learning) entwickeln unter unterschiedlicher Schwerpunktsetzung die für ein kognitives industrielles Internet notwendigen Schlüsseltechnologien. In zwei der drei Zentren vertreten, nimmt das Fraunhofer AISEC eine führende Rolle im Cluster ein.

Das Forschungszentrum IoT-COMMs will die Forschung in den Basistechnologien Vernetzung, Lokalisierung und Informationssicherheit vorantreiben und kombinieren, um die Entwicklung auf zwei Schlüsselbranchen für das Internet of Things (IoT) zu fokussieren: agile und mobile Produktionssysteme im Umfeld der Industrie 4.0 sowie Mobilitätsanwendungen und autonomes Fahren. Im Fokus stehen insbesondere Robustheit, Störsicherheit und kurze Verzögerungszeiten sowie Informationssicherheit.

Das Forschungszentrum Data Spaces (FDS) fokussiert sich auf die Dateninfrastrukturebene und stellt so das Bindeglied zwischen der physischen Kommunikation (Zentrum IOT-COMMs) und der Anwendungsebene (Zentrum ML) dar. Hierbei konzentrieren sich die Arbeiten auf Datensouveränität und Datenökonomie als Grundlage für die datengetriebene Wertschöpfungskette, die der CCIT ermöglichen will. Durch die »Industrial Data Space«-Initiative existiert bereits ein Referenzarchitekturmodell, das derzeit als Blaupause in anderen Initiativen, wie dem Medical und dem Mobility Data Space, aufgegriffen wird.

Das Ziel im Forschungszentrum Machine Learning (FML) ist die Etablierung des sogenannten »Informed Machine Learning« auf breiter Fläche. Darunter versteht man Ansätze, die nicht nur aus Daten lernen, sondern auch vorhandenes Expertenwissen und Modelle, wie sie in der Wirtschaft oft vorhanden sind, zur Leistungsverbesserung nutzen können – für flexible und sich selbst verbessernde intelligente Systeme. Mit diesem Ansatz wird eine zentrale Herausforderung bei KI-Anwendungen im industriellen Kontext gelöst werden: das Fehlen von großen Datensätzen. Anders als im Consumer-Umfeld können KI-Verfahren selten auf Big Data aufsetzen, es stehen nur wenige Datensätze (Small Data) zur Verfügung. Durch deren Anreicherung mit Expertenwissen können die Möglichkeiten der KI auch im industriellen Umfeld genutzt werden.

Gleichzeitig wird die Nachvollziehbarkeit und Verlässlichkeit der Ergebnisse gesichert und so die Voraussetzung für vertrauenswürdige kognitive Internet-Technologien geschaffen.

Erste Schlüsseltechnologien vorgestellt

Bereits im ersten Jahr konnten durch die interdisziplinäre Zusammenarbeit innovative Projekte auf den Weg gebracht, in gemeinsamen Publikationen vorgestellt und erste Demonstratoren erfolgreich auf verschiedenen Messen präsentiert werden.

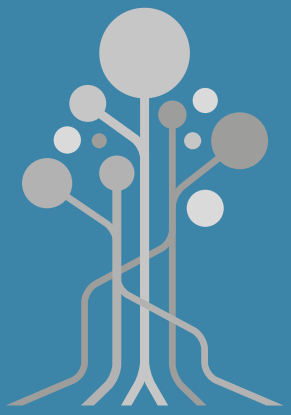
So beispielsweise der Track-and-Trace-Demonstrator, der lückenlose vertrauenswürdige Warenverfolgung mit kognitiver Sensorik und Blockchain-Technologie anhand eines Anwendungsfalls aus der Logistik beschreibt. Dieser zeigt eine Kombination aus sicherer kognitiver Sensorik und Lokalisierung mit der Möglichkeit, Daten souverän und manipulationssicher zu verarbeiten und dezentral zu speichern. Die erhobenen Daten werden in der Trackchain mittels Attribute-based Encryption verschlüsselt gespeichert, um einen selektiven Zugriff darauf zu ermöglichen. Die Verteilung mittels Blockchain schützt vor nachträglicher Manipulation. Auf diese Weise geschützte Daten werden im Industrial Data Space nach definierten Regeln datenschutzkonform weiterverarbeitet und verteilt. Durch Machine-Learning-Verfahren zur Erkennung von Ereignissen und Anomalien können Unternehmen zudem ihre Prozesse kontinuierlich optimieren. Zentraler Bestandteil des Exponats ist der Cognitive Sensor Connector, der im Rahmen des CCIT und unter der Projektleitung des Fraunhofer AISEC entwickelt wurde. Als Edge Device verarbeitet er die anfallenden Rohdaten lokal vor. Damit reduziert sich nicht allein das Volumen der zu übertragenden Daten, sie werden vielmehr bereits am Ort ihrer Erhebung zu Smart Data veredelt, also verarbeitet, analysiert und aggregiert. Die Verarbeitung erfolgt manipulationsgeschützt in speziell isolierten, abgesicherten Applikationen auf dem Connector, die unterschiedliche Funktionen ausführen. Alle Sensoren kommunizieren über verschlüsselte, authentifizierte und integritätsgestützte Funkverbindungen mit dem Connector. Verlassen die Daten den Connector, um beispielsweise Informationen über den Zustand der Ladung an die beteiligten Akteure zu übermitteln, unterliegen sie einer strengen Datenfluss- und Datennutzungskontrolle, die eindeutig regelt, wer welche Daten wie lange, wo und zu welchem Zweck nutzen darf. Die Vertrauenswürdigkeit der Sensordaten und die Einhaltung der Nutzungsregeln kann dabei stets überprüft werden.

Ein strategisches Leuchtturmprojekt des CCIT ist die Entwicklung eines Sprachassistenz-Systems, das durchgängig auf Fraunhofer-Technologien aufsetzt und unter anderem durch Rauschunterdrückungsmodule und die Absicherung der Datenmodelle für einen sicheren Einsatz im industriellen Umfeld sorgen soll. Demonstratoren zu den Themen Smart Intersection, Intelligente Werkzeuge und Selbstregulierende Produktion werden aktuell entwickelt.

Ein Blick zurück – ein Blick nach vorn

Der erfolgreiche Abschluss des ersten Jahres im Fraunhofer Cluster of Excellence CCIT wurde bereits im November 2018 mit dem Fraunhofer-Tag der Kognitiven Internet-Technologien gefeiert. Zahlreiche Vertreter aus Politik und Wirtschaft konnten sich hier über erste Ergebnisse und Projekte informieren. Das nächste Etappenziel des CCIT ist die Stärkung der langfristigen, strategischen und interdisziplinären Zusammenarbeit zwischen den Instituten. Durch die gebündelte Fraunhofer Kompetenz sollen Technologien entwickelt werden, die gemeinsam mit Industriepartnern in die Anwendung überführt werden können. Das langfristige Ziel des Fraunhofer CCIT ist es, der Industrie eine technologische Infrastruktur zu bieten, welche die Unternehmen dabei unterstützt, ihre Produkte, Prozesse und Dienstleistungen zu verbessern und so neue Geschäftsmodelle zu entwickeln, die ihre Wettbewerbsfähigkeit stärken und ihre digitale Souveränität sichern.

www.cit.fraunhofer.de



INDUSTRIAL DATA SPACE

SICHERHEIT FÜR DATENGESTEUERTE GESCHÄFTSÖKOSYSTEME

Durch die fortschreitende digitale Vernetzung von Prozessen und Produkten bei wachsender Größe und Komplexität der mit ihnen verbundenen Informationen werden neue Geschäftsmodelle nicht nur ermöglicht – sie werden im wachsenden Wettbewerbsdruck zur unmittelbaren Notwendigkeit. Der sichere Austausch der Schlüsselressource »Daten« sowie die Möglichkeit ihrer einfachen Kombination in Wertschöpfungsketten sind Voraussetzungen für smarte Services, innovative Leistungsangebote und automatisierte Prozessketten.

Für viele Unternehmen sind mit dem Thema Datenaustausch jedoch noch große Sicherheitsbedenken verbunden. Um diesen und anderen Herausforderungen zu begegnen, startete die Fraunhofer-Gesellschaft im Frühjahr 2015 mit Partnern aus der Industrie und mit der Unterstützung der Bundesregierung (BMBF und BMWi) die Initiative »Industrial Data Spaces« (IDS). Der IDS steht für einen geschützten Datenraum, der Unternehmen verschiedener Branchen und Größen den sicheren und interoperablen Austausch von Daten ermöglicht. Die Souveränität und Authentizität der Daten steht dabei im Mittelpunkt. An diesem Vorhaben sind zwölf Fraunhofer-Institute und mehr als 80 internationale Partner aus Wirtschaft und Wissenschaft beteiligt. Im Zeitraum 2018/2019 wurde dieses Vorhaben entscheidend vorangebracht.

Weiterentwicklung der IDS-Sicherheitsarchitektur und der Referenzimplementierungg

Die Sicherheitsarchitektur ist der wesentliche Beitrag des Fraunhofer AISEC zum IDS. Diese wird permanent weiterentwickelt und erfuhr im letzten Jahr eine Erweiterung um Konzepte für verteiltes Identitätsmanagement, sichere dynamische Attributeverwaltung und neue Protokollerweiterungen für eine entfernte Integritätsüberprüfung und das Metadatenmanagement.

Die zentrale Vertrauensinstanz innerhalb der IDS-Sicherheitsarchitektur ist der »IDS Connector« des Fraunhofer AISEC. Er besteht aus zwei Kompontenten. Die erste ist das hochsichere Betriebssystem »trust|me« mit kleinstmöglicher Trusted Computing Base, das vielfältige Sicherheitsfunktionalitäten wie beispielsweise TPM 2.0, Remote Attestation, ein hoch isoliertes Containermanagement, die Integritätsprüfung aller Komponenten, Full Disk Encryption und Secure Boot unterstützt.

Die zweite Komponente, die Verwaltungskomponente »Trusted Core Container«, wurde um neue Protokolle zur Remote Attestation, also zur entfernten Überprüfung der Integrität einer Komponente wie beispielsweise eines Sensors oder eines IoT-Geräts, sowie ein Metadatenmanagement und Identitätsmanagementkonzepte ergänzt. Außerdem wurde die Kompatibilität zur weiteren IDS-Infrastruktur hergestellt.

Ohne Vertrauen kein Datenaustausch: Standards und Zertifizierungsschema geschaffen

Im Industrial Data Space gibt es keine zentrale Instanz zur Datenhaltung, es existiert vielmehr eine dynamische Verbindung aus Datengebern und Datennutzern. Es gelten jedoch gemeinschaftliche Spielregeln – die Data-Governance-Prinzipien – die die Rechte und Pflichten der Anwender festlegen. Technische Maßnahmen bilden die Basis für die Infrastruktur gegenseitigen Vertrauens, die das Konzept Datensouveränität, für das der IDS steht, mit Leben füllt.

Für Unternehmen, die für einen souveränen Datenaustausch zum Zwecke neuer Wertschöpfungsprozesse von der Referenzarchitektur profitieren wollen, wurde während des letzten Jahres ein Zertifizierungsprozess, der die Vertrauenswürdigkeit von Komponenten und Unternehmen attestieren soll, entwickelt. Grundlage ist die Norm DIN SPEC 27070 für die Referenzarchitektur eines Security-Gateways zum sicheren Austausch von Industriedaten und -diensten, die unter der Mitwirkung der Fraunhofer-Institute AISEC und FOKUS, durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und Unternehmen wie Sick, Siemens, Phoenix Contact im Mai 2019 finalisiert worden ist. Für die Zertifizierung, die der TÜV Süd oder PricewaterhouseCoopers vergeben, prüfen Auditoren die Organisation (Prozesse und Doumentation) oder die Komponenten eines Unternehmens. Die technische Komponentenprüfung übernehmen wiederum die Experten von AISEC und FOKUS. Hier existieren drei Sicherheitslevel: »Base« mit vielfältigen Sicherheitsanforderungen, eine hochsichere Variante »Trust« mit unklonbaren Identitäten und Remote-Attestation, Diensteintegritätsschutz, Secure Boot sowie »Trust+« für Konnektoren, die sogar vor Manipulation durch bösartige Administratoren geschützt sind.

Als Vorbereitung für das breite Ausrollen der Zertifizierungen soll das Label »IDS_ready« Unternehmen einladen, erste Erfahrungen mit dem IDS zu sammeln, und sie so auf die eigentliche Zertifizierung vorbereiten. Das Label haben das Fraunhofer FOKUS und das AISEC gemeinsam definiert. Es stellt sicher, dass Unternehmen oder Organisationen die Anforderungen der IDS-Referenzarchitektur erfüllen oder auf einem nachweisbar guten Weg dorthin sind.

Erste Anwendungsfälle

Der Data Intelligence Hub (DIH), den die Telekom auf der Hannover Messe 2019 präsentiert hat, ist der erste Daten-Marktplatz, für den die Fraunhofer-Institute FOKUS und AISEC die strengen Sicherheitsvorgaben der International Data Spaces Association geprüft haben. Der Trusted DIH-Konnektor ist also die erste Komponente, die IDS_ready geprüft ist. Damit steht ein erprobter Industriestandard zur Verfügung, der dem Datenbesitzer eine kontrollierte Weitergabe von Daten ermöglicht.

Wichtige Meilensteine auf dem Weg zu einem europäischen Modell der Datensouveränität, das eine Alternative zum chinesischen oder amerikanischen Modell der Datenrechte und Datenweitergabe darstellt, sind mit dem IDS also erreicht. Aktuell werden zusammen mit der »International Data Spaces Association« und rund 100 Unternehmen weitere Use Cases auf Basis der von Fraunhofer entworfenen und prototypisch realisierten Rahmenarchitektur umgesetzt. Die Grundidee wird in domänenspezifischen Datenräumen wie dem Medical oder dem Mobility Data Space weiterentwickelt.

LEISTUNGSZENTRUM SICHERE INTELLIGENTE SYSTEME

Ein effektiver Transfer zwischen Forschung und Wirtschaft ist eine wichtige Voraussetzung für die Stärkung der Innovationskraft am Industriestandort Deutschland. Insbesondere durch die zunehmende Digitalisierung der Industrie wächst der Druck auf Unternehmen, eine Digitalisierungsstrategie zu entwickeln und diese konsequent umzusetzen.

Anwendungsorientierte Forschung – vom Sensor in die Cloud

Unternehmen benötigen eine geeignete Plattform, um Konzepte, Technologien und Geräte auszuprobieren, die für die erfolgreiche Umsetzung ihrer Digitalisierungsstrategien notwendig sind. Genau hier setzen die Leistungszentren der Fraunhofer-Gesellschaft an: Im Verbund mit universitären und außeruniversitären Partnern sowie Vertretern aus Industrie und Wirtschaft bearbeiten sie in regionalen Clustern Zukunftsthemen wie »Smart Production«, »Elektroniksysteme« oder »Photonik«. Ziel ist es, durch die enge Vernetzung von Forschung und Industrie ein leistungsfähiges Innovationssystem mit internationaler Bedeutung zu etablieren, Forschungsergebnisse schnell in die Praxis zu überführen und gemeinsam neue Technologien auf den Markt zu bringen.

Das Leistungszentrum Sichere Intelligente Systeme in München

Das Fraunhofer AISEC ist Sprecherinstitut des Leitungszentrums »Sichere intelligente Systeme« (bis Juni 2010 Leistungszentrum »Sichere Vernetzte Systeme«), das eine Plattform für die Digitalisierung in den Schwerpunktbereichen Mobilität, Produktionstechnik und Smart Health bietet. Neben dem Fraunhofer AISEC sind das Fraunhofer EMFT und das Fraunhofer ESK Teil des Leistungszentrums. Forschungspartner sind die TU München und die Universität der Bundeswehr München sowie das Zentrum Digitalisierung.Bayern (ZD.B). Durch die Bündelung der Kompetenzen in einer interdisziplinären Zusammenarbeit entsteht ein einzigartiges Angebot für ein sicheres Internet der Dinge für Unternehmen in der Region.

Die wesentlichen Forschungssäulen des Leistungszentrums sind Intelligente Sensorik, sichere und robuste Vernetzung, Datenanalyse und -verarbeitung sowie integrierte Sicherheit. Im Leistungszentrum werden Standards zur sicheren Vernetzung von Systemen und grundlegende Konzepte zur ingenieurmäßigen Konstruktion nachweislich sicherer Cyber-physischer Systeme erforscht und Lösungen für spezifische Anwendungen zur Produktreife gebracht.

Erfolgreiche Kooperationen mit der Industrie

Ein Beispiel für eine erfolgreiche Zusammenarbeit ist die strategische Kooperation mit dem Vakuumpumpenhersteller Edwards. Sie umfasst die Forschung, Entwicklung und Evaluierung von spezifischen Sensor- und IoT-Technologien. Der Fokus liegt auf der Realisierung von Predictive bzw. Smart Maintenance in spezifischen Anwendungen.

Durch das gemeinsame Angebot aus dem Leistungszentrum profitiert Edwards nicht nur von der langjährigen Erfahrung und Expertise des Fraunhofer EMFT im Bereich Halbleiterfertigung. Die Expertise des Fraunhofer AISEC im Bereich der sicheren Cloud-Anbindung trug dazu bei, Schwachstellen in der »EDcentra«-Technologie von Edwards vor ihrem Roll-out zu identifizieren und sichere Lösungen zu entwickeln.

Erste Ergebnisse der anwendungsorientierten und interdisziplinär ausgerichteten Forschung des Leistungszentrums wurden am 19. Juni 2018 in München präsentiert. Auf der Veranstaltung »Sicher vom Sensor in die Cloud« konnten sich Vertreter aus Forschung und Wirtschaft über aktuelle Projekte informieren, sich direkt mit den Wissenschaftlern über

laufende Projekte im Bereich Predictive and Smart Maintenance austauschen, mögliche Kooperationen diskutieren und so von der gebündelten Kompetenz der vertretenen Fraunhofer-Institute profitieren. Das Fraunhofer AISEC präsentierte an verschiedenen Demonstratoren die Expertise im Bereich sicherer Datenaustausch und Datensouveränität.

Interdisziplinärer Wissenstransfer

Neben der kooperativen Zusammenarbeit mit der Industrie findet im Leistungszentrum Sichere intelligente Systeme auch der interdisziplinäre Wissenstransfer zwischen unterschiedlichen Instituten statt. So entwickeln Forschende des Fraunhofer AISEC und des Fraunhofer EMFT gemeinsam eine PUF-basierte physische Schutzfolie für Hochsicherheitsanwendungen. Elektronische Systeme in Hochsicherheitsanwendungen werden mit Sensorfolien umhüllt, um Manipulationen und Zugriffe von außen zu detektieren. Dazu wurden sie bisher kontinuierlich durch batteriegepufferte Schaltungen überwacht. Im Leistungszentrum wird aktuell ein innovativer, batterieloser Ansatz erforscht: Nach dem Start prüft sich das Gerät selbst, initialisiert und generiert aus den physikalischen Eigenschaften der Folie eine elektronischen Schlüssel, der für die sichere Identifikation und Datenübertragung genutzt wird.

Neue Partner ergänzen das Leistungszentrum

In der aktuell beantragten zweiten Förderphase des Leistungszentrums wird das Konzept weiterentwickelt. Neben den Instituten der Phase 1 werden nun weitere anwendungsorientierte Fraunhofer-Institute aus dem Raum um München einbezogen: Das IVV in Freising befasst sich mit Lebensmittelverpackungen, das IBP in Holzkirchen mit Bauphysik und das IGCV in Garching mit Gießereitechnik. All diese Bereiche stehen vor großen Änderungen durch die Digitalisierung. Als Verbund aus Anwendungsinstituten und Technologieinstituten kann das Leistungszentrum hier wertvolle Beiträge zur schnellen Umsetzung von intelligenten Digitalisierungslösungen leisten. So entwickelt sich das Leistungszentrum weiter von »vernetzten« zu »intelligenten« Systemen.

Ein neu eingerichteter Showroom am Fraunhofer EMFT bietet allen Interessierten ganzjährig die Gelegenheit, das Zusammenspiel der verschiedenen Fachdomänen und aktuelle Projekte des LZSiS näher kennenzulernen. Dieser wurde am 11. Juni 2019 von Staatssekretär Roland Weigert feierlich eröffnet.

Umfassende Sicherheit für vernetzte Systeme

Die mit der Verbreitung von intelligenter Sensorik und deren Vernetzung einhergehende Digitalisierung unserer Welt ist ein zukunftsträchtiges Forschungsfeld. Die Sicherheit der entstehenden Systemkomplexe und der generierten Daten gegen Cyberangriffe ist dabei eine grundlegende Voraussetzung, aber auch eine besondere Herausforderung. Das Leistungszentrum Sichere intelligente Systeme bietet mit dem Kompetenzpaket aus Hardwaresicherheit, Betriebssicherheit und Datensicherheit ein vollständiges Leistungsangebot zur Entwicklung sicherer vernetzter Systeme an.

Das Leistungszentrum Sichere intelligente Systeme ist offen für Kooperationen mit weiteren Forschungseinrichtungen, um das Partnernetzwerk weiter auszubauen. Gefördert und finanziert wird das Leistungszentrum vom Bayerischen Staatsministerium für Wirtschaft und Medien, Energie und Technologie, von der Fraunhofer-Gesellschaft e.V. und von Industriepartnern, die sich in gemeinsamen Projekten engagieren.

Lernlabor **Cybersicherheit**

DIGITALISIERUNG BRAUCHT IT-SICHERHEIT

Nur wer die Grundlagen von Systemen versteht, kann sich vor Angreifern schützen, die die Schwächen eben dieser Systeme ausnutzen wollen. Doch gerade im Bereich der Informations- und Kommunikationstechnologien beträgt die Halbwertzeit von Fachwissen lediglich eineinhalb Jahre. Zudem ändert sich die Bedrohungslage permanent. Sicherheitsexperten, Fachkräfte und Spezialisten, aber auch Führungskräfte und Anwender müssen und sich immer neu mit dem Thema IT-Sicherheit auseinandersetzen und ihre Expertise erweitern.

Die Fraunhofer-Gesellschaft reagiert in Zusammenarbeit mit ausgewählten Fachhochschulen auf diesen Bedarf: Unter dem Dach der Fraunhofer Academy wurde mit dem Kooperationsverbund »Lernlabor Cybersicherheit« ein modulares, berufsbegleitendes Weiterbildungskonzept für IT-Sicherheit geschaffen, das vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wird. Praxisnah und forschungsorientiert werden hier aktuelle Kenntnisse rund um das Thema IT-Sicherheit vermittelt.

Praxisnah und forschungsorientiert – für Anwender, Experten und Entscheider

Das Besondere am Weiterbildungsprogramm des Lernlabors Cybersicherheit ist charakteristisch für Fraunhofer: Die hohe Anwendungsorientierung, die in der Forschung der Institute der Fraunhofer-Gesellschaft gelebt wird, spiegelt sich auch in den Seminaren wider. Aktuelle Forschungsergebnisse können aus erster Hand weitergegeben werden und auf die Bedürfnisse der Seminarteilnehmer adaptiert in die Seminare einfließen. Die Lerninhalte sind so konzipiert, dass die Teilnehmenden realen Bedrohungsszenarien gegenüberstehen und aktuelle Forschungsergebnisse und Lösungskonzepte direkt praktisch anwenden können.

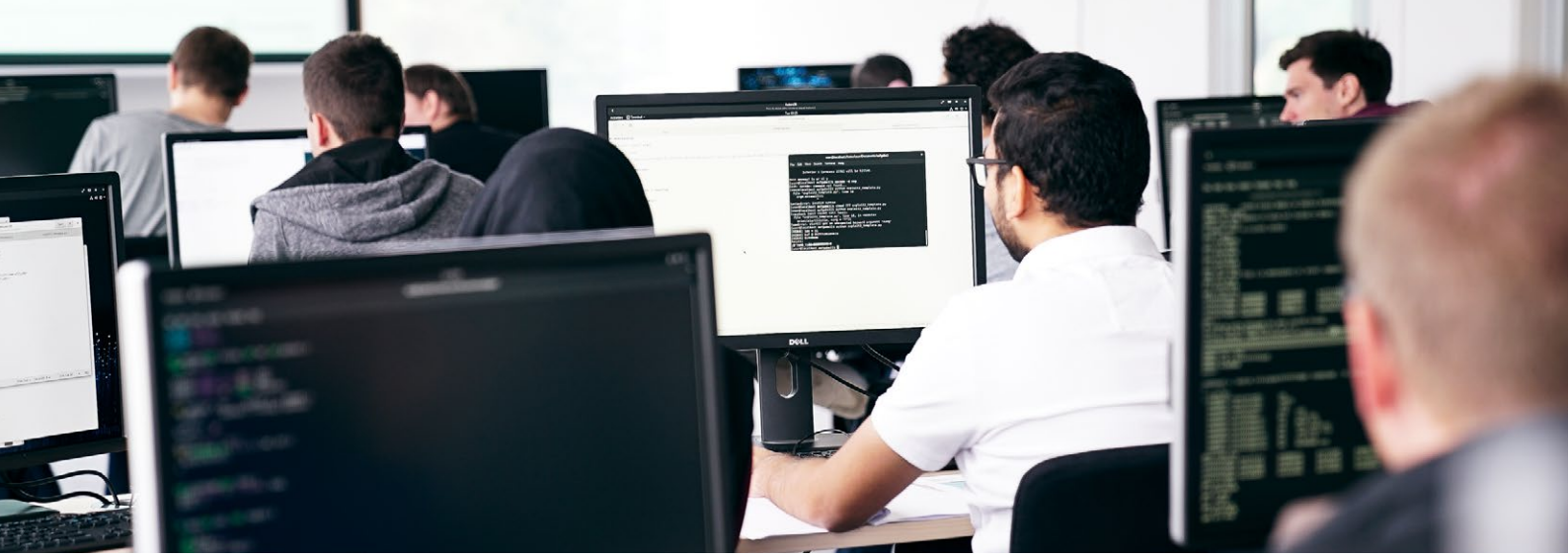
Das Fraunhofer AISEC engagiert sich im Lernlabor-Konsortium »Embedded Systems, Mobile Security und Internet of Things«. Kooperationspartner sind das Fraunhofer IIS, die OTH Amberg-Weiden sowie die Hochschule Aalen. Das Konsortium bietet Schulungen an zahlreichen Standorten in Deutschland, in hochwertigen Laboren erhalten Schulungsteilnehmer kompakte Qualifizierungen. Für das Fraunhofer AISEC ist das Engagement im Lernlabor Cybersicherheit Teil seiner Mission, das Wissen rund um Cybersicherheit an die Gesellschaft weiterzugeben und einem großen Anwenderkreis zur Verfügung zu stellen.

Hohe Nachfrage bei Blockchain, Hacking und Automotive Security

Die Lerninhalte werden bei jeder Schulung branchen-, themen- und funktionsspezifisch auf die Bedarfe der Teilnehmer aus Wirtschaft und Behörden angepasst. Auch das thematische Angebot kann vom Lernlabor Cybersicherheit komplett entsprechend der Wünsche der Kunden, die die Schulungen teilweise mit Teambuilding-Maßnahmen flankieren, adaptiert werden.

Insgesamt neun Schulungen wurden in den letzten 18 Monaten vom Konsortium »Embedded Systems, Mobile Security und Internet of Things« durchgeführt. Auf besonders großes Interesse stießen Weiterbildungsangebote zu den Themen Blockchain, Hacking und Automotive Security. Seit 2019 werden auch Schulungen zu Maschinellem Lernen angeboten.

Seit Ende Mai ist das neue Kursangebot verfügbar unter **www.aisec.fraunhofer.de/lernlabor**



»Das Seminar ›Maschinelles Lernen für mehr Sicherheit‹ empfand ich als einen rundum großartig organisierten Schulungstag. Besonders das umfangreiche Themenspektrum sowie die sehr kompetenten Referenten mit offenkundiger Praxiserfahrung haben mich überzeugt. Die erlernten Methodiken habe ich bereits bei eigenen Problemstellungen im Unternehmen anwenden können.«

Kevin Beck, Specialist Data Analytics, Giesecke&Devrient

»Die Security-Expertise des AISEC im Weiterbildungsprogramm des Lernlabor Cybersicherheit ist ein wertvolles Angebot für jedes Unternehmen, das seine Mitarbeiter für aktuelle Bedrohungen sensibilisieren und für zukünftige Herausforderungen rüsten möchte. Die Schulungsinhalte des Workshops ›Binary Exploitation‹ waren perfekt auf das in unserer Organisation vorhandene Wissensniveau angepasst. Durch den praktischen Teil in jeder Session wurden aus neuen Wissenseinheiten unmittelbar neue Fertigkeiten, auf die im Arbeitsalltag sofort zurückgegriffen werden konnte. Eine nachhaltig gewinnbringende Schulung für die Arbeit in meiner Abteilung.«

Mario Hoffmann, Head of Security & Privacy Consulting, Continental

PROMOTIONEN 2018/2019

Am Fraunhofer AISEC räumen wir dem Thema Promotion der Mitarbeiter einen sehr hohen Stellenwert ein. Dieser lässt sich aufgrund unserer jungen Institutsgeschichte noch nicht an der Zahl der bereits abgeschlossenen Promotionen ablesen. Allerdings spricht die Zahl derjenigen, die aktuell eine Promotion anstreben, für sich: Rund 69 Prozent unserer wissenschaftlichen Mitarbeiter unterhalb der Management-Ebene arbeiten aktuell an einer Dissertation. Insgesamt sind 79 Prozent der wissenschaftlichen Mitarbeiter ohne Führungsverantwortung bereits promoviert oder promovierend.

Im Zeitraum 2018/2019 wurden folgende **Promotionen** abgeschlossen:

- Fabrizio DeSantis. „Algorithmic and Protocol Level Countermeasures to Protect". 2018.
  Doktorvater: Prof. Dr.-Ing. Georg Sigl
- Ralph Nyberg. „New Techniques for Emulating Fault Attacks". 2018.
  Doktorvater: Prof. Dr.-Ing. Georg Sigl
- Hermann Seuschek. „Cryptographic Devices". 2018.
  Doktorvater: Prof. Dr.-Ing. Georg Sigl
- Philipp Stephanow-Gierach. „Continuous Test-based Certification of Cloud Services". 2018.
  Doktormutter: Prof. Dr. Claudia Eckert
- Steffen Wagner. „Implicit Remote Attestation of Microkernel-based Embedded Systems". 2018.
  Doktormutter: Prof. Dr. Claudia Eckert
- Konstantin Böttinger. „Fuzzing with Stochastic Feedback Processes". 2019.
  Doktormutter: Prof. Dr. Claudia Eckert
- Philipp Koppermann. „Curve Based Cryptography: High-Performance Implementations and Speed Enhancing Methods". 2019.
  Doktorvater: Prof. Dr.-Ing. Georg Sigl
- Dennis Titze. „Analysis and Mitigation of Security Issues on Android". 2019.
  Doktormutter: Prof. Dr. Claudia Eckert

MASTERARBEITEN 2018/2019

Durch die enge Zusammenarbeit mit Exzellenz-Universitäten wie der TU München und der FU Berlin werden am Fraunhofer AISEC zahlenreiche Abschlussarbeiten betreut. Die Studierenden profitieren nicht nur von der Reputation und der fachlichen Expertise einer weltweit anerkannten Forschungseinrichtung, sondern auch von der Nähe zu spannenden Industrieprojekten und der Möglichkeit, Forschungsergebnisse auf internationalen Konferenzen zu publizieren. Viele Absolventen haben nach dem erfolgreichen Abschluss des Studiums ihre Forschung als Mitarbeiter des AISEC weitergeführt.

Masterarbeiten

- Adversarial Machine Learning on Capsule Theory
- An Automotive Real-Time Highly Configurable and Fault Tolerant Block-Cipher Concept
- Analysing the Robustness of Memory Augmented Neural Networks
- Analysis of the Wireless Security of an Insulin Pump System
- Analyzing the Robustness of Memory Augmented Neural Networks
- Anomaly Detection In Generative Adversarial Networks
- Anomaly Detection using Generative Adversarial Networks
- Avoiding smart contract vulnerabilites: An inter-contract concolic execution framework for Ethereum contracts
- Burst Eviction: Optimizing Cache Attacks on ARM Cortex-A Processors
- Cryptographic Key Establishment from Physical Smartphone Data
- Data Flow Analysis of EVM Smart Contracts
- Designing Privacy-Preserving Edge Services in the Automotive Domain
- Development of an IT Security Map based on Covert Channels
- Evaluation of Laser Fault Injection on different ARM Cortex-M Microcontrollers
- FPGA Implementations of the CAESAR Candidate Norx with an Error Detecting Control Path

MASTERARBEITEN 2018/2019

Masterarbeiten (Fortsetzung)

- HW/SW-Codesign of CAESAR Authenticated Encryption with Associated Data Building Blocks
- Implementation of an Optimised Navigation Message Authentication Scheme without Performance Degradation
- Improving Sequential Gate-level Netlist Reverse Engineering and Obfuscation
- Investigationof Portability of Cryptographic Algorithms on a Space-borne New-Generation Architecture
- Modellierung und Überprüfung von Security Policies zur Autorisierung von ausgewählten Cloud-Infrastrukturdiensten
- On Using Machine Learning to break obfuscation circuits by golden model identification
- Security Analysis of LWE-based Post-Quantum Cryptography
- Side-Channel Aware Fuzzing
- System Evaluation of CAESAR using the example of Deoxys
- Understanding TBR PUF: State Trajectory Analysis on an FGPA Array

BACHELORARBEITEN 2018/2019

Bachelorarbeiten

- AntiPatterns bei der Anwendung von CryptoPrimitiven am Beispiel von Ransomware
- Aufbau sicheres Bluetooth Mesh Netzwerk und Sicherheitsanalyse
- Backward-Edge Protection against Code Reuse Attacks on Embedded MIPS Devices
- Design and Implementation of a High-Level Toolkit for Non-Interactive Zero-Knowledge Proofs
- Detective technologies on adversarial examples
- Development of a Hardware in the Loop based Testbed to generate fieldbus communication
- Dezentrale Datenverteilung mit TPM-basierter Authentifizierung
- Evaluation of denfense strategies for face recognition system
- Forward and Backward Privacy in Dynamic Searchable Encryption
- Garbled Circuit Generation for Private Set Intersection
- Implementation of a Semantic Attack Vector Modeling Framework for the Smart Grid
- Privacy-preserving linear models over homomorphically encrypted data
- Return-Oriented Programming on RISC-V
- Security Analysis and Extension of Embedded Operating Systems
- Security Analysis of the ARM Mbed uVisor and Implementation of a generally usable Cryptographic Service Application
- Security Measures and Attacks on Video Game Consoles by the Example of the Nintendo Switch
- Security Measures and Attacks on Video Game Consoles by the Example of the Xbox One

VORTRÄGE 2018/2019

Die Ergebnisse ihrer Forschung präsentieren die Mitarbeiterinnen und Mitarbeiter des Fraunhofer AISEC unter anderem auf zahlreichen nationalen und internationalen Veranstaltungen. Als hoch spezialisierte Ansprechpartner repräsentieren sie das Institut als Speaker auf Fachmessen und Kongressen und halten Vorträge zu aktuellen Forschungsergebnissen rund um das Thema angewandte und integrierte Sicherheit.

Vorträge

- Daniel Angermeier, Till Fischer. "IT-Sicherheitsrisiken erkennen, bewerten und vorbeugen". At: Embedded Software Engineering Kongress, Sindelfingen, 2018.
- Christian Banse. "Establishing Continuous Security in Multi-Cloud Environments". At: International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE-2019), Capri, 2019.
- Christian Banse. "Kontinuierliche Sicherheit in der Cloud". At: Netzwerk „Industrie 4.0", Sonthofen, 2018.
- Christian Banse. "Presenting Clouditor in the EUSEC Pilot". At: EUSEC - Workshop on Continuous Audit Based Certification, Barcelona, 2019.
- Gerd Brost. "A security gateway for industrial automation and DIN SPEC". At: IDS Winter Days, Berlin, 2018.
- Gerd Brost. "Industrial Data Space: Trust & Security in the IDS". At: 1st IDSA Webinar Sequel, 2018.
- Gerd Brost. "Security in IIoT and the Industrial Dataspace". At: International Manufacturing Technology Show, Chicago, 2018.
- Gerd Brost. "Security in the Industrial Dataspace". At: Hannover Messe, Hannover, 2018.
- Gerd Brost. "Technische Absicherung von rechtlichen Aspekten im IIoT". At: Plattformen: Ein Einstieg in Industrial IoT, Landshut, 2018.
- Bartol Filipovic. "Risikomanagement der Cyber-Sicherheit in der Supply Chain". At: Zukunftskongress Logistik, Dortmund, 2018.
- Bartol Filipovic. "Vorstellung des wissenschaftlichen Begleitprojektes IUNO Insec". At: Sichere Industrie 4.0 in der Praxis, Berlin, 2018.
- Bartol Filipovic. "Aktuelle Fördermittel für Sichere Industrie 4.0 - DIE Chance für Produktionsfirmen und Systemintegratoren". At: Cluster für Mechatronik und Automation: Kickoff Security in der Produktion - Hilfe zur Selbsthilfe, Augsburg, 2018.

VORTRÄGE 2018/2019

- Matthias Hiller. "Creating Trust between the Physical and the Digital World". At: Digital Future Science Match, Berlin, 2018.
- Daniel Loebenberger. "Chancen und Risiken der Digitalisierung". At: Cybersicherheit - IT-Sicherheit im Berufs- und Lebensalltag, Kemnath, 2019.
- Daniel Loebenberger. "Geschäftsmodelle in der digitalen Welt: von Cyber-Kriminellen und deren Abwehr". At: Gastvortragsprogramm "Geschäftsmodelle in der digitalen Welt", Budapest, 2019.
- Daniel Loebenberger. "Podium: Wissen wirksam machen – wie gelingt der Transfer?". At: 28. Cyber-Sicherheits-Tag, München, 2019.
- Sven Plaga. "Projekt IUNO – Sicherheit in der Industrie". At: VDE Tec Summit, Berlin, 2018.
- Martin Schanzenbach. "Blockchain for cyber security". At: Fraunhofer Venture Meet'n'Mingle, München, 2018.
- Martin Schanzenbach. "Blockchain for Education". At: Fraunhofer Academy Open Discussion 2018, München, 2018.
- Martin Schanzenbach. "reclaimID: Self-sovereign, decentralized identity management using secure name systems". At: Internet Engineering Task Force (IETF 104), Prague, 2019.
- Julian Schütte. "LUCON-Policy-Gateway und Secure Backend als Voraussetzung für die Datennutzungskontrolle im IoT". At: IoT-Security-Kongress, München, 2018.
- Julian Schütte. "TrackChain: Datenschutzfreundliche Logistik-Anwendungen auf der Blockchain". At: Praxisforum Blockchain, Munich, 2019.
- Philipp Stephanow-Gierach. "Kontinuierliche Sicherheit in der Cloud". At: ZD.B Sicher in die Cloud, München, 2019.
- Huang Xiao. "Machine Learning from a IT Security Perspective". At: Digital Future Science Match, Berlin, 2018.

VERÖFFENTLICHUNGEN UND KONFERENZEN

Wissenschaftliche Publikationen zählen zu den wichtigsten Wissenschaftsindikatoren in der Forschung und bilden die Grundlage für die Entwicklung neuer, innovativer Technologien. Das hohe Forschungsengagement am Fraunhofer AISEC spiegelt sich wider in einer gemessen an seiner Größe und seinem Alter sehr hohen Anzahl an Veröffentlichungen, die im Rahmen von nationalen und internationalen Konferenzen entstanden sind. Aktuellen Fragestellungen widmen sich die Wissenschaftlerinnen und Wissenschaftler des AISEC dabei auch in enger Zusammenarbeit mit Forschenden anderer Disziplinen.

2018

- Konstantin Böttinger, Rishabh Singh, and Patrice Godefroid. "Deep Reinforcement Fuzzing". In: IEEE Symposium on Security and Privacy Workshops 2018, 2018.

- Georg Bramm, Mark Gall, and Julian Schütte. "BDABE - Blockchain-based Distributed Attribute Based Encryption". In: Proceedings of the International Conference on Security and Cryptography (SECRYPT). 2018.

- Tilo Fischer. "Testing Cryptographically Secure Pseudo Random Number Generators with Artificial Neural Networks". In: 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). TrustCom '18. Newark, New Jersey: IEEE, 2018, pp. 1214–1223. DOI: 10.1109/TrustCom/BigDataSE.2018.00168, 2018.

- Manuel Huber Gerd S. Brost, Julian Schütte Michael Weiß Mykolai Protsenko, and Sascha Wessel. "An Ecosystem and IoT Device Architecture for Building Trust in the Industrial Data Space". In: CPSS'18: The 4th ACM CyberPhysical System SecurityWorkshop. CPSS'18. Incheon, Republic of Korea: ACM, 2018, pp. 39–50. ISBN: 9781450357555. DOI: 10.1145/3198458.3198459. URL: https://doi.org/10.1145/3198458.3198459.

- Alexander Giehl and Sven Plaga. "Implementing a Performant Security Control for Industrial Ethernet". In: 2018 International Conference on Signal Processing and Information Security. Dubai, United Arab Emirates: IEEE, 2018. DOI: 10.1109/CSPIS.2018.8642758. URL: https: //doi.org/10.1109/CSPIS.2018.8642758.

- Alexander Giehl and Norbert Wiedermann. "Security verification of third party design files in manufacturing". In: 2018 10th International Conference on Computer and Automation Engineering Proceedings. Best Presentation Award. Brisbane, Australia: ACM, 2018. ISBN: 9781450364102/18/02. DOI: 10.1145/3192975.3192984.

- Wolfgang Gräther, Sabine Kolvenbach, Rudolf Ruland, Julian Schütte, Christof Torres, and Florian Wendland. "Blockchain for Education: Lifelong Learning Passport". In: Proceedings of 1st ERCIM Blockchain Workshop 2018. Reports of the European Society for Socially Embedded Technologies: vol. 2, no. 10. European Society for Socially Embedded Technologies (EUSSET), 2018.

- Norman Hänsch, Andrea Schankin, Mykolai Protsenko, Felix Freiling, and Zinaida Benenson. "Programming Experience Might Not Help in Comprehending Obfuscated Source Code Efficiently". In: Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). Baltimore, MD: USENIX Association, 2018, pp. 341–356. ISBN: 9781931971454. URL: https://www.usenix.org/conference/soups2018/presentation/hansch.

- Robert Hesselbarth, Florian Wilde, Chongyan Gu, and Hanley Neil. "Large Scale RO PUF Analysis over Slice Type, Evaluation Time and Temperature on 28nm Xilinx FPGAs". In: IEEE International Symposium on Hardware Oriented Security and Trust (HOST). Washington DC, USA, 2018.

- Stefan Hristozov, Johann Heyszl, Steffen Wagner, and Georg Sigl. "Practical Runtime Attestation for Tiny IoT Devices". In: NDSS Workshop on Decentralized IoT Security and Standards (DISS) 2018, San Diego, CA, USA. 2018. ISBN: 1891562517. DOI: https://dx.doi.org/10.14722/diss.2018.23011. URL: www.ndss-symposium.org.

- Manuel Huber, Julian Horsch, Junaid Ali, and Sascha Wessel. "Freeze and Crypt: Linux Kernel Support for Main Memory Encryption". In: Computers & Security (2018). ISSN: 01674048. DOI: 10.1016/j.cose.2018.08.011. URL: http://www.sciencedirect.com/science/article/pii/S0167404818310435.

- Vincent Immler, Matthias Hiller, Qinzhi Liu, Andreas Lenz, and Antonia Wachter-Zeh. "Variable-Length Bit Mapping and Error Correcting Codes for Higher-Order Alphabet PUFs". In: Journal of Hardware and Systems Security (HASS) 2.4, 2018.

- Vincent Immler, Johannes Obermaier, Martin König, Matthias Hiller, and Georg Sigl. "B-TREPID: Batteryless Tamper-Resistant Envelope with a PUF and Integrity Detection". In: IEEE International Symposium on Hardware Oriented Security and Trust (HOST). 2018, pp. 49–56.

- Vincent Immler, Robert Specht, and Florian Unterstein. "Your rails cannot hide from localized EM: how dual-rail logic fails on FPGAs—extended version". In: Journal of Cryptographic Engineering (2018).

- Anatoli Kalysch, Oskar Milisterfer, Mykolai Protsenko, and Tilo Müller. "Tackling Androids Native Library Malware with Robust, Efficient and Accurate Similarity Measures". In: Proceedings of the 13th International Conference on Availability, Reliability and Security. ARES 2018. Hamburg, Germany: ACM, 2018, 58:1–58:10. ISBN: 9781450364485. DOI: 10.1145/3230833.3232828.

- Stephan Kleber, Florian Unterstein, Matthias Hiller, Frank Slomka, Matthias Matousek, Frank Kargl, and Christoph Bösch. "Secure Code Execution: A Generic PUF-driven System Architecture". In: Information Security Conference (ISC). Ed. by Liqun Chen and Mark Manulis. LNCS. Springer, 2018.

- Philipp Koppermann, Fabrizio De Santis, Johann Heyszl, and Georg Sigl. "Fast FPGA Implementations of Diffie-Hellman on the Kummer Surface of a Genus-2 Curve". In: IACR Trans. Cryptogr. Hardw. Embed. Syst. 2018.1 (2018), pp. 1–17. DOI: 10.13154/tches.v2018.i1.1-17.

VERÖFFENTLICHUNGEN UND KONFERENZEN

2018 (Fortsetzung)

- Matthias Niedermaier, Thomas Hanka, Sven Plaga, Alexander von Bodisco, and Dominik Merli. "Efficient Passive ICS Device Discovery and Identification by MAC Address Correlation". In: Proceedings of the 5th International Symposium for ICS & SCADA Cyber Security Research 2018. Electronic Workshops in Computing (eWiC). Zusammenarbeit mit der Hochschule Augsburg – Status: präsentiert auf der ICSCSR 2018/Hamburg (colocated with ARES 2018). Hamburg: British Computer Society Learning & Development Ltd., 2018. URL: https://ewic.bcs.org/category/19361.

- Mathias Morbitzer, Manuel Huber, Julian Horsch, and Sascha Wessel. "SEVered: Subverting AMD's Virtual Machine Encryption". In: Proceedings of the 11th European Workshop on Systems Security. EuroSec'18. Porto, Portugal: ACM, 2018. ISBN: 9781450356527. DOI: 10.1145/3193111.3193112.

- Johannes Obermaier, Florian Hauschild, Matthias Hiller, and Georg Sigl. "An Embedded Key Management System for PUF-based Security Enclosures". In: 2018 7th Mediterranean Conference on Embedded Computing (MECO). 2018, pp. 1–6. DOI: 10.1109/MECO.2018.8406028.

- Johannes Obermaier and Vincent Immler. "The Past, Present, and Future of Physical Security Enclosures: From Battery-Backed Monitoring to PUF-Based Inherent Security and Beyond". In: Journal of Hardware and Systems Security 2.4 (2018), pp. 289–296. ISSN: 25093436. DOI: 10.1007/s41635-018-0045-2.

- Johannes Obermaier, Vincent Immler, Matthias Hiller, and Georg Sigl. "A Measurement System for Capacitive PUF-based Security Enclosures". In: Proceedings of the 55th Annual Design Automation Conference. DAC '18. San Francisco, California: ACM, 2018, 64:1–64:6. ISBN: 9781450357005. DOI: 10.1145/3195970.3195976.

- Sven Plaga, Melanie Niethammer, Norbert Wiedermann, and Alexander Borisov. "Adding Channel Binding for an Out-of-Band OTP Authentication Protocol in an Industrial Use-Case". In: Proceedings of the 1st International Conference on Data Intelligence and Security. ICDIS '18. Kooperation im Rahmen von IUNO AP4, Fraunhofer AISEC mit BOSCH Corporate Sector Research and Advance Engineering submitted to „The 1st International Conference on Data Intelligence and Security". South Padre Island, Texas, USA: IEEE, 2018. ISBN: 9781538657621. DOI: 10.1109/ICDIS. 2018.00048.

- Sven Plaga, Norbert Wiedermann, Hansch Gerhard, and Newe Thomas. "Secure your SSH Keys! – Motivation and Practical Implementation of a HSM-based Approach Securing Private SSH-Keys". In: Proceedings of the 17th European Conference on Cyber Warfare and Security. ECCWS '18. University of Oslo, Norway: Academic Conferences and Publishing International (ACPI) Limited, 2018, pp. 370–379. ISBN: 9781911218852.

- Cezar Reinbrecht, Bruno Forlin, Andreas Zankl, and Johanna Sepúlveda. "Earthquake - A NoC-based optimized differential cache-collision attack for MPSoCs". In: 2018 Design, Automation & Test in Europe Conference & Exhibition, DATE 2018, Dresden, Germany, March 19-23, 2018. IEEE, 2018, pp. 648–653. ISBN: 9783981926309. DOI: 10.23919/DATE.2018.8342090.

- Sven Plaga, Norbert Wiedermann, Matthias Niedermaier, Alexander Giehl, and Thomas Newe. "Future Proofing IoT Embedded Platforms for Cryptographic Primitives Support". In: 12th International Conference on Sensing Technology 2018. ICST'18. University of Limerick, Ireland: Institute of Electrical and Electronics Engineers (IEEE), 2018, pp. 52–57. DOI: 10.1109/ICSensT.2018.8603610.

- Martin Schanzenbach, Christian Banse, and Julian Schütte. "Practical Decentralized Attribute-Based Delegation using Secure Name Systems". In: Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Aug. 2018.

- Martin Schanzenbach, Georg Bramm, and Julian Schütte. "reclaimID: Secure, Self-Sovereign Identities using Name Systems and Attribute-Based Encryption". In: Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Aug. 2018.

- Peter Schneider and Konstantin Böttinger. "High-Performance Unsupervised Anomaly Detection for Cyber-Physical System Networks". In: Proceedings of the 2018 Workshop on CyberPhysical Systems Security and PrivaCy. CPSSPC '18. Toronto, Canada: ACM, 2018, pp. 1–12. ISBN: 9781450359924. DOI: 10.1145/3264888.3264890.

- Julian Schütte and Gerd Brost. "LUCON: Data Flow Control for Message-Based IoT-Systems". In: Proceedings of the International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). Aug. 2018.

- Bodo Selmke, Kilian Zinnecker, Philipp Koppermann, Katja Miller, Johann Heyszl, and Georg Sigl. "Locked out by Latch-up? An Empirical Study on Laser Fault Injection into Arm Cortex-M Processors". In: 2018 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2018, Amsterdam, The Netherlands, September 13, 2018. IEEE Computer Society, 2018, pp. 7–14. DOI: 10. 1109/FDTC.2018.00010.

- Dominique Seydel, Gereon Weiß, Daniela Pöhn, Sascha Wessel, and Franz Wenninger. "Safety & Security Testing of Cooperative Automotive Systems". In: Embedded World Conference 2018 (2018). Ed. by WEKA Fachmedien.

- Florian Unterstein, Johann Heyszl, Fabrizio De Santis, Robert Specht, and Georg Sigl. "High-Resolution EM Attacks Against Leakage-Resilient PRFs Explained - And An Improved Construction". In: Cryptographers Track RSA Conference (CTRSA 2018). Springer. 2018.

VERÖFFENTLICHUNGEN UND KONFERENZEN

2018 (Fortsetzung)

- Samuel Weiser, Andreas Zankl, Raphael Spreitzer, Katja Miller, Stefan Mangard, and Georg Sigl. "DATA – Differential Address Trace Analysis: Finding Address-based Side-Channels in Binaries". In: 27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018, pp. 603–620. ISBN: 9781931971461. URL: https://www.usenix.org/conference/usenixsecurity18/presentation/weiser.

- Florian Wendland and Christian Banse. "Enhancing NFV Orchestration with Security Policies". In: ARES 2018: International Conference on Availability, Reliability and Security, August 27–30, 2018, Hamburg, Germany. New York, NY, USA: ACM, 2018. ISBN: 9781450364485/18/08. DOI: 10.1145/3230833.3233253.

- Norbert Wiedermann and Sven Plaga. "Rowhammer – A Survey Assessing the Severity of this Attack Vector". In: Proceedings of the 2018 Embedded World Conference. EWC '18. Nuermberg, Germany: WEKA Fachmedien, Feb. 2018. ISBN: 9783645501736.

- Philipp Zieris and Julian Horsch. "A Leak-Resilient Dual Stack Scheme for Backward-Edge Control-Flow Integrity". In: Proceedings of the 2018 ACM Asia Conference on Computer and Communications Security. ASIA CCS '18. Incheon, Republic of Korea: ACM, June 2018. ISBN: 9781450355766. DOI: 10.1145/3196494.3196531.

2019

- Lukas Auer, Christian Skubich, and Matthias Hiller. "A Security Architecture for RISC-V based IoT Devices". In: Design, Automation & Test in Europe Conference & Exhibition (DATE). 2019.

- Alexander Giehl, Norbert Wiedermann, and Sven Plaga. "A framework to assess impacts of cyber attacks in manufacturing". In: 2019 11th International Conference on Computer and Automation Engineering Proceedings. Perth, Australia: ACM, 2019. ISBN: 9781450362870. DOI: 10.1145/3313991.3314003.

- Michael Gruber and Bodo Selmke. "Differential Fault Attacks on KLEIN". In: Constructive Side-Channel Analysis and Secure Design - 10th International Workshop, COSADE 2019, Darmstadt, Germany, April 3-5, 2019, Proceedings. Ed. by Ilia Polian and Marc Stöttinger. Vol. 11421. Lecture Notes in Computer Science. Springer, 2019, pp. 80–95. DOI: 10.1007/978-3-030-16350-1_6.

- Gerhard Hansch, Peter Schneider, and Gerd Brost. "Deriving Impact-driven Security Requirements and Monitoring Measures for Industrial IoT". In: 5th ACM Cyber-Physical System Security Workshop. CPSS '19. Auckland, New Zealand: ACM, July 2019. ISBN: 9781450367875/19/07. DOI: 10.1145/3327961.3329528.

- Gerhard Hansch, Peter Schneider, Kai Fischer, and Konstantin Böttinger. "A Unified Architecture for Industrial IoT Security Requirements in Open Platform Communications". In: 24th IEEE Conference on Emerging Technologies and Factory Automation. ETFA '19. Zaragoza, Spain: IEEE, Sept. 2019.

- Vincent Immler, Johannes Obermaier, Kuan Kuan Ng, Fei Xiang Ke, Jin Ju Lee, Yak Peng Lim, Wie Koon Oh, Keng Hoong Wee, and Georg Sigl. "Secure Physical Enclosures from Covers with Tamper-Resistance". In: IACR Transactions on Cryptographic Hardware and Embedded Systems 2019.1, 2019.

- Vincent Immler and Karthik Uppund. "New Insights to Key Derivation for Tamper-Evident Physical Unclonable Functions". In: IACR Transactions on Cryptographic Hardware and Embedded Systems (2019), pp. 30–65, 2019.

- Dorian Knoblauch and Christian Banse. "Reducing implementation efforts in continuous auditing certification via an Audit API". In: 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). 2019.

- Mathias Morbitzer. "Scanclave: Verifying Application Runtime Integrity in Untrusted Environments". In: 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE). 2019.

VERÖFFENTLICHUNGEN UND KONFERENZEN

2019 (Fortsetzung)

- Mathias Morbitzer, Manuel Huber, and Julian Horsch. "Extracting Secrets from Encrypted Virtual Machines". In: Proceedings of the Ninth ACM on Conference on Data and Application Security and Privacy. CODASPY '19. Richardson, Texas, USA: ACM, 2019, p. 10. ISBN: 9781450360999. DOI: 10.1145/3292006.3300022.

- N. Müller, P. Debus, D. Kowatsch, and K. Böttinger. "Distributed Anomaly Detection of Single Mote Attacks in RPL Networks". In: 16th International Conference on Security and Cryptography (SECRYPT). 2019.

- N. Müller, D. Kowatsch, P. Debus, D. Mirdita, and K. Böttinger. "A Privacy Policy Dataset for GDPR compliance". In: 22nd International Conference on Text Speech and Dialogue (TSD). 2019.

- N. Müller and K. Markert. "Identifying Mislabeled Instances in Classification Datasets". In: 2019 International Joint Conference on Neural Networks (IJCNN). 2019.

- Sven Plaga, Norbert Wiedermann, Simon Duque Anton, Stefan Tatschner, Hans Schotten, and Thomas Newe. "Securing future decentralised industrial IoT infrastructures: Challenges and free open source solutions". In: Future Generation Computer Systems 93 (2019). Ergebnispräsentation im Rahmen von IUNO AP4 in der April 2019 Ausgabe des Elsevier Future Generation Computer Systems Journal, pp. 596 –608. ISSN: 0167739X. DOI: https://doi.org/10.1016/j.future.2018.11.008.

- Martin Schanzenbach, Thomas Kilian, Julian Schütte, and Christian Banse. "ZKlaims: Privacy-preserving Attribute-based Credentials using Non-interactive Zero-knowledge Techniques". In: proceedings of the 16th International Conference on Security and Cryptography (SECRYPT 2019), part of ICETE. 2019.

- Peter Schneider and Alexander Giehl. "Realistic Data Generation for Anomaly Detection in Industrial Settings Using Simulations". In: Computer Security. Ed. by Sokratis K. Katsikas, Frédéric Cuppens, Nora Cuppens, Costas Lambrinoudakis, Annie Antón, Stefanos Gritzalis, John Mylopoulos, and Christos Kalloniatis. Cham: Springer International Publishing, 2019, pp. 119–134. ISBN: 9783030127862.

- Martin Striegel, Carsten Rolfes, Fabian Helfert, Max Hornung, Johann Heyszl, and Georg Sigl. "EyeSec: A Retrofittable Augmented Reality Tool for Troubleshooting Wireless Sensor Networks in the Field". In: Proceedings of the 2019 International Conference on Embedded Wireless Systems and Networks, EWSN 2019, Beijing, China, February 25-27, 2019, pp. 184–193.

- Meng Xu, Manuel Huber, Zhichuang Sun, Paul England, Marcus Peinado, Sangho Lee, Andrey Marochko, Dennis Mattoon, Rob Spiger, and Stefan Thom. "Dominance as a New Trusted Computing Primitive for the Internet of Things". In: 2019 IEEE Symposium on Security and Privacy (SP). IEEE. 2019.


LeCroy

AISEC ON TOUR

MESSEN UND EVENTS

2018

Hannover Messe
Hannover, 23. bis 27. April 2018

Auf der Hannover Messe 2018 präsentierte das Fraunhofer AISEC den »Trusted Connector«. Er ermöglicht eine sichere Nutzung von Daten über Wahrnehmungsgrenzen hinweg und stellt damit eine Kernkomponente der Daten- und Sicherheitsarchitektur des Industrial Data Space dar. Nur vertrauenswürdige und nicht-manipulierte Datenflüsse werden für kritische Entscheidungen genutzt. Eine sichere Ausführungsumgebung basierend auf Containern und die Vorverarbeitung der Daten im Konnektor selbst ermöglichen eine feingranulare Informationskontrolle. Der Trusted Connector steht für flexiblen Datenaustausch bei völliger Datensouveränität.

CEBIT
Hannover, 11. bis 15. Juni 2018

Auf der CEBIT 2018 stellte das Fraunhofer AISEC gemeinsam mit den Fraunhofer-Instituten FIT und IFAM den Prototyp der Zertifizierungsplattform »Blockchain for Education« vor. Die Plattform bietet Vorteile für Lernende, Zertifizierungsstellen, Unternehmen sowie Hochschulen und Bildungseinrichtungen. Lernenden ermöglicht sie den sicheren Zugriff auf ihren lebenslangen Lernausweis sowie den über die Blockchain sicheren Nachweis über dessen Echtheit und Historie. Die analoge Mappe, in der die einzig gültigen Papierformen abgelegt sind, erhält damit ein zeitgemäßes digitales Gegenstück.
Gemeinsam mit dem Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT präsentierte das Fraunhofer AISEC außerdem ein Anwendungsbeispiel des »Cognitive Sensor Connectors«. In einem Logistik-Szenario ermöglicht er allen beteiligten Akteuren eine lückenlose Warenverfolgung, einen jederzeit sicheren Zugriff auf anfallende Daten sowie deren datenschutzkonforme Verarbeitung.

Zukunftskongress Logistik
Dortmund, 11. bis 12. September 2018

Auch auf dem Zukunftskongress Logistik zeigte das Fraunhofer AISEC seine Lösung für sichere Vernetzung und Sensorik, Lokalisierung, Maschinelles Lernen und vertrauenswürdige Datenverarbeitung. Der Demonstrator wurde gemeinsam mit anderen Fraunhofer-Instituten im Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT entwickelt.

it-sa
Nürnberg, 9. bis 11. Oktober 2018

Die steigende Komplexität der vernetzten Systeme, die Vielfalt der eingesetzten Hard- und Software-Komponenten sowie die Schnelllebigkeit von Prozessen erhöhen das Risiko für Angriffe auf Systeme und Infrastrukturen. Um auch in komplexen Systemen frühzeitig skalierbare Risikoanalysen durchführen zu können, hat das Fraunhofer AISEC die »Modell-basierte Risikoanalyse MoRA« (Modular Risk Assessment) entwickelt, die einen nachvollziehbaren und sicheren Systementwurf sowie die Kosten-Nutzen-Analyse von Sicherheitskonzepten ermöglicht.

2019

Pro Sweets Cologne
Köln, 27. bis 30. Januar 2019

Insbesondere beim Transport von sensiblen Gütern wie Lebensmitteln muss eine durchgängig nachweisbare Kühlkette eingehalten werden. Auf der Pro Sweets präsentierte das Fraunhofer AISEC eine Lösung zur sicheren und lückenlosen Warenverfolgung. Über kognitive Sensorik werden Werte wie Temperatur und Zustand der Ware während des Transports kontinuierlich erfasst und sicher für die Weiterverarbeitung gespeichert.

Hannover Messe
Hannover, 1. bis 5. April 2019

Auf der Hannover Messe 2019 präsentierte das Fraunhofer AISEC gemeinsam mit dem Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT Schüsseltechnologien für ein industrielles Internet anhand eines Beispiels aus der Logistik: Die lückenlose vertrauenswürdige Warenverfolgung mit kognitiver Sensorik und Blockchain-Technologie.
Sichere Sensorik, Lokalisierungssysteme sowie souveräne Datenverarbeitung und -verteilung durch Attribute-based Encryption genauso wie die Speicherung der verschlüsselten Daten in der Blockchain machen die Komplexität der anfallenden Daten beherrschbar und ermöglichen Datensouveränität für alle Beteiligten.

hub.berlin
Berlin, 10. bis 11. April 2019

Die datenökonomische und datenschutzkonforme Nutzung von Informationen durch Trackchain-Technologie demonstrierte das AISEC auch auf der hub.berlin 2019: Durch das Ablegen von erhobenen Daten in einer sicheren, den Datenschutz bewahrenden Blockchain können Liefer- und Produktionsketten über Länder- und Firmengrenzen nachverfolgt und festgehalten werden.

ZEHN JAHRE AISEC – EINE ERFOLGSGESCHICHTE

Fraunhofer AISEC

2008

Der Startschuss
Unter der Leitung von **Prof. Dr. Claudia Eckert** wird am 1. Dezember 2008 die Projektgruppe **SIT-München** gegründet.

Frühe Fokussierung
Von Anfang an besetzt das Fraunhofer AISEC die Themen **Embedded Security**, **Hardware Security**, **Automotive Security** und **Network Security**. Auch **Digitale Identitäten** gehören zu den Kompentenz- und Forschungsschwerpunkten.

2009/2010

Rascher Laboraufbau
Moderne Labors zur Untersuchung von **Hardware und Cloud Security** entstehen bereits 2009, im Jahr 2010 wird das **GSM-Labor** eröffnet.

Erweiterung der Forschungsschwerpunkte
Schritt für Schritt werden die Forschungsbereiche um **Industrial Security**, **Kritische Infrastrukturen** und **Service and Application Security** erweitert. Die Kompetenzerweiterung stößt auf große Nachfrage in der Industrie.

2011/2012

Unabhängigkeit
Am **1. Juli 2011** wird die Projektgruppe SIT-München zur selbstständigen Einrichtung Fraunhofer AISEC.

Doppelspitze
Prof. Dr.-Ing. Georg Sigl wird 2012 in die Institutsleitung berufen.

2013/2014

Eigenständiges Institut
Am **1. Dezember 2013** wird das Fraunhofer AISEC nach erfolgreicher Evaluierung bereits nach fünf Jahren in ein eigenständiges Fraunhofer-Institut überführt.

Kontinuierlicher Kompetenzausbau
Das neue **Industrielabor** wird 2013 in Betrieb genommen, seit 2014 sind auch **Roboteranalysen** möglich.

Erste Außenstelle
In **Berlin** wird 2014 mit dem Forschungsschwerpunkt **Secure Systeme Engineering** die erste Außenstelle eröffnet.

LZSiS

Lernlabor Cybersicherheit

Fraunhofer CCIT

2015/2016

Weiterer Laborausbau

Im Jahr 2015 entstehen mit dem **NETSEC-Labor** und dem **Mobile-Payment-Lab** neue innovative Labors.

Neue Schwerpunkte

Seit Oktober 2016 bietet das Fraunhofer AISEC im Rahmen des **Lernlabors Cybersicherheit** Schulungen und Weiterbildungen zum Thema IT-Sicherheit für Industrie und die öffentliche Verwaltung.

2017

Mehr Raum für Sicherheit

Am **26. Oktober 2017** wird der Grundstein für den **AISEC-Neubau** gelegt, mit dem eHouse wird in **Weiden** im gleichen Jahr die **zweite Außenstelle** eröffnet.

Neue Forschungsgruppen

Die Innovationsthemen **Physical und Cognitive Securtiy Technologies** werden Forschungsschwerpunkte eigener Gruppen.

Forschungspartnerschaft

Gründung des **Leistungszentrums Sichere Vernetzte Systeme** München unter der Leitung von Prof. Dr-Ing. Georg Sigl, später **Sichere intelligente Systeme**.

2018

Auszeichnungen

Das Fraunhofer AISEC wird von *brand eins Wissen* und *Statista* zum **Innovator des Jahres** in der Kategorie »Technologie & Telekommunikation« gekürt, **2019** wird das Institut gleichermaßen ausgezeichnet.

Eine Dekade Sicherheit

Das Fraunhofer AISEC feiert sein **10-jähriges Jubiläum**.

Schulterschluss für die Industrie 4.0

Gründung des **Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT** unter der Leitung von Prof. Dr. Claudia Eckert.

2019

KI und Qbits im Fokus

Die Zahl der Projekte im Bereich Machine Learning und Künstliche Intelligenz steigt – die Gruppe **Cognitive Security Technologies** wird eine eigenständige Abteilung. Die **Postquantum-Expertise** erstreckt sich über mehrere Abteilungen am Fraunhofer AISEC.

Neues Kompetenzzentrum für Cybersicherheit

Im September steht mit dem **Institutsneubau** ein auf das Fraunhofer AISEC zugeschnittener Forschungsraum mit über 700m² Laborfläche und Raum für 272 Mitarbeiter zur Verfügung.

UNSER NEUBAU – DAS AISEC ZIEHT UM

In nur drei Jahren Bauzeit ist aus 6.200 Kubikmetern Beton und Stahl auf dem Forschungscampus Garching bei München, einer der modernsten Forschungs- und Ausbildungsstätten Europas, der Institutsneubau des Fraunhofer AISEC entstanden, der im Herbst 2019 in Betrieb genommen wird.

Dieses neue Zentrum für Cybersicherheit eröffnet auf 4.000 m² mehr Raum für Sicherheit: Mehr Raum für Mitarbeiter, mehr Raum für Testräume und mehr Raum für Kooperationen und Projekte. Neben modern ausgestatteten Büroräumen und Innovation Labs finden vor allem insgesamt zwölf neue Forschungslabors ausreichen Platz. Neues Highlight wird das Automotive-Labor sein, in dem mehrere Fahrzeuge parallel getestet und analysiert werden können. Auf einer eigens dafür konzipierten Ausstellungsfläche wird AISEC-Kompetenz ganzjährig direkt anschaulich gemacht.

Die neue Infrastruktur im ersten für seine Zwecke geplanten Haus wird den Handlungsraum des AISEC signifikant erweitern; die unmittelbare Nachbarschaft zur TU München wird die Zusammenarbeit zwischen exzellenter universitärerer und angewandter Forschung noch weiter befördern. Das Investitionsvolumen von rund 30 Millionen Euro tragen zur Hälfte das Bundesministerium für Bildung und Forschung sowie der Freistaat über das Strategieprogramm BAYERN DIGITAL des Staatsministeriums für Wirtschaft, Infrastruktur, Verkehr und Technologie.

78 Büroräume

Innovativer Hochsicherheitsbereich

Platz für 272 MA

13 Meetingräume

12 Labors

FRAUNHOFER-GESELLSCHAFT

Forschen für die Praxis ist die zentrale Aufgabe der Fraunhofer-Gesellschaft. Die 1949 gegründete Forschungsorganisation betreibt anwendungsorientierte Forschung zum Nutzen der Wirtschaft und zum Vorteil der Gesellschaft. Vertragspartner und Auftraggeber sind Industrie- und Dienstleistungsunternehmen sowie die öffentliche Hand.

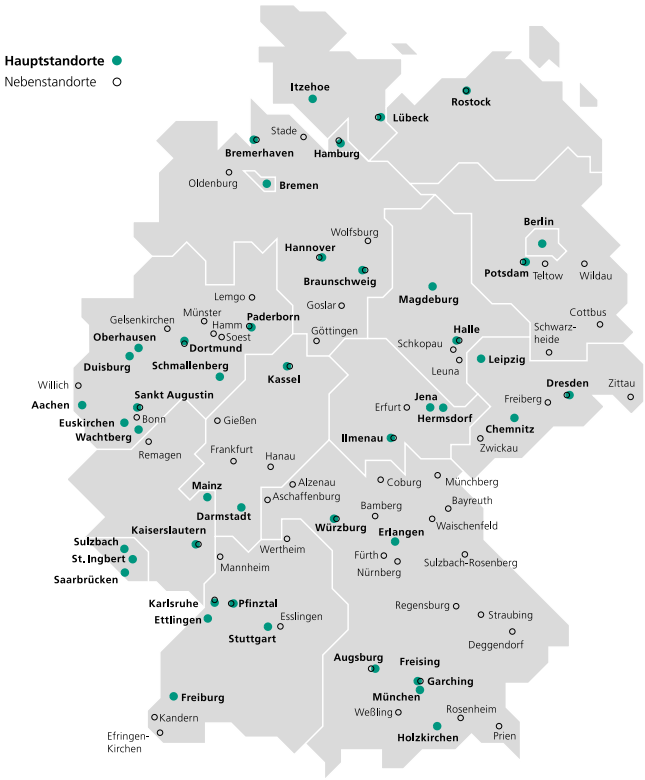
Die Fraunhofer-Gesellschaft betreibt in Deutschland derzeit 72 Institute und Forschungseinrichtungen. Mehr als 26 600 Mitarbeiterinnen und Mitarbeiter, überwiegend mit natur- oder ingenieurwissenschaftlicher Ausbildung, erarbeiten das jährliche Forschungsvolumen von 2,6 Milliarden Euro. Davon fallen 2,2 Milliarden Euro auf den Leistungsbereich Vertragsforschung. Rund 70 Prozent dieses Leistungsbereichs erwirtschaftet die Fraunhofer-Gesellschaft mit Aufträgen aus der Industrie und mit öffentlich finanzierten Forschungsprojekten. Rund 30 Prozent werden von Bund und Ländern als Grundfinanzierung beigesteuert, damit die Institute Problemlösungen entwickeln können, die erst in fünf oder zehn Jahren für Wirtschaft und Gesellschaft aktuell werden.

Internationale Kooperationen mit exzellenten Forschungspartnern und innovativen Unternehmen weltweit sorgen für einen direkten Zugang zu den wichtigsten gegenwärtigen und zukünftigen Wissenschafts- und Wirtschaftsräumen.

Mit ihrer klaren Ausrichtung auf die angewandte Forschung und ihrer Fokussierung auf zukunftsrelevante Schlüsseltechnologien spielt die Fraunhofer-Gesellschaft eine zentrale Rolle im Innovationsprozess Deutschlands und Europas. Die Wirkung der angewandten Forschung geht über den direkten Nutzen für die Kunden hinaus: Mit ihrer Forschungs- und Entwicklungsarbeit tragen die Fraunhofer-Institute zur Wettbewerbsfähigkeit der Region, Deutschlands und Europas bei. Sie fördern Innovationen, stärken die technologische Leistungsfähigkeit, verbessern die Akzeptanz moderner Technik und sorgen für Aus- und Weiterbildung des dringend benötigten wissenschaftlich-technischen Nachwuchses.

Ihren Mitarbeiterinnen und Mitarbeitern bietet die Fraunhofer-Gesellschaft die Möglichkeit zur fachlichen und persönlichen Entwicklung für anspruchsvolle Positionen in ihren Instituten, an Hochschulen, in Wirtschaft und Gesellschaft. Studierenden eröffnen sich aufgrund der praxisnahen Ausbildung und Erfahrung an Fraunhofer-Instituten hervorragende Einstiegs- und Entwicklungschancen in Unternehmen.

Namensgeber der als gemeinnützig anerkannten Fraunhofer-Gesellschaft ist der Münchner Gelehrte Joseph von Fraunhofer (1787–1826). Er war als Forscher, Erfinder und Unternehmer gleichermaßen erfolgreich.



Die Fraunhofer-Gesellschaft in Deutschland.

Fraunhofer

Die Fraunhofer-Gesellschaft weltweit.

IMPRESSUM

Herausgeber
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Prof. Dr. Claudia Eckert

Lichtenbergstraße 11
85748 Garching
Telefon: +49 89 322 99 86-0
E-Mail: info@aisec.fraunhofer.de
www.aisec.fraunhofer.de

Redaktion
Dr. Barbara Eschlberger (Leitung), Melanie Meier, Susanne Starzer

Layout und Produktion
Susanne Starzer, Melanie Meier

Druck
Ortmaier Druck GmbH, Frontenhausen

Anschrift der Redaktion
Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Public Relations & Marketing, Dr. Barbara Eschlberger
Lichtenbergstraße 11
85748 Garching
Telefon: +49 89 322 99 86-169
E-Mail: marketing@aisec.fraunhofer.de

Berichtzeitraum
Januar 2018 - Mai 2019

Redaktionsschluss
30. August 2019

Bildquellen

- Titel: Jens Schwarz
- Seite 2: rechts: Andreas Heddergott, links: Oliver Bodmer
- Seite 8: Jens Schwarz
- Seite 12: Bild Diaw: Jürgen Mai
- Seite 13: Bild Kempf: Christian Kruppa, Bild Prasse: MIKA-fotografie | Berlin
- Seite 21: rechts: Andreas Heddergott, links: Jens Schwarz
- Seite 27: rechts: NürnbergMesse/Heiko Stahl
- Seite 30: oben: brand eins/Statista, unten: Fraunhofer EMFT/Bernd Müller
- Seite 31 oben: StMWi/A.Wechsler, unten links: TISAX, unten rechts: TÜV Süd
- Seite 33: oben: secUnity, unten: Infineon Technologies AG
- Seite 36/37: Industrial Data Space
- Seite 39: Fraunhofer EMFT
- Seite 55: Jens Schwarz
- Seite 57: Fraunhofer-Gesellschaft
- Seite 59: 2018: brand eins/Statista, 2019: Henn GmbH
- Seite 60/61: Henn GmbH
- Seite 62/63: Fraunhofer-Gesellschaft

Bei nicht gekennzeichneten Bildern liegen die Bildrechte beim Fraunhofer AISEC.

Aus Gründen der leichteren Lesbarkeit wird an einigen Stellen die gewohnte männliche Sprachform bei personenbezogenen Substantiven und Pronomen verwendet. Dies impliziert jedoch keine Benachteiligung des weiblichen Geschlechts, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral zu verstehen sein.

Garching, August 2019