Fraunhofer AISEC

Jahresbericht 2022

Mit Sicherheit innovativ

#mitsicherheitinnovativ

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC | Jahresbericht 2022

Jahresbericht 2022

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

Prof. Dr. Claudia Eckert,
geschäftsführende Institutsleiterin

Prof. Dr. Georg Sigl,
Institutsleiter

Willkommen am Fraunhofer AISEC!

Sehr geehrte Leserin, sehr geehrter Leser,

2022 war alles andere als ein gutes Jahr für die Cybersicherheit. Der Krieg in der Ukraine hat uns vor Augen geführt, wie fragil selbst als unerschütterlich geglaubte Grundsätze wie der Frieden in Europa sind. Das Leid der betroffenen Menschen ist unermesslich. Das Fraunhofer AISEC erklärt sich solidarisch mit der Ukraine und verurteilt die russische Aggression aufs Schärfste. Zielgerichtete, großangelegte Cyberattacken haben seit Kriegsbeginn deutlich zugenommen. In der zweiten Jahreshälfte betitelte das Bundesamt für Sicherheit in der Informationstechnik (BSI) seinen Lagebericht 2022 deshalb nicht umsonst mit »Gefährdungslage im Cyber-Raum so hoch wie nie«: Vor allem Ransomware-Angriffe und Störungen von IT-Lieferketten bedrohen die Sicherheit von Gesellschaft, Staat und Wirtschaft. Doch es gab 2022 auch Lichtblicke: Mit dem European Cyber Resilience Act stellte die EU im September einen lange erwarteten Entwurf für ein Gesetz zur Cyber-Resilienz vor.

Das Fraunhofer AISEC hat 2022 weiter intensiv daran gearbeitet, den Angreifenden einen Schritt voraus zu sein, etwa indem wir Zukunftsthemen systematisch angegangen sind: Wir haben z. B. das Kompetenzzentrum Post-Quanten-Kryptografie gestartet, bringen unsere Cybersicherheitsexpertise beim Leuchtturmprojekt 6G-ANNA ein und bauen gemeinsam mit Partnern das Zentrum für vertrauenswürdige Künstliche Intelligenz (ZVKI) auf. Beim Thema sichere digitale Identitäten sind wir an allen wichtigen bundesweiten Projekten beteiligt und spielen eine maßgebliche Rolle bei der Gestaltung sicherer Datenräume. Über das »Zentrum Trusted Electronic Bayern« (TrEB) und das »Bayerische Chip-Design-Center« treiben wir die Forschung und Entwicklung sicherer und vertrauenswürdiger, integrierter Elektroniksysteme voran. Und wir fördern den internationalen Austausch in der Cybersicherheitsforschung, beispielsweise durch Kooperationen mit unserem neuen Partner Fraunhofer Singapore.

Doch das Fraunhofer AISEC ist noch viel mehr als das: Über 220 hochqualifizierte Mitarbeiterinnen und Mitarbeiter bewerten, gestalten und bewahren täglich IT-Sicherheit durch angewandte Forschung. Besonders gefragt ist unsere Fähigkeit, methodisch die Sicherheit von Lösungen, Designs oder auch Architekturen zu beurteilen und die Risiken bei deren Nutzung nachvollziehbar, Werkzeug-gestützt zu ermitteln und adäquate Lösungsvorschläge zu entwickeln. In Forschungsprojekten mit Unternehmen, Behörden und Einrichtungen oder über die Angebote des Lernlabors Cybersicherheit tragen wir unser Wissen in die Praxis und zu den Menschen. Denn um die digitalen Bedrohungen in den Griff zu bekommen, muss die Sicherheitskultur von jeder Einzelnen und jedem Einzelnen von uns gelebt werden. Wir hoffen, dass Ihnen unser Jahresbericht 2022 dafür die notwendige Inspiration liefert.

Wir wünschen Ihnen eine aufschlussreiche Lektüre und interessante Einblicke in unser Tun!

Herzliche Grüße

Prof. Dr. Claudia Eckert

Prof. Dr. Georg Sigl

Inhalt

Cybersicherheit richtig beurteilen

Die Digitalisierung schreitet voran und die Vernetzung nimmt zu. Cybersicherheit zu gewährleisten, wird immer komplexer. Nur wer beurteilungsfähig bleibt, behält den Überblick. Das Fraunhofer AISEC vereint alle dafür notwendigen Kompetenzen.

Für heute verwendete Computer ist charakteristisch, dass ein gemeinsamer Speicher sowohl Programmbefehle als auch Daten vorhält. Diese Rechner unterscheiden nicht zwischen Daten wie Zahlen, Werten und Code wie Befehlen. Programme, die fehlerhaft programmiert sind und beispielsweise die Eingaben oder aber auch die Rückgabewerte nicht prüfen, sind auch heute noch der Ausgangspunkt für viele erfolgreiche Angriffe. So können Angreiferinnen und Angreifer versuchen, über die nicht kontrollierten Eingabeparameter, anstatt Parameterwerte, also Daten, ausführbaren Schad-Code in das System einzuschleusen und zur Ausführung zu bringen. »Je nach Art des infiltrierten Programms und des eingespeisten Schad-Codes kommt die cyber-kriminelle Person auch an kritische Informationen heran«, sagt Prof. Dr. Claudia Eckert, Leiterin des Fraunhofer AISEC.

Immer einen Schritt voraus

Hackerinnen und Hacker bleiben aber nicht bei diesen einfachen Angriffen stehen, sondern verfeinern stetig ihre Technik, kombinieren diese zu komplexen Angriffen und verschleiern ihre Aktivitäten häufig. »Es ist deshalb unerlässlich, dass wir unsere Analysemethoden und Sicherheitskompetenzen stetig auf höchstem Niveau weiter vorantreiben, um den Angreifenden den entscheidenden Schritt voraus zu sein«, sagt Eckert.

»Software wird zwar deutlich häufiger angegriffen als Hardware, aber bei Hardware sind die Folgen gravierender. Denn als Hardware-Sicherheitsanker bildet sie die Basis für alle Software-Sicherheitsfunktionen«, erläutert Prof. Dr. Georg Sigl, Leiter des Fraunhofer AISEC. »Trojaner beispielsweise wurden bislang noch nicht wissenschaftlich fundiert in Hardware nachgewiesen. Doch undenkbar ist das nicht und hätte – vorausgesetzt der Trojaner bliebe unentdeckt – weitreichende Folgen. Denn IT-Infrastrukturen sind wie Zwiebeln aufgebaut: die Hardware im Kern und in den äußeren Schalen das Betriebssystem, die Programm-Bibliotheken und schließlich die Anwendungen.«

Zielobjekt bei Angriffen auf die Hardware ist meist das »Secure Element« – ein Vertrauensanker, auf dem kryptografisch sicher gerechnet werden kann und der Informationen zur Verschlüsselung speichert. Wenn das System nicht »gehärtet« ist, lassen sich durch Seitenkanal- und Fehlerangriffe die Schlüssel auslesen. Angreifende analysieren dafür physikalische Effekte des Hardware-Betriebs, z. B. die elektromagnetische Abstrahlung oder die Reaktion der Hardware auf das Einspeisen von Fehlern und gewinnen so Erkenntnisse über die Schwachstellen des installierten Krypto-Systems. Auch Hardware-Schnittstellen (Debugger), die Entwickler zur Fehlerbehebung nutzen, können Cyberkriminelle als Einfallstor nutzen.

IT-Sicherheit bedarf vertrauenswürdiger Elektronik. Im Hardware Security Lab des Fraunhofer AISEC prüfen Sicherheitsforschende Elektro-Chips präzise auf ihre Manipulationsanfälligkeit, beispielsweise durch Fehlerangriffe mit Laser-Impulsen.

Digitaler, vernetzter, komplexer

Durch die zunehmende Digitalisierung und Vernetzung sind IT-Systeme mittlerweile an allen entscheidenden Stellen einer modernen Volkswirtschaft anzutreffen. Die Integration von Schutzmaßnahmen zur Gewährleistung der Cybersicherheit solcher offener, vernetzter Systeme hat hierbei oftmals nicht Schritt gehalten. So weisen digitale Steuerungskomponenten oder Sensoren in Industrie- oder Alltagsgeräten häufig große Sicherheitslücken auf. Durch das sich immer weiter ausbreitende Internet der Dinge (Internet of Things/IoT) ist die Anzahl digitaler Schnittstellen bereits heute kaum noch zu kontrollieren. Jede einzelne davon ist ein potenzielles Einfallstor für Cyberkriminelle. »Systematische, automatisierte Analysen und Härtungen sind unerlässlich, um solche Einfallstore nachhaltig zu schließen«, sagt Eckert.

Haben Angreifende sich beispielsweise über Phishing die notwendigen Zugangsdaten von Mitarbeitenden ergaunert, können sie das System manipulieren. Gelingt das den Kriminellen nicht, z. B. weil Mitarbeitende entsprechend geschult wurden, können sie versuchen, das Zielsystem mit frei verfügbarer Angriffs-Software, sogenannten Exploits, anzugreifen. »Deshalb ist es für jedes Unternehmen wichtig, stets die neusten Sicherheitspatches einzuspielen, um solchen vorgefertigten Angriffen den Riegel vorzuschieben«, erklärt Eckert.

Beurteilungsfähig bleiben

Cyberangriffe auf IT-Schwachstellen abzuwehren ist eine komplexe Aufgabe. Diese zu lösen, ist nur möglich, wenn man beurteilen kann, auf welche Art und Weise einzelne IT-Komponenten die Abläufe beeinflussen, wie sie funktionieren und wo ihre sensiblen Punkte liegen. Ebenso wichtig ist es zu wissen, welche Funktionen essenziell sind, um das aus unternehmerischer Sicht erforderliche, oder auch vom Gesetzgeber verbindlich erwartete bzw. von der Gesellschaft eingeforderte Niveau an Cybersicherheit zu erfüllen.

Das Fraunhofer AISEC unterstützt Unternehmen, Institutionen und Einrichtungen dabei, diese Herausforderungen zu meistern. Die Expertinnen und Experten für angewandte Cybersicherheits-Forschung sind in der Lage zu beurteilen, was in der jeweiligen IT-Komponente steckt und was ihre Nutzung für die IT-Sicherheit bedeutet. Notwendig ist ein tiefes, systemisches Verständnis vom Aufbau und dem Zusammenwirken von Hard- und Software. Hinzu kommt die Fähigkeit, die Funktionalitäten von einzelnen Komponenten im Detail verstehen zu können – seien es Chips oder Code. Häufig muss spezielles Domänenwissen, z. B. bei Anwendungen für Automotive oder Industrie, mit Fachwissen aus den Bereichen Informatik, Elektrotechnik, Physik und Mathematik vereint werden. Daneben bedarf es expliziter Kenntnisse über Möglichkeiten und Grenzen von automatisierten Werkzeugen, denn durch die immer weiter fortschreitende Digitalisierung und Vernetzung besteht ein erhöhter Sicherheitsbedarf an automatisierten Elementen. Schließlich muss man versteckte, zunächst nicht offensichtliche Funktionalitäten der Komponenten erkennen, die z. B. Trojaner beinhalten könnten. »Wichtig ist außerdem, neben der Technik immer auch weitere Einflussfaktoren zu berücksichtigen, z. B. Lieferketten oder globale Entwicklungen in Wirtschaft und Politik. Auch die Security-Gesetzgebung einzelner Länder muss bei einer Risikoeinschätzung im Blick sein, wie die aktuelle geopolitische Lage leider dramatisch zeigt«, erläutert Eckert.

Für die Risikoanalyse komplexer vernetzter IT-Systeme hat das Fraunhofer AISEC eine Methode entwickelt, die es erlaubt, diese facettenreiche Aufgabe ganzheitlich anzugehen: das Modular Risk Assessment (MoRA). »MoRA versetzt unsere Expertinnen und Experten in die Lage, methodisch vorzugehen, die richtigen Fragen zu stellen und die Sachlage sowie alle Problemfelder vollständig zu erfassen«, sagt Sigl. Haben die Teams dieses umfassende Basis-Verständnis eingeholt, arbeiten sie sich weit in das Innere der Komponenten vor. »Insbesondere bei Hardware sind wir da nicht zimperlich«, sagt Sigl. Die Werkzeuge der Hardware-Spezialistinnen und -Spezialisten des Fraunhofer AISEC reichen vom sachgemäßen, physischen Aufbrechen von mikroelektronischen Chips über systematische Laserangriffe auf elektronische Schaltungen bis hin zu Fuzzing. Die Spezialistinnen und Spezialisten für Software Security tauchen tief in die Programm-Codes ein. Falls die Informationen nicht im Quellcode vorliegen, greifen die Forschenden auf die Technik des Reverse Engineering zurück. In diesem Fall wird unter Nutzung von Werkzeugen und Know-how versucht, aus dem Binärcode das ursprüngliche Programm zu rekonstruieren, um es dann eingehend analysieren zu können. »Unsere Kunden fragen vor allem zwei Dinge nach: Risikoanalysen bei der Produktentwicklung sowie für bestehende Produkte und das Erstellen von Sicherheitskonzepten und die Begleitung bei deren korrekter Umsetzung«, sagt Eckert.

Kontinuierliche Aufgabe

Cybersecurity ist ein kontinuierlicher Vorgang, der weitreichend im operativen Prozess verankert sein muss. Aber auch dann gibt es nie eine 100-prozentige Sicherheit. Denn Technologien verändern sich immer rascher. Doch es gibt Hoffnung: So wie es viele Möglichkeiten gibt, Software oder Hardware abzusichern, wird es auch zukünftig möglich sein, die neuen Gefahren einzudämmen. »Voraussetzung dafür ist jedoch, dass man in der Lage bleibt, die Gefahren und die Möglichkeiten von IT-Komponenten richtig zu beurteilen«, sagt Eckert. »Analysen und Risikoeinschätzungen müssen aber zwingend durch den Einsatz von passgenauen Sicherheitskonzepten und Kontrollen ergänzt werden.«

Gerade bei den Kontrollen findet derzeit ein bereits seit langem geforderter Paradigmenwechsel in Unternehmen statt: der schrittweise Übergang auf Zero-Trust-Architekturen. »Das heißt nicht, dass ich nichts und niemandem trauen darf, um beurteilungsfähig zu bleiben. Das wäre nur sehr aufwändig und energieintensiv umzusetzen«, sagt Sigl. Zero-Trust besagt vielmehr, Wege zu finden, Bereiche zuverlässig gemäß ihren Sicherheitsniveaus unterscheiden und differenziert die Zugriffe in diesen Bereichen kontrollieren zu können.

Kontakt

Prof. Dr. Claudia Eckert
Institutsleitung (geschäftsführend)
Tel. +49 89 3229986-292
claudia.eckert@aisec.fraunhofer.de

Kontakt

Prof. Dr. Georg Sigl
Institutsleitung
Tel. +49 89 3229986-292
georg.sigl@aisec.fraunhofer.de

Projekte

Codyze
Codyze unterstützt sowohl Entwickler als auch Auditoren bei der Programmierung und Evaluierung sicherheitskritischer Software.

Clouditor
Der Clouditor ist ein Werkzeug, das die sichere Konfiguration von Diensten und Anwendungen in der Cloud überprüft.

IntelliSecTest
Im Forschungsprojekt IntelliSecTest entwickeln vier Fraunhofer-Institute ein kostengünstiges und leicht anwendbare Security-Testing.

Trusted Electronic Bayern
Im Projekt Trusted Electronic Bayern entsteht ein gehärtetes »Secure Element« auf Basis von Open Source Risk-V-Prozessoren.

Mit Sicherheit erfahren

Die Industrial Security Labs des Fraunhofer AISEC bieten alle Voraussetzungen, um Fahrzeuge und Produktionsstraßen testweise anzugreifen und Abwehrmechanismen zu entwickeln und zu evaluieren. Hier generiertes Wissen schafft die Grundlage für die industrielle Sicherheit von heute und morgen.

Im Automotive Security Lab des Fraunhofer AISEC stehen drei Fahrzeuge. »Bei diesen Fahrzeugen können wir mit unseren Möglichkeiten alle digitalen Funktionalitäten testen, die für das Thema Security relevant sind«, sagt Bartol Filipovic. Er ist Leiter der Abteilung »Product Protection and Industrial Security« am Fraunhofer AISEC und an entscheidender Stelle mit dafür verantwortlich, dass sich Kunden auf die IT-Sicherheit ihrer Systeme verlassen können. Sei es bei vernetzten Fahrzeugen, Produktionsanlagen oder bei den Produkten selbst. Deshalb kann – oder besser muss – Filipovic oder ein anderer der insgesamt fast 20 Expertinnen und Experten in den Fraunhofer AISEC-Laboren für automobile und industrielle Sicherheit alle denkbaren IT-Attacken auf diese drei Fahrzeuge starten. Schließlich könnten sie auch von Unbefugten und Kriminellen durchgeführt werden.

»Wer erfolgreich angreift, weiß auch, wo die Schwachstellen für Industrie-Spionage oder Sabotage sind und kann entsprechende Gegenmaßnahmen entwickeln. Das ist nicht nur wichtig, um die immer strenger werdenden gesetzlichen Regularien einzuhalten, sondern auch, um vorausschauend eine möglichst umfangreiche Sicherheit zu gewährleisten«, sagt Filipovic. Das sei auch deshalb wichtig, weil es Jahre dauert, bis neue Fahrzeuge oder Industrieanlagen auf den Markt kommen, die dann Angriffen ausgesetzt sind. Durch die steigende Lieferantenabhängigkeit und die zunehmend vernetzte Produktion bestehen aber auch heute schon viele Schwachstellen: Sie werden jetzt ausgenutzt, aber eventuell erst später entdeckt. All das könne dann neben finanziellen Einbußen auch Verluste der Reputation zur Folge haben.

Status quo erfassen und Überblick bekommen

In der Studie Produktpiraterie etwa, die das Fraunhofer AISEC regelmäßig im Auftrag des Verbands Deutscher Maschinen- und Anlagenbau (VDMA) durchführt, hat sich in der Erhebung von 2022 gezeigt, dass aktuell 72 Prozent der befragten Mitgliedsunternehmen von Produktpiraterie betroffen sind. Die Schadenssumme belief sich auf 6,4 Milliarden Euro im Jahr 2022.

Damit Unternehmen sich einen Überblick über die individuellen Gefährdungen durch Piraterie und Manipulation verschaffen können, hat das Fraunhofer AISEC ein Industry 4.0 & IT Security Audit entwickelt, auf das bereits eine Vielzahl von international agierenden Industrieunternehmen zurückgreifen. »Kern dabei ist eine systemische Risikoanalyse, die den Status quo erfasst und einen Überblick ermöglicht«, erklärt Filipovic: Was ist verbaut im einzelnen Objekt, im Fahrzeug oder der Industriestraße? Auf welche Weise sind die Module vernetzt? Dank der Modular Risk Assessment Methodik (MoRA) [Glossar], auf der das Audit basiert, besteht die Chance, dass nur einzelne Komponenten ausgetauscht werden müssen, um einen deutlich höheren Sicherheitsstandard zu erreichen.

Auf Übersicht als einen wichtigen Schritt Richtung »Hilfe zur Selbsthilfe« setzte auch das Konsortialprojekt IUNO Insec, das vom Fraunhofer AISEC koordiniert wurde. »Ziel war es, Lösungen speziell für kleine und mittlere Unternehmen (KMU) zu entwickeln, damit sie selbstständig ihr IT-Sicherheitsniveau anheben können«, erklärt Filipovic. So sei es nun möglich, mit vergleichsweise einfach zu handhabenden Werkzeugen eine Anomalie-Erkennung und Security-Tests bei Steuergeräten durchzuführen.

Team vereint Anwender- und Technologie-Know-how

Filipovic und sein Team bringen das nötige Know-how für umfassende Analysen und Tests sowie für die Entwicklung von Security-Tools mit: Sie vereinen Erkenntnisse unterschiedlicher Forschungsschwerpunkte und verschiedener Industriesparten. Sie haben eine Vielzahl von speziellen Instrumenten und teilweise selbstentwickelten Tools zur Verfügung, um einzelne Komponenten und eingebettete Systeme vielfältigen, fortgeschrittenen Sicherheitsprüfungen zu

Cybersicherheits-Experten des Fraunhofer AISEC prüfen ein Fahrzeug in der geschützten Umgebung des Automotive Lab.

unterziehen. Um die unterschiedlichsten Gefahren-Szenarien abbilden zu können, sind in den Labors für Industrial & Automotive Security die elektronischen Infrastrukturen von Fahrzeugen und Anlagen für die industrielle Produktion nachgebildet. Ein Beispiel ist eine moderne Industriestraße mit Vernetzungen, Andockstellen sowie mobilen und stationären Robotern. Außerdem stehen den Expertinnen und Experten digitale Zwillinge zur Verfügung, die die Prozesse digital abbilden und das Durchführen vielfältiger Simulationen erlauben.

Autonomes Fahren, Sensorik, Industrie 4.0 – IT-Security für konkrete Anwendungen

Parallel zur Suche nach Angriffsmöglichkeiten an konkreten oder virtuellen Objekten, bei denen spezielle Kundenanfragen und -wünsche im Vordergrund stehen, sind die Labore auch Ausgangspunkt für richtungweisende Forschungsprojekte bei Industrial und Automotive Security. Dazu gehört beispielsweise ATLAS-L4, das die Grundlagen schafft für überwiegend selbstständig fahrende Lkws, die nicht nur Unfälle vermeiden, sondern auch alle bestehenden und zukünftig geplanten Security-Regeln erfüllen, wie sie etwa im Cyber Resilience Act (CRA-E) der EU [Glossar] vorgesehen sind. Eine andere Ausrichtung hatte das Projekt DigitalTWIN, in dem das Fraunhofer AISEC einen Security-Leitfaden für die Sensorik von Fassadenelementen ausgearbeitet und veröffentlicht hat. »Die Industrie hat nun Vorgehensweisen an der Hand, um auf elementare Fragen der Sicherheit von Sensoren, der Kommunikation mit der Zentraleinheit und der Cloud-Nutzung Antworten geben zu können«, erklärt Filipovic. Eine konkrete Antwort auf Sicherheitsfragen soll auch das Projekt »PoQsiKom – Post-Quanten-sichere Kommunikation für die Industrie 4.0« geben. Das Fraunhofer AISEC leitet dieses Konsortialprojekt, um neuartige Hardware-Vertrauensanker für Betriebstechnik und Edge-Devices zu entwickeln. »Diese Art von Hochsicherheitschips wird resistent sein auch gegen Angriffe durch Quantencomputer. Sie können dann genutzt werden, um beispielsweise Geräte in intelligenten Fabriken so abzusichern, dass Sicherheitsfunktionen wie die unbedingte Rücksicht auf Menschen gewährleistet bleiben«, sagt Filipovic. Auch der vollständige Fernbetrieb einer Maschine wird damit zuverlässig geschützt.

Glossar

*Das **Modular Risk Assessment (MoRA)** ist eine modular aufgebaute und auf die Entwicklung von sicheren Automobilsystemen spezialisierte Methode zur Risikobewertung.*

*Der **Cyber Resilience Act (CRA-E)** ist ein Verordnungsvorschlag der Europäischen Kommission. Durch grundlegende IT-Sicherheitsanforderungen an digitale Produkte und ihren Herstellungsprozess soll die Cybersicherheit im europäischen Raum nachhaltig erhöht werden.*

Realitätsnahe Simulationsumgebungen im Industrial Security Lab am Fraunhofer AISEC ermöglichen die Verwendung echter, praxiserprobter Industriekomponenten.

Industrial & Automotive Security | Mit Sicherheit erfahren

Projekte

PoQsiKom
Im Projekt Post-Quanten-sichere Kommunikation für Industrie 4.0 (PoQsiKom) entwickelt das Fraunhofer AISEC einen neuartigen Hardware-Vertrauensanker.

DigitalTWIN
Das Fraunhofer AISEC hat die Security-Aspekte von Digitalen Zwillingen untersucht, Szenarien und Schutzkonzepte entwickelt und veröffentlicht.

ATLAS-L4
Das Projekt ATLAS-L4 hat zum Ziel, autonom fahrende Lkw auf der Autobahn zum Einsatz zu bringen.

IUNO Insec
Das Fraunhofer AISEC hat im Projekt IUNO Insec Lösungen weiterentwickelt, die speziell KMU unterstützen, das eigene IT-Sicherheitsniveau anzuheben.

Industry 4.0 & IT Security Audit
Das vom Fraunhofer AISEC entwickelte Audit basiert auf einer Risikoanalyse mittels der Modular Risk Assessment (MoRA) Methode.

Studie »Produktpiraterie 2022«
Im Auftrag des VDMA hat das Fraunhofer AISEC die Studie »Produktpiraterie 2022« erstellt.

Kontakt

Bartol Filipovic
Abteilungsleiter Product Protection and Industrial Security
Tel. +49 89 3229986-128
bartol.filipovic@aisec.fraunhofer.de

PoQsiKom

DigitalTWIN

ATLAS-L4

IUNO Insec

Industy 4.0 & IT Security Audit

Studie zur Produktpiraterie 2022

Datensouverän? Aber sicher!

Digitale Souveränität wird immer mehr zum marktentscheidenden Faktor. Mit den Tools des Fraunhofer AISEC können Unternehmen ihr Sicherheitsniveau systematisch verbessern.

Für ein Drittel der Unternehmen in Deutschland ist die digitale Selbstbestimmung zentral für ihre IT- und Businessstrategie geworden. Diese Entwicklung dürfte sich weiter verstärken, denn digitale Souveränität bedeutet, dass ein Unternehmen über Nutzung und Nachnutzung seiner Daten bestimmen kann, auch wenn diese Verarbeitung außerhalb seiner direkten Kontrolle, wie z. B. auf Cloudplattformen stattfindet. Und das nicht nur, um vor Diebstahl, Manipulation und Sabotage bestmöglich geschützt zu sein, sondern auch, um die Abhängigkeit von einzelnen Anbietern zu reduzieren und im Bedarfsfall auf Alternativen zurückgreifen zu können.

»Datensouveränität und technologische Souveränität sind zu einem marktentscheidenden Kennzeichen zukunftsorientierter Industrie geworden«, sagt Christian Banse, Abteilungsleiter »Service and Application Security« am Fraunhofer AISEC. Das Implementieren von einfachen Abwehrmaßnahmen, wie beispielsweise verschlüsselte Datenkommunikation, die Authentisierung beim Zugang zu einem System oder die Kontrolle der Rechtmäßigkeit von Zugriffen, ist ein guter Ausgangspunkt. Sie reichen bei einem spezifischen, zielgerichteten Angriff jedoch nicht aus, um Souveränität zu gewährleisten. Das wissen auch die Verantwortlichen der Unternehmen, z. B. aus der Digitalwirtschaft, der Industrie 4.0 oder dem Automotiv- und Finanzsektor. Deshalb sind in den vergangenen Jahren die Anfragen zum Confidential Computing gestiegen. Der Begriff steht für Technologien, die die Vertraulichkeit und Integrität von Daten bei deren Übertragung, Verarbeitung und Speicherung sicherstellen.

Resiliente, verteilte Systeme aufbauen

2022 haben die Expertinnen und Experten des Fraunhofer AISEC eine Vielzahl grundlegender und nutzerfokussierter Projekte initiiert, fortgeführt oder abgeschlossen. Alle mit dem Ziel, die Grundlage dafür zu schaffen, Cybergefahren sicher einzuschätzen und Datensouveränität zu ermöglichen. Im Fokus dabei: Unternehmen, die ihr Sicherheitsniveau in den kommenden Jahren systematisch verbessern wollen. Ein Beispiel ist das vom Fraunhofer AISEC fortlaufend weiterentwickelte Betriebssystem GyroidOS, mit dem Anwendungen auf IoT- oder Edge-Geräten und in der Cloud »abgriffssicher« genutzt werden können. »Das auf dem Linux-Kernel aufsetzende GyroidOS stellt alle nötigen Funktionalitäten bereit, um ein System zu härten«, sagt Sascha Wessel, Abteilungsleiter »Secure Operating Systems«.

Wegweisend ist GyroidOS nicht nur, damit Rechenzentrumsbetreiber im Bereich Confidential Computing und 5G-Infrastrukturkomponenten die Daten ihrer Kunden schützen, sondern beispielsweise auch, um Angriffe auf leistungsstarke Steuergeräte in Fahrzeugen

abzuwehren. Genutzt wurde das Betriebssystem unter anderem im Konsortialprojekt IMMUNE, bei dem das Fraunhofer AISEC gemeinsam mit Partnern aus Wissenschaft und Industrie an einer SDN-Plattform [Glossar] für Industrie 4.0-Szenarien gearbeitet hat.

Beim vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekt 6G-ANNA veranschaulicht GyroidOS wie zukünftige 6G-Dienste abgesichert werden können. Die Forschungsergebnisse ermöglichen der Industrie konkrete Weiterentwicklungen, um in Zukunft cyberresiliente, verteilte Systeme aufzubauen. Cyberresiliente Systeme sollen in der Lage sein, Angriffe z. B. auf Geräte zu detektieren und – im Fall des Falles – betroffene Funktionen zu isolieren oder auf einen anderen Knoten zu migrieren, um trotz Angriff die Funktionalität sicher aufrechterhalten zu können. GyroidOS wird auch in dem ebenfalls am Institut entwickelten Trusted Connector eingesetzt, eines der Forschungsergebnisse der durch Fraunhofer angestoßenen Initiative International Data Spaces (IDS). »Der Trusted Connector ist eine Software, die eine sichere Ausführungsumgebung anbietet und IDS-Protokolle zum Datenaustausch sowie zur Interaktion mit einem Dienstebroker und einem Clearinghaus unterstützt«, erläutert Christian Banse.

Tools für den Security-Check

Neue nationale und europäische Regularien wie das wohl kommende European Union Cybersecurity Certification Scheme on Cloud Services (EUCS) fordern von den Unternehmen, ihre Datensouveränität weiter zu verbessern. »Unter Umständen sind noch nicht alle auf diese und andere Vorgaben eingestellt und müssen nun ihre Listen Punkt für Punkt abarbeiten, um zu überprüfen, ob sie die jeweiligen Anforderungen erfüllen«, sagt Banse. Um den Ablauf zu erleichtern hat das Fraunhofer AISEC das Tool Clouditor entwickelt. Es untersucht die Sicherheit der Cloud-Anbindungen und fasst alle Informationen für notwendige Änderungen oder ein späteres Audit zusammen. Ähnlich, allerdings mit Fokus auf Applikationen, arbeitet das Analysetool Codyze, das das Fraunhofer AISEC gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Verfügung stellt. Es überprüft den Krypto-Code von Programmen und meldet mögliche Auffälligkeiten beziehungsweise Schwachstellen. Sowohl der Clouditor als auch Codyze werden kontinuierlich weiterentwickelt und sind grundlegend auch für das von der Europäischen Kommission geförderte Projekt MEDINA, bei dem das Fraunhofer AISEC gemeinsam mit Partnern einen Baukasten entwickelt, um verschiedene Sicherheitsbewertungen auf Basis aktueller Standards automatisiert durchzuführen. Banse: »Unser Ziel ist es, Unternehmen und Institutionen ein je nach Anwendungsfall passendes Tool zur Verfügung zu stellen, mit dem sie Kontrollen ihrer Datensouveränität durchführen können.«

Glossar

*Beim Konzept **Software-defined Networking / SDN** liegt die Kontrolle über ein Netzwerk nicht auf der Hardware sondern der Software im zentralen Server des Netzwerks.*

Kontakt

Sascha Wessel
Abteilungsleiter Secure Operating Systems
Tel. +49 89 3229986-155
sascha.wessel@aisec.fraunhofer.de

Projekte

Clouditor
Der am Fraunhofer AISEC entwickelte Clouditor überprüft kontinuierlich Anforderungen an Dienste und Anwendungen und kann nachweisen, dass genutzte Cloud-Dienste zugesagte Sicherheits- oder Compliance-Anforderungen erfüllen.

Trusted Connector
Mit dem Trusted Connector, der 2021 das Label »IDS-ready« erhalten hat, stellt das Fraunhofer AISEC einen Ansatz zum sicheren Austausch von Daten über Unternehmensgrenzen hinweg vor – bei Kontrolle der Datenflüsse und der Datennutzung.

MEDINA
Ein Konsortium aus Industrie und Forschung bündelt im Projekt MEDINA Kompetenzen im Bereich Cloud-Sicherheit, um Sicherheitsbewertungen auf Basis zukünftiger Standards (d. h. europaweit einheitlicher Zertifizierungskataloge) zu automatisieren und die damit verbundene Einhaltung von Zertifizierungskriterien kontinuierlich zu überprüfen.

Codyze
Das von Fraunhofer AISEC und Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte automatisierte Analysetool Codyze unterstützt bei der Programmierung und Evaluierung sicherheitskritischer Software.

GyroidOS
Die am Fraunhofer AISEC entwickelte, auf IT-Sicherheit ausgerichtete Virtualisierungslösung GyroidOS isoliert besonders schützenswerte Anwendungen und Daten in Service-Containern, die von kritischen Komponenten abgekoppelt sind.

IMMUNE
Im Projekt IMMUNE entwickelt das Fraunhofer AISEC gemeinsam mit Partnern eine selbstverteidigende, resiliente SDN-Plattform für Industrie-4.0-Szenarien.

Clouditor

Trusted Connector

MEDINA

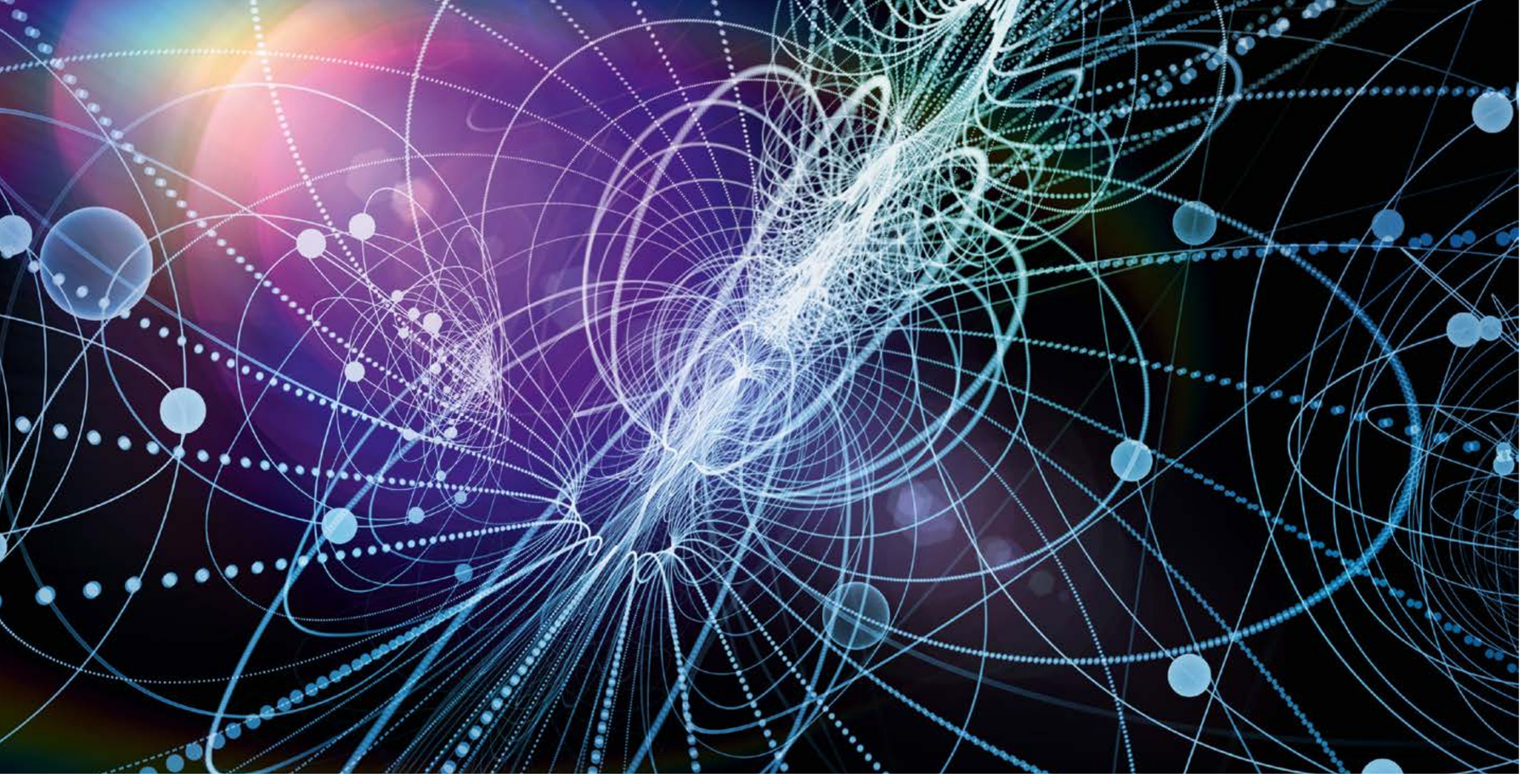
Codyze

GyroidOS

IMMUNE

Kontakt

Christian Banse
Abteilungsleiter Service and Application Security
Tel. +49 89 3229986-119
christian.banse@aisec.fraunhofer.de



Wir müssen mit allem rechnen

Im Interview sprechen Prof. Dr. Daniel Loebenberger, Prof. Dr. Marian Margraf und Dr. Matthias Hiller über Post-Quanten-Kryptografie (Post Quantum Cryptography / PQC) und die Vorbereitung der IT-Sicherheit auf das Quantenzeitalter.

Herr Prof. Dr. Loebenberger, Sie leiten die Abteilung Secure Infrastructure am Fraunhofer AISEC und sind, zusammen mit Prof. Dr. Margraf und Dr. Hiller, die Ansprechpartner des Kompetenzzentrums Post-Quanten-Kryptografie. Was bietet das PQC-Kompetenzzentrum Unternehmen und Einrichtungen konkret an?

Loebenberger: Wir unterstützen Unternehmen beim Umstieg auf Quanten-resistente Kryptografie. Im Grunde führen wir hier die geballte PQC-Kompetenz aus den einzelnen Abteilungen des Fraunhofer AISEC zusammen: Dazu gehören die Migration von PQC-Verfahren, Sicherheitsanalysen und das stetige Vorantreiben des Wissensstands bei PQC. Außerdem kümmern wir uns um Standardisierungen, bieten Schulungen an und bauen ein Informationsportal auf.

Einige der Angebote haben Sie auch auf dem jährlichen PQC-Netzwerk-Event umrissen, das das Fraunhofer AISEC seit 2022 veranstaltet.

Margraf: Dabei stand die Forschung im Vordergrund: von Protokollen und kryptografischen Aspekten über Implementierung, Kryptoagilität oder Domänenwissen bis zu Analysen. Ziel des Events ist es, verschiedenste Kompetenzen aus diesen Bereichen zu bündeln. Die Veranstaltung mit rund 200 Teilnehmenden aus Wissenschaft und Wirtschaft ist eine der größten zu PQC im deutschsprachigen Raum.

Das Interesse verdeutlicht auch die wachsende Relevanz der Post-Quanten-Kryptografie.

Loebenberger: PQC beschäftigt sich mit einer Bedrohungslage, die eintreffen könnte – also Konjunktiv, deren Eintreten allerdings extreme Auswirkungen hätte. Möglicherweise gibt es in den kommenden Jahren einen Quantencomputer, der die Verschlüsselungstechnik, wie wir sie heute anwenden, brechen kann und die IT-Sicherheit auf den Kopf stellt. Dass dieser Moment eintritt, ist zwar wahrscheinlich, wann das sein wird, wissen wir jedoch nicht.

Margraf: Das zeigt das Spannungsfeld, in dem sich Forschung und Praxis bewegen. Wenn es dazu kommt und Unternehmen und Institutionen nicht darauf vorbereitet sind, ist der Schaden kaum zu beziffern. Wir haben das intern als »kryptografisches Armageddon« bezeichnet. Wir müssen uns also auf diesen Fall vorbereiten. Und hier hilft eine einfache Weiterentwicklung aktueller Kryptoverfahren, z. B. die Erhöhung der Schlüssellänge nicht in jedem Fall.

Ebenso ist es häufig sehr kompliziert, die Kryptoverfahren auszutauschen, da die Infrastrukturen hierauf nicht vorbereitet sind. Deshalb arbeiten wir am Fraunhofer AISEC intensiv daran, wie Verschlüsselungen vorausschauend gegen Angriffe durch Quantencomputer gesichert werden können und wie die Wege in die Sicherheitsstrukturen der Zukunft aussehen müssen.

Loebenberger: Unser Ziel ist eine Art Kryptoagilität, die Unternehmen und Institutionen generell sicherer macht. Wir arbeiten daran, hybride Verfahren einzusetzen, die die bisherige Kryptographie mit PQC kombinieren. Gleichzeitig muss die Umsetzung bezahlbar sein.

Herr Prof. Margraf, Sie sind Abteilungsleiter von Secure Systems Engineering am Institut und unter anderem verantwortlich für das Projekt »Full-Lifecycle-Post-Quantum-PKI (FLOQI)«, dass auf diese hybriden Verfahren setzt.

Margraf: Richtig, bei FLOQI sind wir Teil eines Konsortialprojekts, in dem dieser Ansatz im Kontext von digitalen Zertifikaten praktisch umgesetzt werden soll. Wir wollen den Übergang von aktuellen zu neuen Verfahren so unterbrechungsfrei wie möglich gestalten. Dafür entwickeln wir Verfahren für Public-Key-Infrastrukturen, die den parallelen Einsatz von Quantencomputer-resistenten Verfahren heute schon ermöglichen.

Starken Praxisbezug hat auch das Projekt »Quantencomputerresistente Kryptografie in die Anwendung bringen«, kurz: Aquorypt. Herr Dr. Hiller, Sie leiten die Abteilung Hardware Security, die in diesem Konsortialprojekt arbeitet.

Hiller: Im Gemeinschaftsprojekt Aquorypt untersuchen wir die Anwendbarkeit und praktische Umsetzung von Quantencomputer-resistenten kryptografischen Verfahren bei eingebetteten Systemen und Chipkarten-basierten Sicherheitsanwendungen. Schwerpunkt ist dabei die Implementierung von PQC im Hinblick auf die Verwundbarkeit gegen Seitenkanalangriffe. Außerdem suchen wir nach möglichen neuen Angriffstechniken, um Cybergefahren richtig einzuschätzen und geeignete Abwehrmaßnahmen zu entwickeln.

Antworten auf die Frage »Was wäre wenn?« scheinen ein Treiber zu sein bei Ihren Forschungen zu PQC.

Loebenberger: Richtig. Neben der allgemeinen Forschung und unserem Informationsangebot etablieren wir aber beispielsweise auch Sicherheitsstandards, machen eine Bestandsaufnahme möglicher realer Angriffspunkte bei Unternehmen und migrieren praktische Anwendungen.

Margraf: Beispiele sind unsere Forschungen in Konsortialprojekten wie »Kryptografie-Bibliothek Botan: Langlebige Sicherheit für IT-Anwendungen und Dienste (KBLS)« und »Quanten-Sichere VPN-Module und -Operationsmodi (QuaSiModO)«. In KBLS implementieren wir Quantencomputer-resistente Verfahren in der Kryptobibliothek Botan und betrachten hier auch Mechanismen, die es Entwicklerinnen und Entwickler ermöglichen, effizient Kryptoalgorithmen austauschen zu können. Botan stellt lizenzfrei Krypto-Algorithmen zur Verfügung, die so angelegt sind, dass Implementierungsfehler vermieden werden können. Dieses Angebot haben wir nun um Post-Quanten-Algorithmen erweitert.

Hintergrund bei QuaSiModO ist, dass eine Implementierung von Post-Quanten-Mechanismen in virtuelle private Netzwerke aktuell noch deutliche Nachteile mit sich bringt, unter anderem weil das System störanfällig wird. Gemeinsam mit der Internet Engineering Task Force [Glossar] arbeiten wir daran, Standards zu entwickeln, die dieses Handicap verhindern können.

Vielen Dank für das Gespräch.

Glossar
*Die **Internet Engineering Task Force** ist eine Standardisierungsorganisation für das Internet und verantwortlich für die technischen Standards, aus denen sich das Internet-Protokoll zusammensetzt.*

Prof. Dr. Daniel Loebenberger spricht beim Workshop »Post-Quanten-Kryptografie« über Kryptoagilität und die Migration auf Quanten-resistente Verschlüsselungsverfahren.

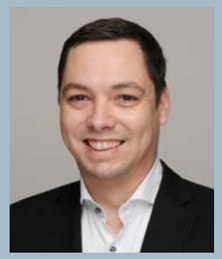
Projekte

FLOQI
Ziel des Projekts »Full-Lifecycle-Post-Quantum-PKI (FLOQI)« ist die Entwicklung einer Quantencomputer-resistenten PKI.

QuaSiModO
Im Projekt »Quanten-Sichere VPN-Module und -Operationsmodi (QuaSiModO)« werden neuartige Quantencomputer-resistente Algorithmen untersucht, getestet und umgesetzt.

KBLS
Die bestehende freie Kryptografie-Bibliothek Botan wird im Rahmen des Projekts »Kryptografie-Bibliothek Botan: Langlebige Sicherheit für IT-Anwendungen und Dienste (KBLS)« um Quantencomputer-resistente Verfahren erweitert.

Aquorypt
Das Projekt »Anwendbarkeit quantencomputerresistenter kryptografischer Verfahren (Aquorypt)« untersucht die Anwendbarkeit und praktische Umsetzung von Quantencomputer-resistenten kryptografischen Verfahren.



Kontakt

Prof. Dr. Daniel Loebenberger
Abteilungsleiter Secure Infrastructure
Tel. +49 89 3229986-139
daniel.loebenberger@aisec.fraunhofer.de

Prof. Dr. Marian Margraf
Abteilungsleiter Secure Systems Engineering
Tel. +49 89 3229986-152
marian.margraf@aisec.fraunhofer.de

Dr. Matthias Hiller
Abteilungsleiter Hardware Security
Tel. +49 89 3229986-162
matthias.hiller@aisec.fraunhofer.de

FLOQI

QuaSiModO

KBLS

Aquorypt

Das ***Kompetenzzentrum Post-Quanten-Kryptografie*** unterstützt beim Umstieg auf Quanten-resistente Kryptografie und Protokolle.

Die Hardware-Härter

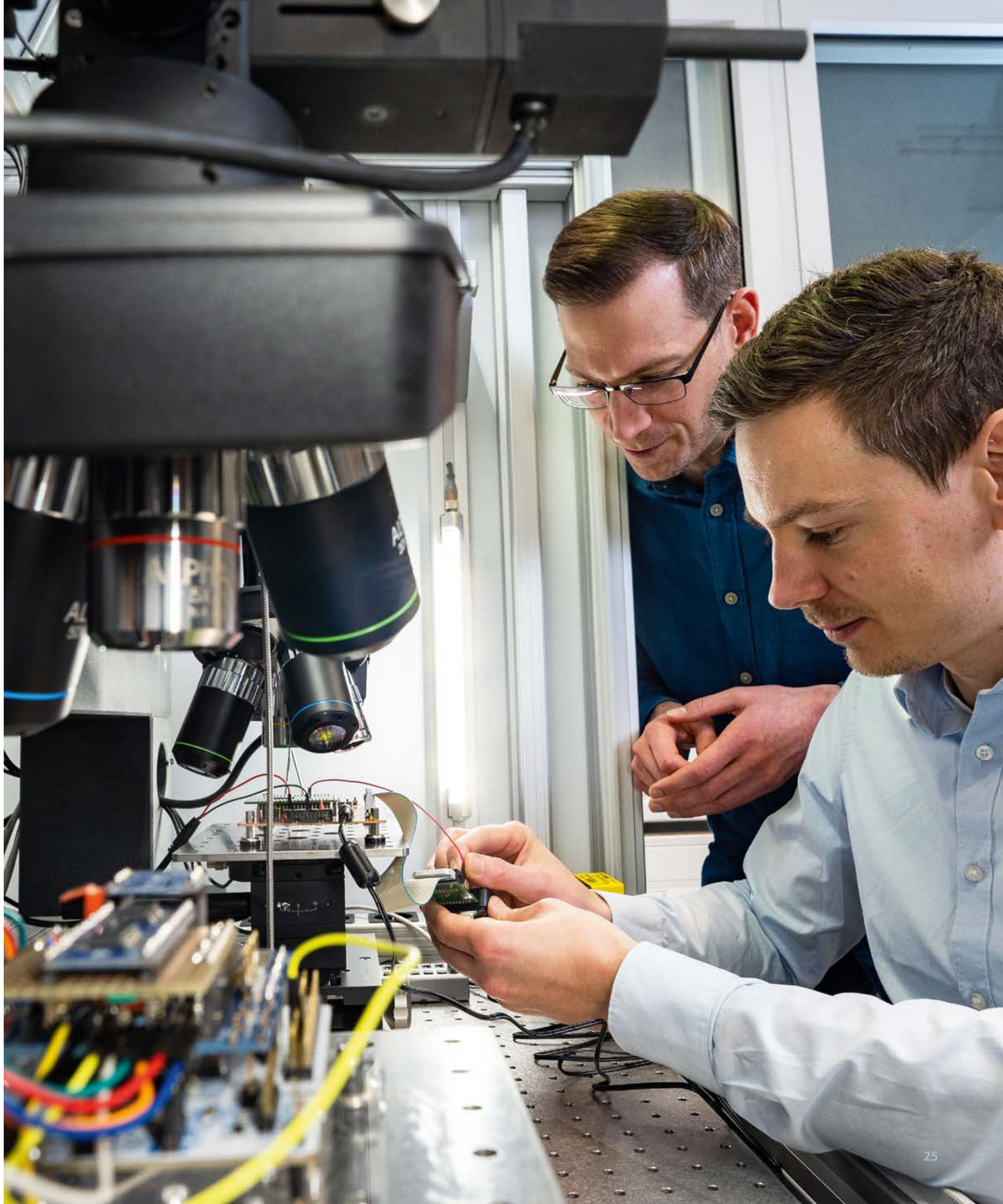
Security-Schwachstellen von Hardware-Komponenten wie Chips oder elektronische Schaltungen zu identifizieren, erfordert nicht nur umfassendes elektrotechnisches Know-how sondern auch tiefes Wissen über die notwendige Labortechnik. Das Fraunhofer AISEC besitzt beides und noch viel mehr.

Das Objekt der Begierde misst nur den Bruchteil eines Millimeters. Genau darüber, mit geringem Abstand, ist eine Nahfeldsonde platziert. »Jetzt«, sagt Dr. Matthias Hiller, und zeigt auf das angeschlossene Oszilloskop, »ist das Signal gut erfassbar und das Rauschen vertretbar gering.« Der Angriff auf den drei mal drei Millimeter großen, offen liegenden Chip und seine Millionen Transistoren kann starten. Von nun an wird die Sonde mikrometerweise weitergeführt, um feine, elektromagnetische Impulse auszulesen. An der richtigen Position zeigt sich eine Struktur in den Daten. Messung für Messung werden nun die Ergebnisse auf einen angeschlossenen Computer übertragen, um eine so genannte Seitenkanalanalyse [Glossar] durchzuführen. Dazu wird ein Baukasten verschiedener, aufeinander aufbauender Analysetools genutzt, um die Geheimnisse des vermeintlich sicheren Chips offenzulegen. Dafür benötigt man umfassendes Know-how, beispielsweise um spezielle Analysewerkzeuge zu entwickeln und zielgerichtet einzusetzen. Dabei ist Geduld erforderlich, denn es kann Tage, Wochen oder unter Umständen sogar Monate dauern, bis ein Chip seinen kryptografischen Schlüssel, und damit später seine damit verschlüsselten Daten, preisgibt.

Jetzt können Hiller und sein Team mit dem zweiten Teil ihrer Arbeit beginnen: Sie forschen nach Mechanismen, mit denen Prozessoren oder Mikrocontroller, sowie der darauf ausgeführte Code und auch FPGAs [Glossar] so gesichert werden können, dass Angriffe wie beispielsweise der durchgeführte Seitenkanalangriff künftig verhindert werden können. Dafür forschen die Sicherheitsexpertinnen und -experten am Fraunhofer AISEC an der Entwicklung sicherer Hardware, der sicheren, Seitenkanal-resistenten Implementierung kryptografischer Verfahren oder der Härtung von Prozessoren. »Unser Ziel ist es, unser Wissen über Angriffe und Gegenmaßnahmen kontinuierlich zu erweitern, damit wir Hardware-Komponenten, wie Chips oder Microcontroller, auch in Zukunft zuverlässig bewerten und verbessern können«, sagt Hiller. Um das Gesamtsicherheitsniveau der IT zu erhöhen, sei es entscheidend, auch deren »Grundpfeiler«, also die Hardware, abzusichern.

Im Angriffsmodus

Hiller ist Abteilungsleiter Hardware Security am Fraunhofer AISEC und damit auch wichtiger Ansprechpartner, wenn es um das fast 120 Quadratmeter umfassende Hardware Security Lab des Instituts geht. Über ein Dutzend Expertinnen und Experten setzen hier Tag für Tag auf Angriff. Die Seitenkanäle eines Chips sind dabei nur ein möglicher Weg. Auch Design- und Implementierungsfehler machen Spionage oder gar Sabotage möglich, indem beispielsweise die Buskommunikation abgehört, eine Debug-Schnittstelle ausgenutzt oder Speicher ausgelesen werden. Für Fault Injection-Angriffe



[Glossar], haben die Hardware-Härter am Fraunhofer AISEC einen eigenen Laborbereich reserviert, um hochpräzise Laser einzusetzen. An der High-End-Dual-Laser-Station beispielsweise können sie Werte auf einem Chip so gezielt verändern, dass er unter falschen Voraussetzungen weiterrechnet. »So kann man beispielsweise Schutzmaßnahmen im Chip umgehen oder Abläufe verändern«, sagt Hiller. Eine Alternative zu dieser Art von aktiven Eingriffen in das Chipverhalten sind sogenannte Glitching-Angriffe [Glossar], für die das Hardware Security Lab ebenfalls ausgestattet ist. Hier werden Versorgungsspannung oder Taktfrequenz für Bruchteile einer Sekunde geändert, um das System zu fehlerhaften Berechnungen zu zwingen.

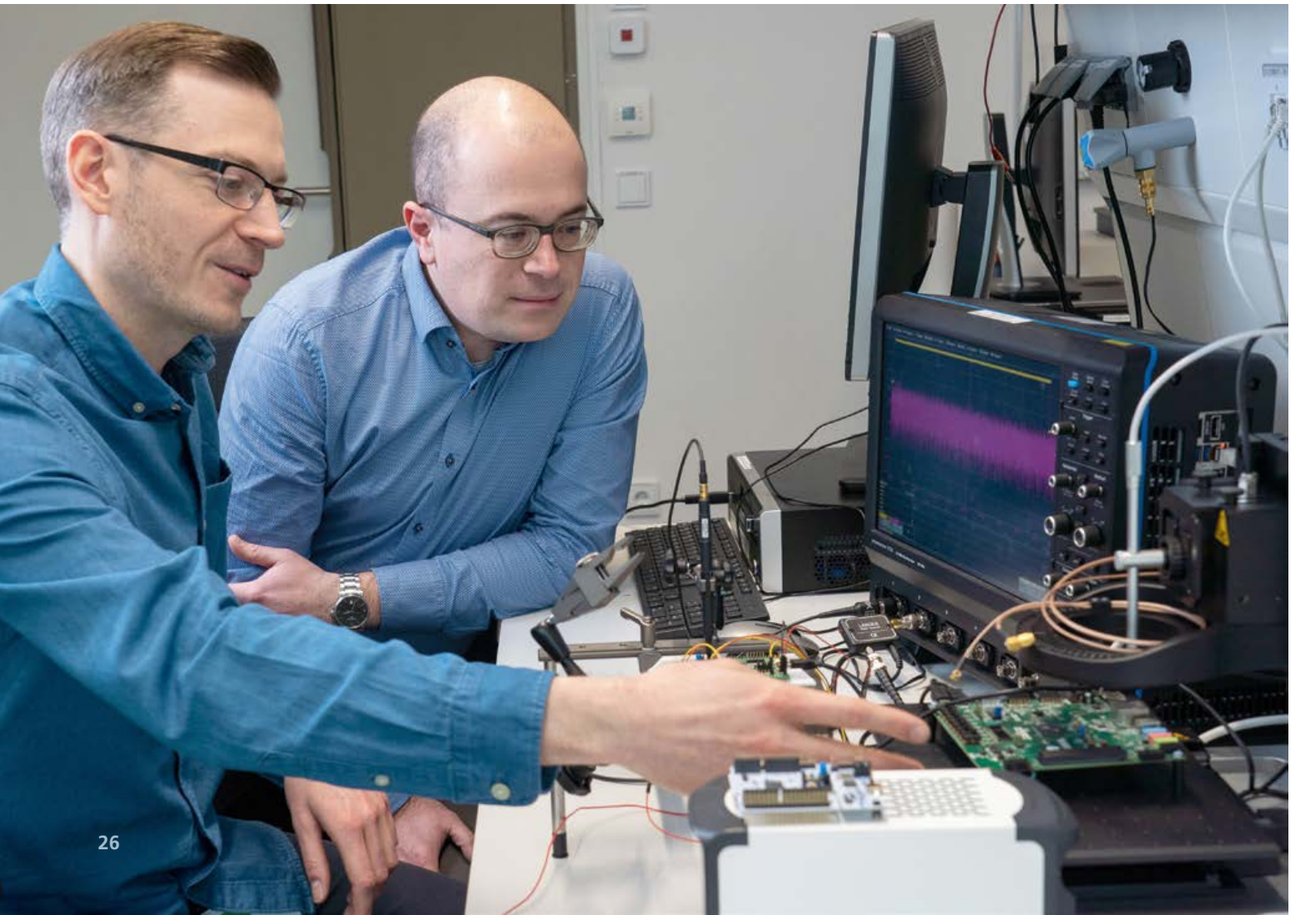
Industrielle Wertschöpfungskette absichern

Das Wissen, das sich das Team in den vergangenen fast 15 Jahren seit Gründung des Labors angeeignet hat, unterstützt nicht nur Kunden und Institutionen, die einen hohen oder höchsten Sicherheitsbedarf haben. Es fließt auch in die Entwicklung neuer und weitreichender Sicherheitssystematiken ein. Im Gemeinschaftsprojekt Velektronik beispielsweise, das vom Fraunhofer AISEC fachlich koordiniert wird, steht nicht eine bestimmte Hardware im Vordergrund, sondern die gesamte industrielle Wertschöpfungskette für Mikroelektronik. »Weil bei der Entwicklung und Produktion in der Regel zahlreiche Zulieferer, Designer und Produzenten rund um den Globus beteiligt sind, ist es bislang nahezu unmöglich, die Gewähr dafür zu übernehmen, dass in einem System wirklich nur das steckt, was auch spezifiziert wurde«, erklärt Hiller. Gemeinsam mit Partnern erforscht das Fraunhofer AISEC deshalb Möglichkeiten, wie Entwurfsmethoden, Analyse- und Fertigungsverfahren vertrauenswürdig gestaltet werden können, beispielsweise, um in jeden Chip einzigartige Merkmale einzubringen, über die die einzelnen Glieder der Wertschöpfungskette sicher nachverfolgt werden können. 2024 wollen die Kooperationspartner ein entsprechendes Portfolio an Konzepten und Methoden vorstellen, das dann über eine Plattform zugänglich sein wird.

Manipulationssicher durch Schutzfolie

Wie grundlegend die Zusammenarbeit des Fraunhofer AISEC mit den Expertinnnen und Experten anderer Fraunhofer-Institute ist, veranschaulicht die Gründung des Zentrum Trusted Electronic Bayern (TrEB). Dort arbeiten das Fraunhofer-Institut für Elektronische Mikrosysteme und Festkörper-Technologien EMFT und das Fraunhofer-Institut für Integrierte Schaltungen IIS eng mit den Hardware-Teams des Fraunhofer AISEC zusammen, um ein Kompetenzzentrum für die Forschung und Entwicklung sicherer und vertrauenswürdiger, integrierter Elektroniksysteme zu etablieren. »Eines der Ziele des vom Freistaat Bayern geförderten Projekts ist es, eine Schutzfolie zu entwickeln, mit der kritische Schaltungen manipulationssicher eingeschlossen und noch besser geschützt werden können«, sagt Hiller. Physische Manipulationen, insbesondere bei Systemen für Hochsicherheitsbereiche wie beispielsweise hoheitliche Ausweisdokumente sollen so ausgeschlossen werden. Der offene Standard RISC-V [Glossar] ermöglicht es, Prozessoren gezielt für die Einsatzzwecke bei Kunden zu entwickeln und nach ihren Anforderungen zu härten. Zudem wird das Hardware Security Lab kontinuierlich weiterentwickelt. »Der weitere Ausbau des Labors und das Forschen an immer ausgefeilteren Sicherheitsmechanismen sind entscheidend – auch für die Kunden, die in den kommenden Jahren zu uns kommen werden«, so Hiller. Denn nur so kann sichergestellt werden, dass die Sicherheit industrieller Hardware tatsächlichen Angriffen möglichst immer den entscheidenden Schritt voraus ist.

Im Hardware Lab analysieren Sicherheitexperten eingebettete Systeme gegenüber Hardware-basierten Angriffsvektoren.



Glossar

*Bei einer **Seitenkanalanalyse** wird die physische Implementierung eines Kryptosystems, z. B. Chipkarte, Hardware-Sicherheitsmodul, auf Schwachstellen hin untersucht.*

*Das **FPGA (Field-programmable gate array)** ist ein Mikrochip mit konfigurierbaren Schaltungsblöcken, der auch nach der Herstellung programmierbar bleibt.*

*Mit **Glitching-Angriffen** können Berechnungen von Prozessoren gezielt manipuliert werden.*

***RISC-V (Reduced instruction set computer)** ist ein Open-Source-Befehlssatz für die Ansteuerung von Prozessoren.*

***Fault Injection (Fehlerinjektion)** ist eine Testtechnik, um zu verstehen, wie sich Computersysteme verhalten, wenn sie auf ungewöhnliche Weise belastet werden.*

Kontakt

Dr. Matthias Hiller
Abteilungsleiter Hardware Security
Tel.+49 89 3229986-162
matthias.hiller@aisec.fraunhofer.de

Projekte

Velektronik
Bei Velektronik arbeiten die Leibniz-Gemeinschaft, die Forschungsfabrik Mikroelektronik, das edacentrum und die Fraunhofer-Gesellschaft für sichere, industrielle Wertschöpfungsketten in der Mikroelektronik zusammen.

TrEB
Das Zentrum Trusted Electronic Bayern (TrEB) etabliert Forschung und Entwicklung sicherer und vertrauenswürdiger, integrierter Elektroniksysteme.

Kompetenzlücken schließen

Vivija Čeprkalo-Simić ist Projektleiterin Lernlabor Cybersicherheit am Fraunhofer AISEC. Im Interview erklärt sie, wie die Weiterbildungsangebote des Lernlabors Unternehmen unterstützen und für wen sie geeignet sind. Im Mittelpunkt dabei: Trainings zu den Bereichen maschinelles Lernen, Fahrzeugkommunikation und Embedded Systems Security.

Warum sollten Unternehmen oder Behörden ihre Mitarbeitenden zum Lernlabor Cybersicherheit des Fraunhofer AISEC schicken?

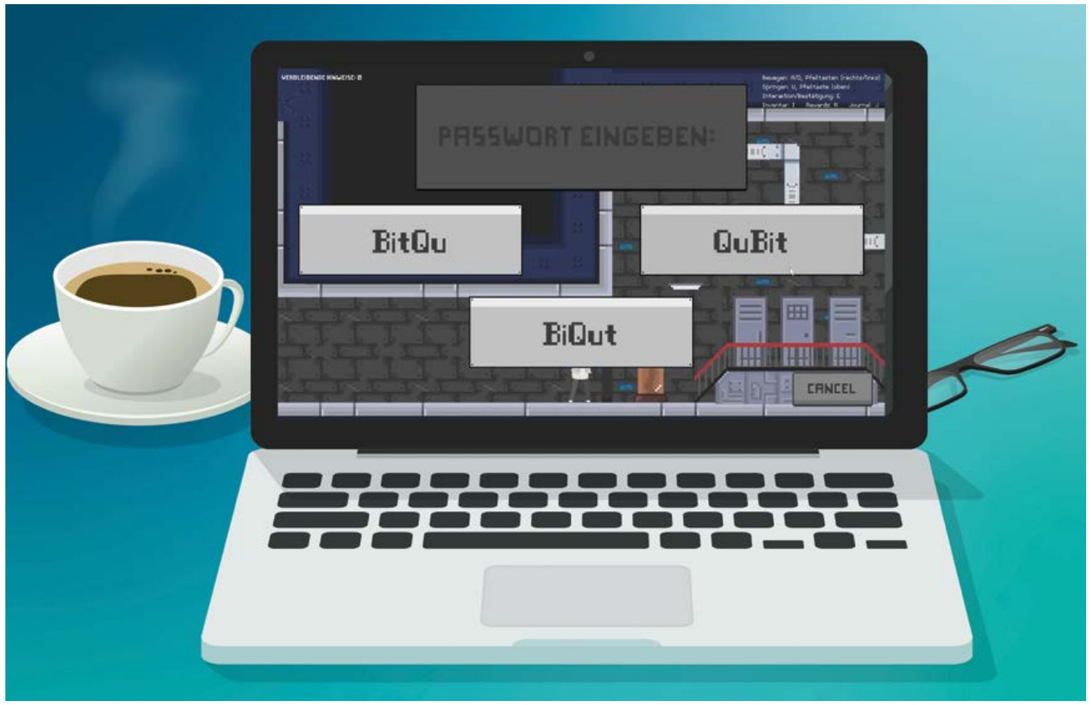
Wer bei uns war, kann die Gefahren für die IT-Sicherheit in seiner Einrichtung besser einschätzen und das Risiko minimieren. Wissen ist der Schlüssel dafür. Dieses Wissen bieten wir an – für Mitarbeitende vom Fach ebenso wie für Führungskräfte. Und das entweder in unseren Labors hier in Garching bei München oder in Weiden in der Oberpfalz. Oft finden die ein- oder zweitägigen Seminare und Workshops mit speziell auf die jeweilige Bedarfe ausgerichteten Inhalten aber auch bei den Unternehmen vor Ort statt.

Dabei geht es eher um das Update von Kompetenzen als um ein Upgrade im Sinne einer grundlegenden, allgemeinen Unterrichtung.

Verantwortliche für IT-Sicherheit müssen Cybergefahren richtig einschätzen, um sie abwehren zu können. Am Fraunhofer AISEC generieren wir Fachwissen, das wir über das Lernlabor Cybersicherheit in Unternehmen und öffentliche Einrichtungen weitertragen. Wir sind kein Schulungsunternehmen mit stringentem Lehrplan, das Wissen »von der Stange« anbietet. Unsere Arbeit orientiert sich einerseits an den realen Bedarfen unserer Industriekunden und deckt andererseits Zukunftsthemen ab, um unsere Kunden fit zu machen, zukünftige Herausforderungen im Bereich der Cybersicherheit zu beurteilen und frühzeitig geeignete Maßnahmen ergreifen zu können. Wir orientieren uns dabei sowohl an den Belangen der Unternehmen als auch an den gesetzlichen Anforderungen zur Erfüllung von Sicherheitskriterien. Die Trainings sind deshalb kompakt an die aktuelle Situation eines Unternehmens angepasst.

Welche Inhalte bieten Sie an und welche Themen waren in letzter Zeit besonders gefragt?

Das Lernlabor des Fraunhofer AISEC ist spezialisiert auf die Themenfelder Embedded Systems, Internet of Things und Mobile Security. Andere Fraunhofer-Institute bieten innerhalb des Lernlabor Cybersicherheit der Fraunhofer Academy Schulungen zu weiteren Schwerpunktthemen



Einblick in das Spiel »Charlie und die Quantenfabrik«

an. Im Fokus bei uns stehen Trainings etwa zum maschinellen Lernen für mehr Sicherheit, zur Absicherung FPGA-basierter Systeme, zur Fahrzeugkommunikation oder zur Hardware-gestützten Analyse von eingebetteten Systemen. Im vergangenen Jahr haben wir zudem eine sehr hohe Nachfrage zur Post-Quanten-Sicherheit erlebt. Das dürfte auch damit zusammenhängen, dass unser Institut hier führend in der Forschung ist. Auch Angebote zur Risikoanalyse werden häufig gebucht. Wir erstellen dann gemeinsam mit dem Unternehmen individuelle Lerninhalte, um möglichst bedarfsgerecht zu schulen.

Die Webseite des Lernlabors, die ich über die Homepage des Fraunhofer AISEC finde, gibt also nur einen ersten Überblick über mögliche Themen.

Richtig. Da wir uns bei unserem Angebot an Maßnahmen für ein Sicherheitsniveau auf hohem Level für spezifische Problemstellungen orientieren, wäre es nicht zielführend, generalisierte Trainings zu veranstalten. Deshalb werden Sie auf unserer Webseite eher Umrisse möglicher Themen finden. Wir konzipieren und erstellen die Trainings bedarfsgerecht – das ist unsere spezifische Herangehensweise, die auch die Unternehmen honorieren: 2022 ist der Ertrag aus den Schulungen um 50 Prozent gewachsen. Anfang des Jahres 2023 sind unsere Experten und Expertinnen bereits so gefragt, dass wir einzelne Trainings weit im Voraus planen müssen.

Die Dozentinnen und Dozenten sind nicht nur fachlich, sondern auch didaktisch Expertinnen und Experten?

Viele unserer Dozierenden bieten an Hochschulen Seminare und Vorlesungen an und haben dadurch auch didaktische Erfahrung. Sie arbeiten kontinuierlich daran, ihre Kompetenzen in diesem Bereich auszubauen. Zum Beispiel besuchen sie Train-the-Trainer-Kurse der Fraunhofer Academy, an die wir organisatorisch und inhaltlich angebunden sind.

Wie wichtig Ihnen Maßnahmen zur eingängigen Wissensvermittlung sind, zeigt »Charlie«, der zunächst gefangen scheint in einer Welt voller Quanten.

»Charlie und die Quantenfabrik« ist ein webbasiertes Computerspiel mit Rätseln und Mini-Games, das wir 2022 am Institut entwickelt haben, um einen eher spielerischen Einstieg in das Wissen zur Arbeitsweise von Quantencomputern zu ermöglichen. Niedrigschwellige Angebote wie diese waren 2022 beim Girls' Day ein großer Erfolg. Zusätzlich bieten wir auch kostenfreie Selbstlern-Kurse zum Einstieg in die Funktion und Anwendung von Quantencomputern an. Solche Verlinkungen zur interessierten Öffentlichkeit sind auch für uns wichtig, denn wir wollen Know-how auf verschiedensten Ebenen und über unterschiedliche Ansätze vermitteln. Serious Games und Online-Angebote sind ein Teil davon.

Beim Lernlabor Cybersicherheit gehört dazu auch der starke Bezug zur praktischen Umsetzung.

Das ist sogar grundlegend für uns, denn wir wollen Teilnehmenden und ihren Unternehmen einen konkreten Nutzen bieten. Deshalb bieten wir – im wahrsten Sinne des Wortes – Platz zur Erprobung passgenauer Lösungsstrategien an. Wir verfügen beispielsweise über einen modernen Schulungsraum mit einem eigenen, abgeschirmten Netz, in das wir Viren einspeisen können, um die praktische Abwehr zu trainieren. Dank unserer Labors – etwa für Hardwaresicherheit oder für industrielle und automobile Sicherheit – haben wir spezielle Demonstratoren und Instrumente, an denen unter anderem Seitenkanalangriffe oder Werkzeuge zur Absicherung der Kommunikation »ausprobiert« werden können. Dabei verknüpfen wir unsere Forschungen mit den laufenden und zu erwartenden Security-Problemstellungen von Unternehmen. Die Teilnehmenden kommen mit einem Anwendungswissen aus unseren Trainings, das sich nicht nur am aktuellen, sondern bereits am künftigen »Puls der Zeit« orientiert.

Lernlabor **Cybersicherheit**

Kontakt

Vivija Čeprkalo-Simić
Project Manager, Lernlabor Cybersicherheit
Tel.+49 89 3229986-138
vivija.ceprkalo@aisec.fraunhofer.de

Weiterbildung und Seminare rund um die IT-Sicherheit

Das **Lernlabor Cybersicherheit am Fraunhofer AISEC** ist spezialisiert auf die Themen Embedded Systems, Internet of Things und Mobile Security.

Das Serious Game **»Charlie und die Quantenfabrik«** ermöglicht einen spielerischen Einstieg in das Wissen zur Arbeitsweise von Quantencomputern.

Das **Lernlabor Cybersicherheit der Fraunhofer Academy** organisiert den Wissenstransfer aus den Fraunhofer-Instituten in die Praxis.

Fraunhofer Singapore wird zu einem Cybersicherheitszentrum

Zur Pressemitteilung

Fraunhofer Singapore, eine selbstständige Fraunhofer-Auslandsgesellschaft, ist seit 2022 ein Zentrum für Cybersicherheit (Fraunhofer Center for Applied and Integrated Security CAIS). Im Fokus der Forschungsaktivitäten steht die sichere Kommunikation mittels Quantentechnologie und Quantensicherheit. Partnerinstitut des Standorts in Singapur ist seit 2022 das Fraunhofer AISEC. Ein enger Kooperationspartner in Singapur ist die Nanyang Technological University (NTU). »Mit der Partnerschaft bauen wir unsere Kompetenzen in sicherer Quantenkommunikation systematisch aus, wovon auch unsere Kunden in Deutschland und Europa profitieren«, sagt Prof. Dr. Georg Sigl, Institutsleiter des Fraunhofer AISEC.

Zentrum für vertrauenswürdige Künstliche Intelligenz schafft diskriminierungsfreie KI

Zur Pressemitteilung

»KI-Systeme müssen diskriminierungsfrei arbeiten. Wir möchten das technisch garantieren«, sagt Prof. Dr. Marian Margraf, Abteilungsleiter der »Abteilung Secure Systems Engineering« am Fraunhofer AISEC in Berlin und Projektleiter für Grundlagenforschung am Zentrum für vertrauenswürdige künstliche Intelligenz (ZVKI). Das ZVKI schafft eine Basis für die Umsetzung verständlicher und vor allem sicherer KI-Systeme. Eine wichtige Rolle spielt dabei das Vertrauen in die Technologie. Um dieses aufzubauen und KI gemäß ethischen Grundsätzen nutzbar zu machen, müssen dafür die notwendigen Rahmenbedingungen geschaffen werden. Der Schutz von personenbezogenen Daten und die Nachvollziehbarkeit der Entscheidungen einer KI stellen dabei notwendige Komponenten dar. Ziel des ZVKI ist es, umfassend Regulierungsansätze herauszuarbeiten und ihre technische Umsetzbarkeit zu prüfen. Mit der Unterstützung des Bundesministeriums für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV) baut der unabhängige Think Tank iRights.Lab das Zentrum in Zusammenarbeit mit den Fraunhofer-Instituten AISEC und IAIS sowie der Freien Universität Berlin auf.

Prof. Dr. Claudia Eckert zieht in die Hall of Fame der deutschen Forschung ein

Seit mehr als 20 Jahren ist Prof. Dr. Claudia Eckert, Leiterin des Fraunhofer AISEC, einer der profiliertesten Köpfe für IT-Sicherheit. Als eine der führenden Informatikerinnen Deutschlands wird sie 2022 für ihren herausragenden Beitrag zur Forschung in der Cybersicherheit geehrt und in die Hall of Fame der deutschen Forschung berufen. Ihre Mission ist stets, durch exzellente IT-Sicherheitsforschung Lösungen zum unmittelbaren Nutzen für die Wirtschaft und zum Vorteil für die Gesellschaft zu schaffen. Die Hall of Fame der deutschen Forschung würdigt alljährlich Wissenschaftlerinnen und Wissenschaftler, die durch ihre Lebensleistung Deutschland als Wissenschafts- und Wirtschaftsstandort zukunftsfähig gemacht haben. Die Ehrung wurde 2009 vom manager magazin ins Leben gerufen. Seit 2015 wird die Auszeichnung gemeinsam mit dem Unternehmen Merck vergeben.

Zum Video-Portrait anlässlich der Preisverleihung

Cybersecurity-Blog gestartet

Das Fraunhofer AISEC hat im Juli 2022 mit dem Cybersecurity-Blog ein neues Format für Themen aus der IT-Sicherheitsforschung gestartet: Unsere Expertinnen und Experten bieten spannende Einblicke in ihre wissenschaftliche Arbeit. Die Blog-Artikel beschäftigen sich mit aktuellen und innovativen Themen u.a. rund um vertrauenswürdige KI, IoT Security, Post-Quanten-Kryptografie, White Hat Hacking, Secure Digital Identities und Industrial Security. Die Texte entspringen direkt aus der täglichen Forschungsarbeit der Wissenschaftlerinnen und Wissenschaftler, stellen neue wissenschaftliche Erkenntnisse vor oder liefern Lösungen für konkrete Problemstellungen. Interessierte erhalten Einblicke in die Forschungsschwerpunkte und in die Arbeitsweisen von IT-Sicherheitsforschenden.

Zum Cybersecurity-Blog

Unser Auftrag: Cybersicherheit bewerten, gestalten und bewahren

Im Spannungsfeld zwischen wirtschaftlichen Erfordernissen, Benutzerfreundlichkeit und Sicherheitsanforderungen beurteilen am Fraunhofer AISEC über 230 Cybersecurity-Spezialistinnen und Spezialisten systematisch die IT-Sicherheit von Produkten, vernetzten Systemen und Infrastrukturen, steigern ihre Robustheit gegen Angriffe und wahren ihre Sicherheit nachhaltig.

Bewerten: Vermessen, verstehen, beurteilen

Macht die Software das, und nur das, was ich erwarte? Sind ihre Entscheidungen nachvollziehbar? Woher stammen die Komponenten meiner Hardware?

Zur Bewertung der Vertrauenswürdigkeit von Systemen benötigt es Werkzeuge, um sie tiefgehend und möglichst automatisiert auf Schwachstellen zu untersuchen – über deren gesamten Lebenszyklus, vom Design über die Fertigung bzw. Programmierung und Integration in bestehende Systeme bis hin zum operativen Einsatz.

Die nötige Transparenz, um die Konsequenzen der Nutzung einer Hard- oder Software abzuschätzen, wird in den Testlabors des Fraunhofer AISEC geschaffen. Im Kundenauftrag sowie in Eigenforschung werden Funktions-, Interoperations-, Penetrations-, Konformitäts- und Compliance-Tests an vernetzten und eingebetteten Systemen, Hard- und Software-Produkten sowie webbasierten Diensten und Cloud-Angeboten durchgeführt. Durch strategische Allianzen mit internationalen Partnern und Universitäten basiert die Forschung auf neuesten wissenschaftlichen Erkenntnissen und Verfahren.

Gestalten: Konzipieren, kombinieren, härten

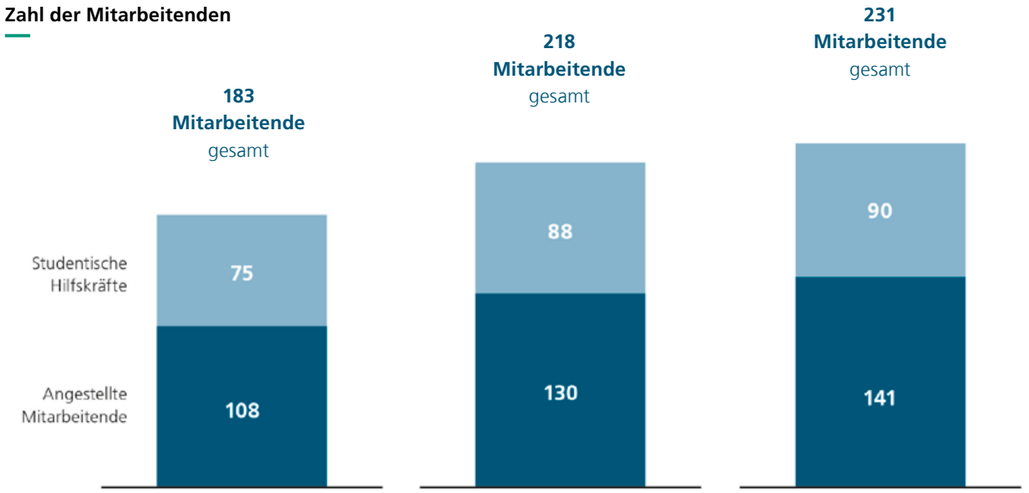
Die von den Forschenden entwickelten Sicherheitslösungen halten mit der steigenden Komplexität unserer IT-Systeme nicht nur Schritt, sondern sind den Angreifenden den entscheidenden Schritt voraus. Die maßgeschneiderten Sicherheitskonzepte sichern Daten und schützen wirksam vor Cyberkriminalität. Das gelingt durch vertrauenswürdige, sichere Designs, das sichere Einbinden sonst unsicherer Teile und die kontinuierliche Überwachung des Sicherheitszustands. Die Forschenden arbeiten eng mit global agierenden Industrieunternehmen sowie spezialisierten Unternehmen aus dem Mittelstand und der öffentlichen Hand zusammen. Sie kennen ihre Bedarfe, setzen Lösungen marktgerecht mit den Auftraggebern um und schulen sie darin, Entwicklungen in der Cybersicherheit fundiert zu bewerten sowie das eigene Sicherheitsniveau kontinuierlich auszubauen.

Bewahren: Erhalten, festigen, schützen

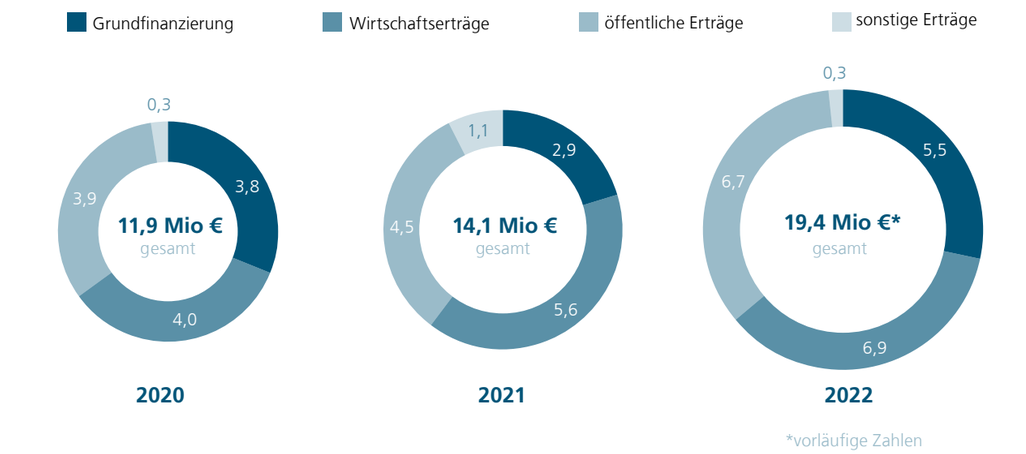
Mit den anwendungsorientierten Cybersecurity-Lösungen treffen die Kunden des Fraunhofer AISEC bereits heute Schutzvorkehrungen für morgen, die im Zuge des rasanten technologischen Fortschritts kontinuierlich bewertet und angepasst werden können. So bewahren sie die Integrität, Verfügbarkeit und Vertraulichkeit ihrer Daten und IT-Systeme nachhaltig. Die Forschung des Fraunhofer AISEC schützt nicht nur Privatpersonen, unsere Infrastruktur und Demokratie, sondern steigert auch die Wettbewerbsfähigkeit von Kunden sowie Partnern und liefert langfristig einen zentralen Beitrag zur digitalen Souveränität Deutschlands und Europas.

Zahlen und Daten

Zahl der Mitarbeitenden



Forschungsvolumen (in Mio €)

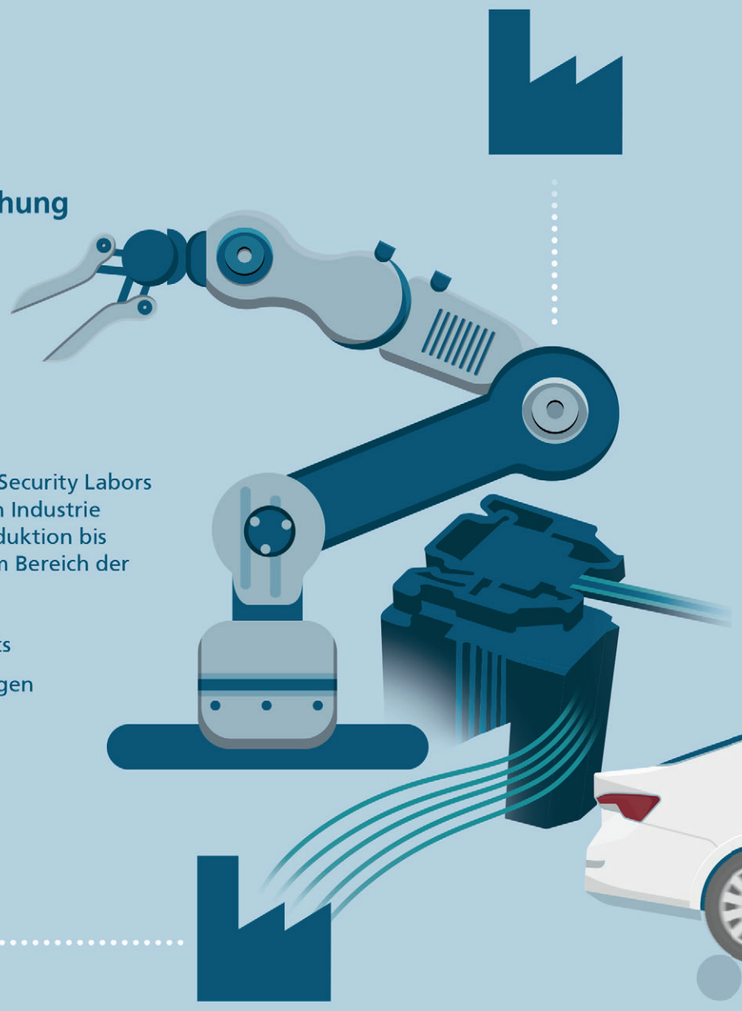


*vorläufige Zahlen

Laborlandschaft am Fraunhofer AISEC

Laborlandschaft am Fraunhofer AISEC

Maßgeschneiderte Lösungen, beruhend auf exzellenter Forschung



INDUSTRIAL SECURITY LAB

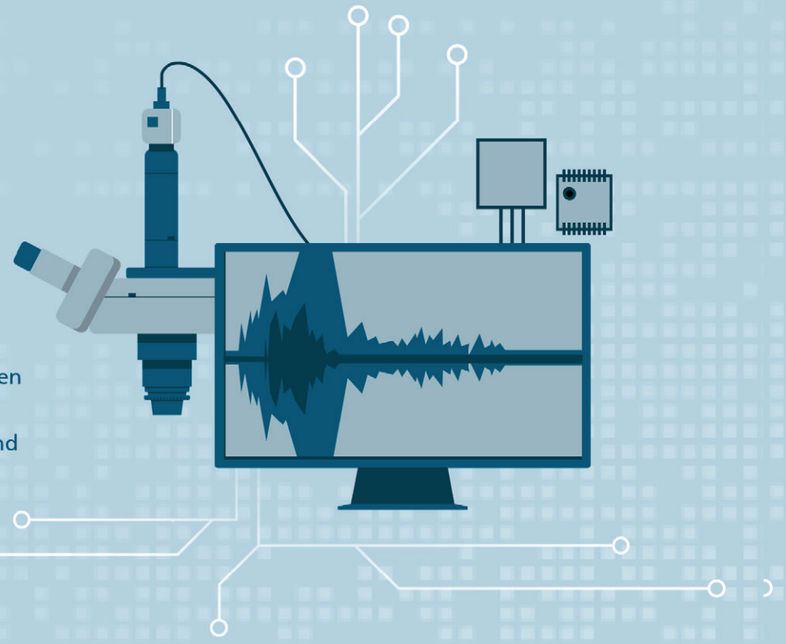
Das Angebotsspektrum der Industrial Security Labors reichen von Analysen in den Bereichen Industrie 4.0, Internet der Dinge, vernetzte Produktion bis hin zur Untersuchung der Sicherheit im Bereich der Gebäudeautomation.

- Risikoanalysen und Penetrationstests
- Realitätsnahe Simulationsumgebungen durch reale Komponenten
- Erhöhte Rechenkapazität für mehr Simulationen (AR und VR)

Hardware Security LAB

Das Hardware Security Labor bietet ein Spektrum an Hardware-Sicherheitsanalysen – darunter Penetrationstests, Seitenkanalanalysen sowie Angriffe auf Sicherheitsimplementierungen.

- Hochpräzise EM-Messungen für die Seitenkanalanalyse
- Sicherheitsevaluierung eingebetteter Systeme gegenüber Hardware-basierten Angriffsvektoren
- Mehrere Laserstationen für Vorder- und Rückseitenfehlerinjektion



AUTOMOTIVE SECURITY LAB

Das Automotive Security Labor ermöglicht Sicherheitsanalysen an kompletten Fahrzeugen sowie an mehreren, miteinander interagierenden Komponenten in einer gesicherten, vertrauenswürdigen Umgebung.

- Risikoanalysen und Penetrationstests
- Security Engineering und Methoden für die Fahrzeugentwicklung
- Entwicklung und Test von Security-Maßnahmen

LAB FÜR ISOLATIONS-MECHANISMEN

Das Labor für Isolationsmechanismen testet modularisierte Softwarestacks. Schwerpunkte sind Evaluationen von Isolationsmechanismen systemnaher Komponenten sowie das Beheben von Bugs.

SYSTEM SECURITY LAB

Das System Security Lab entwickelt und evaluiert sichere Systemlösungen für eingebettete und mobile Geräte und für Server. Hauptaugenmerk ist Resilienz und Resistenz gegenüber Angriffen.

SOFTWARE SECURITY LAB

Das Software Security Labor erforscht Ansätze zur Analyse und Härtung von Software. Ziel ist es, Schwachstellen in Programmen zu beheben und die Ausnutzung von Schwachstellen zu verhindern.

CLOUD SECURITY LAB

Das Cloud Security Labor ermöglicht eine Vielzahl von Dienstleistungen zur Evaluierung und Absicherung von Cloud-Diensten.

SMART SENSOR LAB

Das Smart Sensor Labor untersucht mit Hilfe von Software-Defined-Radio-Komponenten gängige Funkstandards und darauf aufsetzende IoT-Protokolle auf Schwachstellen.

IOT SECURTY LAB

Das Testlabor für IoT-Security analysiert Software von vernetzten Geräten und behebt Schwachstellen. Im Fokus stehen Geräte mit unvollständigem Source Code.

SECURE DATA ECOSYSTEMS

Das Labor Secure Data Ecosystems liefert die Infrastruktur für die Entwicklung, Planung und Umsetzung von vertrauenswürdigen Datenräumen für Cloud- und Edge-Computing.

Fraunhofer AISEC – A great place to work

Zehn Gründe am Fraunhofer AISEC zu arbeiten

Die Vielfalt der Cybersicherheits-Forschung in unterschiedlichen Anwendungsfeldern erfahren.

In einem Forschungsfeld tätig sein, das immer relevanter wird: Cybersicherheit.

Die Usability und Vertrauenswürdigkeit von digitalen Anwendungen erhöhen.

Sicherheitsrelevante Schwachstellen sowohl in Hardware als auch in Software finden und schließen.

In modern ausgestatteten Cybersicherheitslaboren forschen.

Neueste Forschungsergebnisse in die Praxis bringen und anwenden.

Praktisch arbeiten und gleichzeitig im gewünschten Themenfeld promovieren.

Forschung und Industrie zusammenbringen und beide Welten verbinden.

Mit flexiblen Arbeitszeiten und mobilem Arbeiten das Berufliche gut mit dem Privaten ausbalancieren.

Den aktuellen Stand der Cybersicherheit nutzen, mit hohem Tempo vorantreiben und sich schnell weiterentwickeln.

Auszeichnungen der Fraunhofer-Gesellschaft als Arbeitgeber

glassdoor BESTE ARBEITGEBER 2022

2. PLATZ Attraktivste Arbeitgeber 2022 Für Absolventen Forschung Informatik trendence

Most Attractive Employers universum 2022

Most Attractive Employers Germany universum 2022

Mitglieder des Kuratoriums

Dr.-Ing. Stefan Hofschen
Sprecher des Kuratoriums,
Vorsitzender der Geschäftsführung,
Bundesdruckerei GmbH

Naby Diaw
Chief Information Security Officer,
Vice President, Lufthansa Group

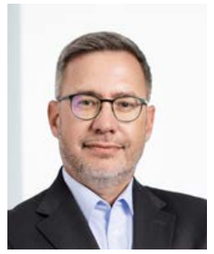
Dr. Astrid Elbe
Vice President Product Development,
Aviat Networks

Prof. Dr.-Ing. Georg Carle
Lehrstuhl für Netzarchitekturen und Netzdienste, Fakultät für Informatik,
Technische Universität München

Andreas Könen
Abteilungsleiter »Cyber- und IT-Sicherheit«, Bundesministerium des Innern und für Heimat (BMI)

Dr. Manfred Paeschke
Chief Visionary Officer,
Bundesdruckerei GmbH

Dr.-Ing. Heike Prasse
Referatsleiterin »Kommunikation und Sicherheit digitaler Systeme«, Bundesministerium für Bildung und Forschung (BMBF)



Thomas Rosteck
Division President Connected Secure Systems, Infineon Technologies AG

Dr. Stefan Wimbauer
Referatsleiter »Angewandte Forschung, Cluster-Politik«, Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie

Dr. Bettina Horster
Vorstand
VIVAI Software AG

Dr. Andreas Kind
Vice President Cybersecurity & Trust, Head of Technology SiGREEN, Siemens AG

Prof. Dr. Dr. h.c. Mira Mezini
Leiterin Fachgebiet Softwaretechnik,
Fachbereich Informatik,
Technische Universität Darmstadt

Vera Schneevoigt
ehem. Chief Digital Officer / Senior Vice President Engineering,
Bosch Sicherheitssysteme GmbH

Neutraler Technologielieferant der Datenwirtschaft

Die Digitalisierung verbessert Prozesse sowie Produkte und schafft neue Geschäftsmodelle nur dann, wenn Daten vertrauenswürdig und automatisiert erfasst, gespeichert und genutzt werden. Für dieses Ziel vereint der Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT neueste wissenschaftliche Erkenntnisse, Know-how und Lösungskompetenz entlang der gesamten digitalen Wertschöpfungskette. Das Fraunhofer AISEC ist Sprecher-Institut des Clusters und deckt in den Projekten die Security-Bereiche ab.

In Deutschland stagniert die Digitalisierung. Das zeigt der Digitalisierungsindex [Glossar] des Bundesministeriums für Wirtschaft und Klimaschutz (BMWK): So stieg der Durchschnittswert 2022 nur um einen Punkt auf 108,9 Punkte. Zum Vergleich: Der Branchen-Spitzenreiter »Informations- und Kommunikationstechnologie« erreichte einen Indexwert von 275,9 Punkten. Es ist also noch ein langer Weg bis aus der branchenübergreifenden, sicheren Zusammenführung von Daten ein energie- und kosteneffizienterer Ressourceneinsatz, Prozessverbesserungen, Produktinnovationen oder neue Geschäftsmodelle entstehen.

Daten und Nutzende zusammenbringen

Damit die Vision einer digitalen Wirtschaft Realität wird, müssen zahlreiche Akteure sehr viele Daten aus heterogenen Datenquellen, wie z. B. von Sensoren in mobilen Endgeräten und in Maschinen, oder gespeicherte Dokumentationen sowie ganze Produktionsprozesse erfassen, zusammenführen bzw. austauschen und automatisiert analysieren, verarbeiten und in Mehrwert-Diensten zur Anwendung bringen. Das Austauschen und Anwenden muss vertrauenswürdig und aufgrund der großen Datenmenge automatisiert erfolgen. Erst dann werden Daten »intelligent«, lassen sich, z. B. indem man Techniken des maschinellen Lernens (ML) anwendet, neue Erkenntnisse aus ihnen gewinnen, die notwendig sind, um Prozess- und Produktinnovationen zu ermöglichen. Ein Beispiel ist der Datenraum zu Catena-X, der aktuell entsteht. Dort treffen sehr heterogene Datensätze, z. B. Daten aus der Nutzung von Produkten bis hin zu Produktionsdaten, auf sehr unterschiedliche Anwenderbedarfe, wie z. B. die Optimierung der Warenrückverfolgbarkeit oder die Reduzierung des CO_2-Fußabdrucks. Zudem sind Technologiebereiche, die für den Aufbau des Datenraums notwendig sind, wie z. B. Elektronik-Komponenten der Hardware und Software-Apps, durch sehr unterschiedliche Entwicklungszeiten und Verwertungspfade charakterisiert. »All diese Aspekte im Sinne der Vision einer funktionsfähigen und vertrauenswürdigen digitalen Wirtschaft zusammenzubringen, ist eine komplexe Aufgabe«, sagt Michael Fritz, Leiter der Geschäftsstelle des Fraunhofer CCIT.

Technologien entlang der gesamten Daten-Wertschöpfungskette

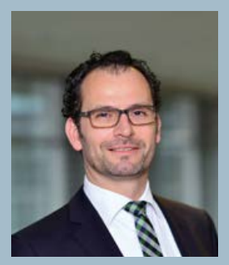
Der Fraunhofer CCIT hat sich zur Aufgabe gemacht, einen wesentlichen Teil zur Lösung dieser Herausforderung beizutragen. Als einer der wenigen Akteure am Markt vereint er neuste wissenschaftliche Erkenntnisse, Know-how und Lösungskompetenz entlang der gesamten Daten-Wertschöpfungskette und kann als neutraler Technologielieferant ein für alle Beteiligten offenes System anbieten. Der Cluster kombiniert die Vorlaufforschung mit der angewandten Forschung der Fraunhofer-Institute über interdisziplinäre Fachgrenzen hinweg. »Anwender- und Technologie-Institute arbeiten Hand in Hand und gehen Industrie-relevante Problemstellungen gemeinsam und Hersteller-neutral an«, sagt Fritz. Partner und Kunden profitieren von Lösungen, die den Reifegrad eines Proof-of-Concept-Status haben, und von Wissen, wie verschiedene Technologien für eine marktfähige Gesamtlösung miteinander kombiniert werden können. Dafür bringen die Expertinnen und Experten des Fraunhofer CCIT Ergebnisse der Vorlaufforschung, die bereits Produktcharakter haben, zusammen und adaptieren sie gemeinsam mit den Kunden auf deren Anwendungsfall, oder passen spezifisches Technologie-Know-how gemeinsam mit dem Anwendenden nach dessen jeweiliger Spezifikation an. Durch den intensiven Austausch entstehen ganz konkrete Lösungen mit klar definiertem Mehrwert. Beispiele aus 2022 sind der intelligente Nutenstein, die intelligente Kreuzung und die intelligente Schraube.

Auf dem Weg zum Edge Cloud Continuum

»2022 haben wir die Fortsetzung des Trends einer verstärkten Cloud-Nutzung, eine erhöhte Nachfrage nach Cybersecurity sowie nach Sprach-Assistenz-Systemen im industriellen Umfeld gesehen. Diese Entwicklung wird sich auch 2023 fortsetzen«, sagt Fritz. 2023 will der Cluster daher das Thema »Edge Cloud Continuum« vorantreiben. Der noch junge Begriff steht für eine durchgängige Daten-Wertschöpfungskette, vom Sensor über Edge-Devices bis in Cloud-Plattformen. Das Continuum ist als eine intelligente, verteilte Managementsoftware zu verstehen, in der die Verarbeitung der Daten automatisiert so organisiert wird, dass die von den Kunden vorgegebenen Ziele, wie z. B. ein minimaler CO_2-Fußabdruck oder ein hohes Maß an Sicherheit durchgängig nachvollziehbar umgesetzt werden. »Neben einer Potentialanalyse bringen wir die relevanten Stakeholder zusammen, ermitteln die notwendigen Forschungsbedarfe und definieren konkrete Anwendungsfälle«, sagt Fritz.

Glossar

*Der **Digitalisierungsindex** misst jährlich den Stand der Digitalisierung der Wirtschaft am Standort Deutschland mithilfe von 37 Indikatoren.*



Kontakt

Michael Fritz
Leiter der Geschäftsstelle, Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT
Tel. +49 89 3229986-1026
michael.fritz@aisec.fraunhofer.de

Projekte

Der **intelligente Nutenstein smartNotch** erhöht mithilfe kognitiver Transformation von Industrieprozessen die Effizienz von Umformmaschinen.

Bei der **intelligenten Kreuzung** kommt ein neuartiges Sensorsystem zum Einsatz, das Verkehrsdaten an beliebigen Orten entlang der Straße datenschutzkonform KI-basiert zusammenführt und analysiert.

Die **intelligente Schraube** kann jederzeit per Fernüberwachung kontrolliert werden, erhöht so die Sicherheit und senkt den Aufwand für Inspektionen.

Thomas Caspers

Direktor, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Welche Themen haben das BSI 2022 beschäftigt und warum? Welche sehen Sie für 2023?

Die Bedrohung im Cyberraum stellte sich 2022 für das BSI so hoch wie nie dar. Ransomware war dabei das ganz zentrale Risiko für den sicheren Betrieb von IT-Infrastrukturen, vor allem auch in Unternehmen. Neue Bedrohungen im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine, denen wirksam begegnet werden musste, kamen hinzu. 2023 werden auch technologische Entwicklungen mit disruptivem Potential alle fordern, die – wie das BSI – umfassende wie umsetzbare Lösungen zur Gewährleistung der IT-Sicherheit verfügbar machen müssen. Das BSI arbeitet daher in Bereichen wie Künstliche Intelligenz, Kryptografie und Quantencomputing intensiv mit weltweit führenden Forschungseinrichtungen in den gesellschaftlich und politisch zu Recht mit hohen Erwartungen verbundenen Fragen der IT-Sicherheit zusammen.

Zu welchen Themen haben Sie 2022 mit dem Fraunhofer AISEC zusammengearbeitet und welche stehen 2023 an?

Schwerpunkt 2022 war die Hardware-Sicherheit von Mikrocontrollern, die breite Verwendung in der Industrie finden. Zertifizierte Chips bieten ein sehr hohes Sicherheitsniveau. In vielen Bereichen werden aber oftmals handelsübliche Chips verwendet, die Hardware-basierten Angriffen nicht standhalten.

Ein prominentes Beispiel war 2022 der Hack des Starlink-Systems – mit potenziell sehr schädlichen Auswirkungen. Mit dem Fraunhofer AISEC hat das BSI in einer Studie untersucht, welche Angriffspfade auf Mikrocontroller existieren und wie Gegenmaßnahmen umsetzbar sind. Auch wenn Gegenmaßnahmen Angriffe nicht vollständig verhindern, können sie doch die Aufwände für einen Angreifer soweit in die Höhe treiben, dass entsprechende Angriffsversuche nicht mehr attraktiv sind.

System-On-A-Chip-Systeme (SoCs) [Glossar] folgen dem Trend in der Industrie nach immer höherer Integration. Statt separaten Chips wird Sicherheitsfunktionalität dabei direkt in den SoC als Subsystem integriert. Aufgrund der hohen Komplexität ist ein solcher Integrationsschritt aber nicht trivial. Die Fragestellung, ob zuvor getätigte Sicherheitsaussagen über ein Subsystem auch nach der Integration noch gültig sind, welche Sicherheitslücken potenziell entstehen und wie diesen begegnet werden kann, steht 2023 im Mittelpunkt der Zusammenarbeit des BSI mit dem Fraunhofer AISEC.

Warum haben Sie sich für das Fraunhofer AISEC als Partner entschieden?

Entscheidend für die Zusammenarbeit ist neben der erforderlichen Wirtschaftlichkeit insbesondere die hohe fachliche Expertise des Fraunhofer AISEC im Bereich Hardware-Sicherheit, die etwa mit zahlreichen wissenschaftlichen Publikationen fortwährend unter Beweis gestellt wird. Hier ist für das BSI von unmittelbarer Bedeutung, dass gewonnene Erkenntnisse nicht reine Grundlagenforschung sind, sondern einen hohen Praxisbezug aufweisen und damit direkt in die fachlichen Arbeiten des BSI einfließen können. Daher ist für das BSI ein kritischer Erfolgsfaktor, dass die umfangreiche technische Ausstattung des Fraunhofer AISEC stets die Umsetzung von sehr anspruchsvollen Präparations- und Analysearbeiten im Bereich der Chipsicherheit ermöglicht.

Thomas Caspers ist Leiter der Abteilung Technik-Kompetenzzentren und Direktor beim Bundesamt für Sicherheit in der Informationstechnik (BSI).

Glossar

*Bei einem **System-on-a-Chip** bzw. einer monolithischen Integration sind alle oder ein Großteil der Funktionen eines programmierbaren elektronischen Systems auf einem Chip verbaut.*

Dirk Kretzschmar

Geschäftsführer, TÜV Informationstechnik GmbH (TÜViT)

Wo sehen Sie derzeit die größten Herausforderungen in der IT-Sicherheit?

Es gibt aktuell zahlreiche große Herausforderungen in der IT-Sicherheit, die von verschiedenen Faktoren beeinflusst werden. Dazu gehört die zunehmende Professionalisierung, Spezialisierung und somit resultierende Arbeitsteilung von Cyberkriminellen. Angreifende bedienen sich umfangreicher konfektionierter Dienstleistungsangebote aus dem Darknet, sind also selbst nicht mehr unbedingt die Experten für das Ausnutzen von Schwachstellen. Somit treten immer mehr hochkriminelle und skrupellose neue Player in der Szene auf, die nur darauf aus sind, mit geringem Risiko finanzielle Gewinne zu erzielen.

Die größte Herausforderung sehe ich aber noch immer in zu vielen Chefetagen, die sich ihrer Verantwortung nicht bewusst sind – eben, weil sie sich die Risiken gar nicht vorstellen können und diese eher anzweifeln. Viele wissen einfach nicht, dass Cyberkriminelle sich schon monatelang Zugang verschafft haben, bevor sie den Angriff starten.

Welchen Handlungsbedarf sehen Sie, um Zuverlässigkeit und Sicherheit von KI-Systemen zu erhöhen?

Ich bin der Überzeugung, dass es nicht ausreicht, sich allein auf die gängigen KI-Entwicklungsprozesse, die dazugehörigen Trainingsdaten und reine Funktionsprüfungen zu verlassen. Viele haben ein ungutes Gefühl, sprichwörtlich das Lenkrad einer KI zu überlassen. Dabei spielen insbesondere Kontrollverlust und ein unvorhersehbares Verhalten von KI-Lösungen eine große Rolle.

Fakt ist aber auch, dass KI-Lösungen vorsätzlich getäuscht werden können. Entscheidungen könnten darüber in die eine oder andere Richtung manipuliert und in sensiblen und kritischen Anwendungsszenarien katastrophale Auswirkungen verursachen. Das ist ganz klar ein Thema der IT-Sicherheit, also auch hier der Schutz vor dem Ausnutzen von Schwachstellen der KI. Der Fachbegriff dafür ist: Adversarial Attacks. Über spezielle Stresstests können KI-Lösungen sehr umfangreich auf ihre Widerstandsfähigkeit gegen solche Angriffe geprüft und Aussagen über die Robustheit in bestimmten Anwendungsszenarien getroffen werden. Als Handlungsbedarf sehe ich daher die verpflichtende Prüfung von KI-Lösungen in sensiblen Bereichen.

Was schätzen Sie und Ihre Kollegen an der Zusammenarbeit mit dem Fraunhofer AISEC?

TÜViT arbeitet schon sehr lange erfolgreich mit dem Fraunhofer AISEC im Umfeld der IT-Sicherheit zusammen. Das Fraunhofer AISEC ist ein renommiertes Institut für angewandte Forschung im Bereich der IT-Sicherheit. Die Expertise und Erfahrung des Instituts in diesem Bereich ist hochgeschätzt und wird von vielen Unternehmen und Institutionen weltweit genutzt.

Unsere Herausforderung ist, insbesondere bei neuen Technologien am Markt, geeignete und verlässliche Prüfverfahren zu deren IT-Sicherheit zu entwickeln. Das geht nicht ohne umfangreiche Forschung, aber für Forschungsarbeit ist die TÜViT als Prüfstelle nicht aufgestellt. Die Zusammenarbeit mit dem Fraunhofer AISEC ermöglicht es uns, über die Forschungsergebnisse die Prüfung von IT-Sicherheit in vielen Branchen und Anwendungsbereichen zu verbessern. So auch im Falle zur Entwicklung eines Frameworks zur Prüfung von KI.

Insgesamt kann die Zusammenarbeit mit dem Fraunhofer AISEC als äußerst wertvoll angesehen werden, um die IT-Sicherheit zu verbessern und Risiken zu minimieren.

Dirk Kretzschmar ist Geschäftsführer TÜV Informationstechnik GmbH (TÜViT) und Mitglied der Konzerngeschäftsleitung TÜV NORD GROUP.

Sandra Kostic

Leitung der Forschungsgruppe »Usable Security & Privacy«

Die Entwicklung von Applikationen ohne Einbeziehung der Nutzenden birgt das Risiko, dass Sicherheitsmechanismen nicht richtig verstanden und als Folge nicht korrekt angewendet werden. Dies bei sicherheitsrelevanten Applikationen zu verhindern, ist Aufgabe der Usable Security.«

Mit dieser Devise übernahm Sandra Kostic im Herbst 2022 die Leitung der Forschungsgruppe »Usable Security & Privacy« am Berliner Standort des Fraunhofer AISEC. Für die Informatikerin wird zu selten die Gebrauchstauglichkeit einer Anwendung bedacht. Daher hat sie sich mit ihrem fünfköpfigen Team der systematischen Beurteilung und Förderung der Benutzbarkeit von IT-basierten Systemen und der Stärkung des Vertrauens in die Sicherheit dieser Systeme verschrieben.

Den Weg, Cybersicherheits-Maßnahmen nutzbarer zu machen, schlug Sandra bereits im Bachelorstudium in Informatik ein, als sie sich der Arbeitsgruppe »ID-Management« der Freien Universität Berlin unter der Leitung von Prof. Dr. Marian Margraf anschloss. Die benutzerorientierte IT-Sicherheitsforschung verbindet für die vielseitig interessierte Wissenschaftlerin den pragmatischen Technologieansatz der Informatik mit der Kreativität des Designs und bietet gleichzeitig Einblicke in diverse Branchen. Denn Benutzerfreundlichkeit und benutzbare Sicherheit werden überall benötigt – von der Hardware, wie einer simplen Fernbedienung, über den intelligenten Fernseher im Smart-Home bis hin zu komplexen Anwendungen mit sehr hohen Sicherheitsanforderungen, wie dem Umgang mit sensiblen digitalen Patientendaten. Sobald bei der Konzeption einer Anwendung eine Interaktion mit Nutzenden vorgesehen ist, ist die Expertise der Berlinerin über die Bedarfe, Kenntnisse und Fähigkeiten der Nutzenden gefragt.

Praxisnahe Forschung an sicheren digitalen Identitäten

Die Gelegenheit, ihr Wissen in konkrete Lösungen einfließen zu lassen, bot sich der Forscherin 2020 am Fraunhofer AISEC, als sie die Leitung des Projekts »ONCE« übernahm. Aufbauend auf ihren Masterabschluss in Informatik sowie ihrer Forschungserfahrung im Bereich digitaler Identitäten an der FU Berlin entwickelt sie hier mit Industriepartnern sichere, nutzerfreundliche Wallet-Lösungen, mit denen Bürgerinnen und Bürger unterschiedliche Ausweisdokumente, wie ihren Personalausweis oder Führerschein, Tickets oder Kundenkarten, geschützt auf ihrem Smartphone hinterlegen und sich sicher digital ausweisen können.

Schlüssel für den Erfolg einer solchen Anwendung ist für Sandra die Berücksichtigung der Perspektive der Nutzenden sowie die Einbindung der Usable-Security-Expertise bereits zu Beginn der Konzeptionsphase. Die Terminologie und Gestaltung der Anwendungsoberfläche sowie der Interaktionsfluss entscheiden darüber, ob Nutzende oder Programmierende der Anwendung vertrauen und sie so verwenden, dass Security-Features greifen. Dabei helfen Sandra ihre Abschlüsse in Graphic Design sowie User Interface (UI) und User Experience (UX) des California Institute of the Arts, die sie während ihrer Zeit am Fraunhofer AISEC erwarb.

Was genau das Vertrauen der Nutzenden in die Sicherheit einer Anwendung bedingt, ist Gegenstand der Promotion der jungen Forscherin. Mit ihren Publikationen vertrat Sandra das Fraunhofer AISEC 2022 auf renommierten Wissenschaftskonferenzen wie dem »Symposium on Usable Privacy and Security (SOUPS)« und vernetzt sich mit Privacy- und Usable Security-Expertinnen und -Experten weltweit. So bewahrt sie sich auch in der Rolle als Teamleitung die Nähe zur angewandten Forschung. Mit ihrem Team aus Fachleuten aus den Bereichen Usable Security sowie Machine Learning möchte sie die Themen Privacy und Trust stärker im Kosmos des Maschinellen Lernens und der Künstlichen Intelligenz verankern. Auch hier verfolgt sie pragmatische Ansätze, die Nutzenden unmittelbar helfen, um z. B. nachzuvollziehen, wie KI-Systeme ihre Daten verarbeiten.

Michael Heinl

Wissenschaftlicher Mitarbeiter in der Abteilung »Product Protection and Industrial Security«

Verschiedene Perspektiven einnehmen, ergebnisoffen an Probleme herangehen – das ist mein Ansatz, um langfristige Erfolge zu erzielen.«

Michael Heinl beginnt seine berufliche Laufbahn mit einer Ausbildung zum Informatikkaufmann und arbeitet danach im erlernten Beruf als Netzwerk- und Systemadministrator bei einem Automobilzulieferer. Regelmäßig kommen Studierende der Dualen Hochschule Baden-Württemberg für Praxisphasen in den Betrieb und erzählen von ihrem Studium. Durch den Austausch mit ihnen wird für Michael der Gedanke an ein Studium immer interessanter. Doch ohne Abitur bleibt ihm dieser Weg vorerst verschlossen. Er reduziert deshalb seine Vollzeitstelle und legt zielgerichtet das Abitur auf dem zweiten Bildungsweg ab.

Aufenthalte in den USA und Israel

Direkt im Anschluss beginnt er ein Bachelorstudium der Unternehmens- und IT-Sicherheit an der Hochschule Offenburg. Mit dem Ziel, sich fachlich breiter aufzustellen, folgt darauf ein Master in Informatik mit Nebenfach Philosophie an der Universität Ulm. Da sein Herz nach wie vor an der IT-Sicherheit hängt, studiert er im Rahmen eines Fulbright-Stipendiums ein Jahr im Master »Information Security and Assurance« an der George Mason University (Bundesstaat Virginia, USA).

Seine ersten Berührungspunkte mit Fraunhofer hat Michael 2017 durch das Programm »Hessian Israel Partnership Accelerator«, welches mit Aufenthalten am Fraunhofer SIT sowie an der Hebrew University of Jerusalem in Israel verknüpft ist. Das Thema seiner Masterarbeit bringt ihn schließlich ans Fraunhofer AISEC: Eine Metrik zur Bewertung der Vertrauenswürdigkeit von Zertifizierungsstellen im Rahmen von Public-Key-Infrastrukturen (PKIs).

Auf dem Weg zur Promotion

Besonders die Vielfalt der Anwendungen, ihre hohe Alltagsrelevanz sowie die Interdisziplinarität des Themengebiets machen Fragestellungen rund um die Vertrauenswürdigkeit und Sicherheit von PKIs für Michael so interessant. Auch als wissenschaftlicher Mitarbeiter der Abteilung »Product Protection and Industrial Security« sind PKIs ein Baustein, mit dem er sich in Projekten häufig auseinandersetzt. Um passgenaue Lösungen zu finden, geht er ergebnisoffen an Probleme heran und betrachtet sie aus unterschiedlichen Blickwinkeln. »Ich möchte Technologien und ihre Wirkung verstehen, bevor ich sie anwende«, sagt der Wissenschaftler. Herangehensweisen, die er als Doktorand an der Technischen Universität München (TUM) und als Lehrbeauftragter der Hochschule Heilbronn auch an Studierende weitergibt. Die hohe Dynamik und Komplexität im Bereich der IT-Sicherheit erfordert viel Flexibilität und Lernbereitschaft. Für Michael ist das ein besonderer Ansporn: In seinem Promotionsprojekt bearbeitet er Fragestellungen rund um die Themen Lieferkettensicherheit und kritische Informationsinfrastrukturen. Die gewonnenen wissenschaftlichen Erkenntnisse wendet er direkt in Kundenprojekten an und trägt so sein Wissen unmittelbar in die Praxis.

Vivija Čeprkalo-Simić

Projektleitung Lernlabor Cybersicherheit | Koordinatorin Duales Studium

Für Vivija Čeprkalo-Simić ist das eine der lebendigsten Erinnerungen der Studienzeit: In ihrem kleinen Studentenzimmer macht sie Freudensprünge. Sie hat eine anspruchsvolle mathematische Aufgabe gelöst und ihr hartnäckiges Dranbleiben hat sich gelohnt. Besonders das Regelhafte und Klare hat sie an der Mathematik immer fasziniert und führt sie zu ihrem Mathematikstudium an die Technische Universität München (TUM). Das Interesse für Kryptografie zeichnet sich gegen Ende des Studiums ab. So spezialisiert sie sich auf mathematische Aspekte in der Kryptografie an der Queensland University of Technology (Brisbane, Australien) und an der Université Toulouse III - Paul Sabatier (Toulouse, Frankreich), an der sie mit ihrer Diplomarbeit beginnt. Darin beschäftigt sie sich mit Edwards-Kurven, einer speziellen Form elliptischer Kurven, und deren Anwendung bei der kryptografischen Verschlüsselung in Smart Cards.

Mit einem Diplom der Mathematik und Informatik (als Nebenfach) bleibt sie in ihren ersten Berufsjahren an der Universität – zunächst an der Carl von Ossietzky Universität in Oldenburg. Kurz darauf ist sie an der TUM im Servicebüro Studium Informatik für den Masterstudiengang Informatik verantwortlich und später in der Studienfachberatung der ehemaligen Fakultät Informatik. In den ersten Berufsjahren kamen wichtige Softskills dazu, z. B. die Fähigkeit, priorisiert und strategisch zu arbeiten, sich in einer Männerdomäne zu behaupten, sowie faktenbasiert und selbstbewusst den eigenen Standpunkt zu vertreten. Die Notwendigkeit weiterzudenken und sich persönlich und beruflich zu entfalten ist für sie die wichtigste Maxime, die sie seit 2018 den Studierenden auch in ihrer Funktion als Leiterin der Studienfachberatung (TUM Informatik) mitgibt.

Menschen in ihren Fähigkeiten bestärken

»Ich möchte mich jederzeit weiterentwickeln und die Freiheit haben, mich selbst einzubringen«, sagt Vivija. Deshalb wurde sie auf das Fraunhofer AISEC aufmerksam. Durch ihre Tätigkeit an der TUM, auch als Dozentin für algebraische Methoden in der Kryptografie oder Post-Quanten-Algorithmen am Lehrstuhl für Sicherheit in der Informatik, war es nur ein kurzer Weg zum Büro der Inhaberin des Lehrstuhls und Leiterin des Fraunhofer AISEC, Prof. Dr. Claudia Eckert. Spontan entsteht ein unkompliziertes und offenes Gespräch zu den Entwicklungsmöglichkeiten am Fraunhofer AISEC, bei dem Vivija vor allem die Wertschätzung und Fürsorge der Institutsleiterin für ihre Mitarbeitende begeistert.

Seit 2019 ist Vivija Projektleiterin für das Lernlabor Cybersicherheit am Fraunhofer AISEC. Ihr Ziel ist es, Kunden aus der Industrie und dem öffentlichen Sektor durch individuelle, an ihren Bedarf angepasste Weiterbildungen im Bereich der IT-Sicherheit in ihrer Resilienz zu stärken. Mit Angeboten zu lebenslangem Lernen und zur beruflichen Weiterentwicklung unterstützt sie Unternehmen und Behörden dabei, den aktuellen wirtschaftlichen und sicherheitskritischen Herausforderungen zu begegnen. Dabei hilft ihr ihre Menschenkenntnis und ihr Anliegen, Menschen in ihren Fähigkeiten zu bestärken. Damit ist sie sehr erfolgreich. 2022 hat das Lernlabor Cybersecurity die erwarteten Erträge um 50 Prozent übertroffen.

»Zu lernen und mich auszuprobieren – das brauche ich. Denn nur durch Nachforschen und Verbessern ist es möglich, zu wachsen und Herausforderungen zu begegnen.«

Philip Sperl

Co-Leitung der Forschungsabteilung »Cognitive Security Technologies«

Philip Sperl leitet zusammen mit Dr. Konstantin Böttinger die auf Künstliche Intelligenz spezialisierte Forschungsabteilung »Cognitive Security Technologies« des Fraunhofer AISEC. Im Laufe seiner jungen Karriere hat der Elektrotechniker und Informatiker vielfältige Rollen am Institut innegehabt, z. B. Bachelor- und Master-Student und wissenschaftlicher Mitarbeiter.

Er kommt 2015 zunächst für seine Bachelorarbeit ans Fraunhofer AISEC. Darin widmet er sich der Untersuchung von Fehlerangriffen auf eingebettete Systeme. Einmal auf den Geschmack der angewandten Forschung gekommen, bleibt er dem Fachbereich »Hardware Security« des Fraunhofer AISEC während seines Masterstudiums an der TU München als wissenschaftliche Hilfskraft für Seitenkanalanalysen erhalten. Gut vernetzt und offen für die Forschung unterschiedlichster Themen der IT-Sicherheit entscheidet sich Philip für eine bereichsübergreifende Masterarbeit zu Hardware-Sicherheit gepaart mit Machine Learning am Fraunhofer AISEC. Die interdisziplinären Querschnittsthemen am jungen Institut bewegen Philip dazu, der angewandten IT-Sicherheitsforschung auch nach Abschluss des Studiums treu zu bleiben. Als wissenschaftlicher Mitarbeiter der Abteilung »Cognitive Security Technologies« geht er einen weiteren Schritt in Richtung Informatik und Maschinelles Lernen. Vier Jahre später steigt er in die Rolle des Co-Abteilungsleiters auf.

Offenes Mindset und viel Neugier

Es ist fast symbolisch, dass das Büro von Philip heute an die Abteilung Hardware Security angrenzt, denn seine Forschungsarbeit ist weiterhin interdisziplinär. Das schätzt er auch in seinem Team: Mitarbeitende mit Abschlüssen aus der Mathematik, Informatik, Elektrotechnik und Physik sind hier gleichermaßen vertreten. Gemeinsam entwickeln sie Lösungen, damit KI-Methoden zur IT-Sicherheit beitragen und die Verlässlichkeit von KI-Algorithmen gewährleistet bleibt. Philip ist überzeugt: Die Vielfalt im Team hilft, die Fragestellungen aus dem richtigen Blickwinkel zu betrachten und fortschrittliche Lösungen zu erarbeiten, die Partnern und Kunden in der Praxis helfen.

Dass seine Forschung Praxisrelevanz hat, zeigt sein Promotionsvorhaben im Studienfach Informatik. Unter dem Titel »Defending Neural Networks with Activation Analysis« entwickelt er Schutzmechanismen gegen Angriffe auf KI-Systeme, die z. B. zur verlässlichen Objekterkennung beim autonomen Fahren genutzt werden können. Obwohl er die Lötarbeiten zu seiner Studienzeit nicht vermisst, bewahrt Philip sich so auch in der Leitungsfunktion seine Hands-on-Mentalität, betreut weiterhin Abschlussarbeiten von Studierenden und publiziert zu KI-gestützter Anomalie-Erkennung und »Adversarial Attacks« (gezielte Versuche, ein KI-System mit manipuliertem Material zu Fehlern zu bringen).

Forschung ist für den Münchener die Grundvoraussetzung, um die Entwicklung der Branche mitzugestalten und besser auf den Bedarf der Kunden eingehen zu können. Das Ziel seines Teams ist eine anwendungsorientierte Forschung, die einen echten Mehrwert für Wirtschaft und Gesellschaft bietet.

»Das Thema KI wird in der IT-Sicherheit weiter an Bedeutung gewinnen. Wir werden diese Entwicklung mitgestalten und sind für die damit einhergehenden Herausforderungen bestens aufgestellt.«

Quantencomputing – Schon jetzt den Sprung wagen

Noch ist die Leistungskraft von Quantenrechnern gering. Aber Quantencomputing (QC) besitzt ein großes Potenzial zur Lösung spezieller Fragestellungen, wie Optimierungsprobleme, die aufgrund der erforderlichen Berechnungszeiten mit heutigen Computern nicht effektiv berechenbar sind. Das Fraunhofer AISEC leistet wichtige Vorarbeiten, um QC sicher in die Anwendung zu bringen.

433 Qubits groß war 2022 der leistungsstärkste Quantenprozessor der Welt. Im Gegensatz zum Bit kann ein Qubit nicht nur den Zustand 0 oder 1 annehmen, sondern beide Zustände zur gleichen Zeit. Superposition nennt sich das und ist Grund für den Hype um quantengestützte Rechner. Denn damit lässt sich rechnen: Superpositionen aus mehreren Qubits ergeben exponentiell viele Zustände. Quantencomputer sind deshalb in der Lage, spezielle mathematische Probleme so effizient und schnell zu lösen, wie es klassische Computer niemals tun könnten. »Es besteht die Hoffnung, dass QC das maschinelle Lernen, Herz jeder Künstlichen Intelligenz, erheblich verbessern kann«, sagt Pascal Debus, Leiter der »Gruppe Quantum Security Technologies« in der Abteilung »Cognitive Security Technologies« am Fraunhofer AISEC.

Bedrohung für klassische Verschlüsselungsverfahren

Der Blick der Cybersecurity auf das Quantenzeitalter ist weniger optimistisch: Quantencomputer bedrohen durch ihre Rechenkraft klassische Verschlüsselungsverfahren. Diese basieren häufig auf praktisch »unlösbaren« mathematischen Rechenproblemen, wie z. B. dem Faktorisierungsproblem [Glossar]. Quantencomputer können diese Aufgaben schneller lösen. Die Forschung zu Cybersicherheit beschäftigt sich daher bereits seit mehreren Jahren mit dem Thema Post-Quanten-Kryptografie. Am Fraunhofer AISEC ist dazu das Kompetenzzentrum Post-Quanten-Kryptografie entstanden (siehe S. 20). Auf den zweiten Blick ergeben sich durch Quantencomputer aber auch Chancen für die Cybersicherheit. Zwei Beispiele sind das Lösen des Verifikationsproblem in der Software-Entwicklung oder die Anomalie-Erkennung in IT-Systemen.

QC-Algorithmen für die Anwendung

Neben dem Kompetenzzentrum Post-Quanten-Kryptografie ist das Fraunhofer AISEC daher auch in die QC-Vorlaufforschung involviert: Im »Munich Quantum Valley (MQV)« setzen die Expertinnen und Experten QC-basiertes Maschinelles Lernen beispielsweise zur Betrugserkennung im Finanzumfeld ein, entwickeln sichere Software-Bibliotheken, um die Erstellung von QC-Programmen auch für Nicht-Spezialisten zu erleichtern, und erforschen, wie QC datenschutzkonform eingesetzt werden kann. Im »Bayerischen Kompetenzzentrum Quanten Security and Data Science (BayQS)« identifiziert das Fraunhofer AISEC Quantenvorteile bei Software-Fragestellungen und minimiert QC-Risiken, die in Hinblick auf das geistige Eigentum entstehen. Im Projekt »Quantum-enabling Services und Tools für industrielle Anwendungen (QuaST)« beschäftigen sich die Forschenden mit Quantencomputing-gestützten Lösungen und Werkzeugen für die klassische Software-Verifikation. »Denn bei 433 Qubits wird es mittelfristig nicht bleiben«, sagt Debus.

Glossar
*Das **Faktorisierungsproblem** besteht darin, eine vorgegebene Zahl in ein Produkt aus Primfaktoren zu zerlegen.*

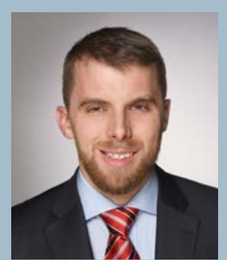
Projekte

Kompetenzzentrum Post-Quanten-Kryptografie
Im Kompetenzzentrum Post-Quanten-Kryptografie werden Quanten-resistente kryptografische Verfahren und Kryptoagilität erforscht.

MQV
Innerhalb des MQV (Munich Quantum Valley) werden QC-basiertes Maschinelles Lernen zur Betrugserkennung, Software-Bibliotheken für die QC Programmierung und datenschutzkonformes QC entwickelt.

BayQS
Bei BayQS (Bayerisches Kompetenzzentrum Quanten Security and Data Science) wollen Forschende Quantenvorteile für Software-Anwendungen identifizieren und QC-Risiken für das geistige Eigentum minimieren.

QuaST
Im Projekt QuaST (Quantum-enabling Services und Tools für industrielle Anwendungen) wird an QC-gestützten Lösungen und Werkzeugen für die klassische Software-Verifikation gearbeitet.



Kontakt

Pascal Debus
Gruppenleiter Quantum Security Technologies
Abteilung Cognitive Security Technologies
Tel. +49 89 3229986-180
pascal.debus@aisec.fraunhofer.de

Kompetenzzentrum PQC

MQV

BayQS

QuaST

Cybersicherheit für 6G

Während in Deutschland noch an einer flächendeckenden 5G-Verfügbarkeit gearbeitet wird, stellen Wirtschaft und Wissenschaft die Weichen für den nächsten Mobilfunkstandard 6G. Im BMBF-geförderten Projekt 6G-ANNA bringt das Fraunhofer AISEC seine Cybersicherheits-Expertise mit ein.

Die Markteinführung des neuen Mobilfunkstandards 6G wird für etwa 2030 prognostiziert. Er verspricht höhere Datenraten, schnellere Reaktionszeiten und verbesserte Ortungsgenauigkeit. Das macht 6G interessant für konkrete Anwendungen wie die ferngesteuerte Nutzung von Robotern oder das autonome Fahren. Um die dafür notwendigen Technologien zu entwickeln und eine 6G-Infrastruktur aufzubauen, setzen Technologiehubs und Universitäten bereits seit einigen Jahren Testfelder für 6G auf. Auch Wirtschaft und Wissenschaft arbeiten bei 6G eng zusammen. So beteiligen sich 29 Unternehmen und Forschungseinrichtungen im Forschungsprojekt »6G-Access, Network of Networks, Automation & Simplification (6G-ANNA)«. Das Fraunhofer AISEC bringt dabei seine Cybersicherheits-Expertise in den Feldern »Confidential Computing« und »Code-Analyse« ein. Ziel ist der Aufbau einer gemeinsamen 6G-Infrastruktur, die leistungsfähiger, nachhaltiger und vertrauenswürdiger als die 5G-Netze ist.

Ein Schwerpunkt der Forschungsarbeiten des Fraunhofer AISEC ist dabei das Thema Confidential Computing. Der Begriff steht für Technologien, die die Vertraulichkeit und Integrität von Daten bei deren Übertragung, Verarbeitung und Speicherung sicherstellen.

Confidential Computing mit GyroidOS

Kern ist dabei die sichere Container-Virtualisierung [Glossar] GyroidOS des Fraunhofer AISEC, die auf dem Open-Source-Betriebssystem Linux basiert. »GyroidOS schützt Integrität, Authentizität und Vertraulichkeit der Daten im virtualisierten Container. Damit bringen wir Confidential Computing in zukünftige 6G-Architekturen ein. Diese sind modularer aufgebaut und bieten dadurch mehr Angriffsfläche«, sagt Sascha Wessel, Leiter der Abteilung Secure Operating Systems am Fraunhofer AISEC.

Automatisierte Codeanalyse für Netz-Software

Eine weitere Technologie des Fraunhofer AISEC, die bei 6G-ANNA eingesetzt wird, ist das Codeanalyse-Werkzeug Codyze. Es prüft, ob die geltenden Regularien für die sichere Kommunikation, Verschlüsselung, Compliance und Zertifizierung von Software erfüllt werden. Automatisierte Security-Checks verkürzen dabei die Entwicklungszyklen der Software.

»Wir nutzen Codyze bei 6G-ANNA als statisches Codeanalyse-Werkzeug für die Einhaltung relevanter Standards und Richtlinien von Softwarekomponenten in 6G-Netzen«, sagt Christian Banse, Leiter der Abteilung Service and Application Security am Fraunhofer AISEC.

Glossar

*Unter dem Begriff **Virtualisierung** versteht man eine virtuelle Abstraktion physischer IT-Ressourcen, wie z. B. Hardware, Software, Speicher und Netzwerkkomponenten.*

Projekte

6G-ANNA
6G-ANNA ist 2022 gestartet und läuft bis Mitte 2025. Das Projekt hat ein Volumen von 38,4 Mio und wird vom Bundesministerium für Bildung und Forschung (BMBF) gefördert.

GyroidOS
Die sichere Container-Virtualisierung GyroidOS nutzt interne Funktionen des Open-Source-Betriebssystem Linux dazu, Anwendungen voneinander isoliert auf demselben Hostsystem zu betreiben.

Codyze
Das Codeanalyse-Werkzeug Codyze prüft Software automatisiert auf geltende Security-Regularien. Für 6G-ANNA wird es um die Analyse 6G-relevanter Programmiersprachen und für Anwendungsfelder jenseits von sicherer Verschlüsselung ausgebaut.

Kontakt

Sascha Wessel
Abteilungsleiter Secure Operating Systems
Tel. +49 89 3229986-155
sascha.wessel@aisec.fraunhofer.de

Christian Banse
Abteilungsleiter Service and Application Security
Tel. +49 89 3229986-119
christian.banse@aisec.fraunhofer.de

6G-ANNA

GyroidOS

Codyze

Publikationen

Antoine d'Aligny, Emmanuel Benoist, Florian Dold, Christian Grothoff, Özgür Kesim, Martin Schanzenbach: »Who comes after us? The correct mindset for designing a Central Bank Digital Currency«. In: SUERF Policy Note 279 (2022).

Daniel Angermeier, Hannah Wester, Kristian Beilke, Gerhard Hansch, Jörn Eichler: »Security Risk Assessments: Modeling and Risk Level Propagation«. In: ACM Transactions on Cyber-Physical Systems. 2022.

Ahmed Alqattaa, Daniel Loebenberger, Lukas Moeges: »Analyzing the Latency of QUIC over an IoT Gateway«. In: IEEE International Conference on Omnilayer Intelligent Systems, COINS 2022, Barcelona, Spain, August 13, 2022. IEEE, 2022, pp. 1–6. DOI: 10.1109/COINS54846.2022.9854951.

Oliver Braunsdorf, Stefan Sessinghaus, Julian Horsch: »Compiler-based Attack Origin Tracking with Dynamic Taint Analysis«. In: Information security and cryptology - ICISC 2021 (2022). DOI 10.1007/978-3-031-08896-4_9.

Manuel Brosch, Matthias Probst, Georg Sigl: »Counteract Side-Channel Analysis of Neural Networks by Shuffling«. In: Design, Automation & Test in Europe Conference & Exhibition, DATE 2022. Proceedings (2022). DOI 10.23919/DATE54114.2022.9774710.

Shanatip Choosaksakunwiboon, Karla Pizzi, Ching-Yu Kao: »Comparing Unsupervised Detection Algorithms for Audio Adversarial Examples«. In: International Conference on Speech and Computer (pp. 114-127). Springer, Cham. (2022).

Adam Dziedzic, Haonan Duan, Muhammad Ahmad Kaleem, Nikita Dhawan, Jonas Guan, Yannis Cattan, Franziska Boenisch, Nicolas Papernot: »Dataset inference for self-supervised models.« arXiv e-prints, pages arXiv–2209, NeurIPS'22. 2022.

Armando Miguel Garcia, Matthias Hiller: »Lightweight Authentication and Encryption for Online Monitoring in IIoT Environments«. In: International Symposium on Foundations and Practice of Security 2021 (2022). DOI 10.1007/978-3-031-08147-7_17.

Mathieu Gross, Nisha Jacob, Andreas Zankl, Georg Sigl: »Breaking TrustZone memory isolation and secure boot through malicious hardware on a modern FPGA-SoC«. In: Journal of cryptographic engineering (2022). DOI 10.1007/s13389-021-00273-8.

Jan Dennis Gumz, Simon Sebastian Hunt, Michael Stemmer, Sebastian Bock, Nikolay Vassiley Tcholtchev, Denny Mattern, Adrian Paschke, Marian Margraf: »Quanten-IKT. Quantencomputing und Quantenkommunikation.« (2022).

Michael P. Heinl, Simon Gölz, Christoph Bösch: »Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey«. In: ACM Comput. Surv. (2022). Just Accepted. ISSN: 03600300. DOI: 10.1145/3551386.

Alexander Hepp, Johanna Baehr, Georg Sigl: »Golden Model-Free Hardware Trojan Detection by Classification of Netlist Module Graphs«. In: Design, Automation & Test in Europe Conference & Exhibition, DATE 2022. Proceedings (2022). DOI 10.23919/DATE54114.2022.9774760.

Julius Hermelink, Silvan Streit, Emanuele Strieder, Katharina Thieme: »Adapting Belief Propagation to Counter Shuffling of NTTs«. In: IACR Transactions on Cryptographic Hardware and Embedded Systems 2023.1 (2022), 60–88. DOI: 10.46586/tches.v2023.i1.60-88.

Stefan Hristozov, Moritz Wettermann, Manuel Huber: »A TOCTOU Attack on DICE Attestation«. In: CODASPY 2022, Twelveth ACM Conference on Data and Application Security and Privacy. Proceedings (2022). DOI: 10.1145/3508398.3511507.

Monika Huber, Sascha Wessel, Gerd Brost, Nadja Menz: »Building Trust in Data Spaces«. In: Designing Data Spaces (2022). DOI: 10.1007/978-3-030-93975-5_9; DOI: 10.24406/publica-654

Ching-Yu Kao, Junhao Chen, Karla Pizzi, Konstantin Böttinger: »Rectifying adversarial inputs using XAI Techniques.« In: Proceedings of the European Association for Signal Processing 2022 (EURASIP 2022).

Ching-Yu Kao, Hongjia Wan, Karla Pizzi, Konstantin Böttinger: »Real or Fake? A Practical Method for Detecting Tempered Images«. In: Proceedings of the international image processing application and systems 2022 (IPAS 2022). (Best session paper award).

Patrick Karl, Tim Fritzmann, Georg Sigl: »Hardware Accelerated FrodoKEM on RISC-V«. In: 25th International Symposium on Design and Diagnostics of Electronic Circuits and Systems, DDECS 2022. Proceedings (2022). DOI 10.1109/DDECS54261.2022.9770148.

Özgür Kesim, Christian Grothoff, Florian Dold, Martin Schanzenbach: »Zero-Knowledge Age Restriction for GNU Taler«. In: Proceedings of 27rd European Symposium on Research in Computer Security (ESORICS). Lecture Notes in Computer Science. Springer, 2022.

Sandra Kostic, Maija Poikela: »Do Users Want To Use Digital Identities? A Study Of A Concept Of An Identity Wallet« In: SOUPS 22. 2022.

Alexander Küchler, Christian Banse: »Representing LLVM-IR in a Code Property Graph«. In: Information Security. Ed. by Willy Susilo, Xiaofeng Chen, Fuchun Guo, Yudi Zhang, and Rolly Intan. ISC '22. Springer, 2022, pp. 360–380.

Immanuel Kunz, Andreas Binder: »Application-Oriented Selection of Privacy Enhancing Technologies«. In: Annual Privacy Forum. Springer. 2022, pp. 75–87.

Immanuel Kunz, Angelika Schneider, Christian Banse, Konrad Weiss, Andreas Binder: »Poster: Patient Community – A Test Bed for Privacy Threat Analysis«. In: Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. CCS '22. 2022. DOI: 10.1145/ 3548606.3564253.

Immanuel Kunz, Angelika Schneider, Christian Banse: »A Continuous Risk Assessment Methodology for Cloud Infrastructures«. In: 2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid). IEEE. 2022, pp. 1042–1051.

Florian Lauf, Marcel Klöttgen, Hendrik Meyer zum Felde, Robin Brandstädter: »Donating Medical Data as a Patient Sovereignly: A Technical Approach«. In: 15th International Conference on Health Informatics (HEALTHINF 2022). 2022.

Christopher Mühl, Franziska Boenisch: »Personalized pate: Differential privacy for machine learning with individual privacy guarantees«. PoPETs'23. 2022.

Nicolas M. Müller, Pavel Czempin, Franziska Dieckmann, Froghyar Adam, Konstantin Böttinger »Does Audio Deepfake Detection Generalize?« In: Interspeech (2022).

Nicolas M. Müller, Franziska Dieckmann, Jennifer Williams: »Attacker Attribution of Audio Deepfakes«. In: Interspeech (2022).

Nicolas M. Müller, Karla Markert, Konstantin Böttinger: »Human Perception of Audio Deepfakes«. ACM Multimedia (2022).

Jannis Priesnitz, Rolf Huesmann, Christian Rathgeb, Nicolas Buchmann, Christoph Busch: »Mobile Contactless Fingerprint Recognition: Implementation, Performance and Usability Aspects«. In: Sensors. Online journal (2022). DOI 10.3390/s22030792.

Maximilian Richter, Magdalena Bertram, Jasper Seidensticker, Alexander Tschache: »A Mathematical Perspective on Post-Quantum Cryptography.« In: Mathematics 10, no. 15: 2579. 2022.

Paul Andrei Sava, Jan-Philipp Schulze, Philip Sperl, Konstantin Böttinger: »Assessing the Impact of Transformations on Physical Adversarial Attacks«. In: Proceedings of the 15th ACM Workshop on Artificial Intelligence and Security (AISec 2022).

Jan-Philipp Schulze, Philip Sperl, Konstantin Böttinger: »Double-Adversarial Activation Anomaly Detection: Adversarial Autoencoders are Anomaly Generators.« In: International Joint Conference on Neural Networks (IJCNN 2022).

Jan-Philipp Schulze, Philip Sperl, Konstantin Böttinger: »Anomaly Detection by Recombining Gated Unsupervised Experts.« In: International Joint Conference on Neural Networks (IJCNN 2022).

Jan-Philipp Schulze, Philip Sperl, Radutoiu, A., Sagebiel, C., Konstantin Böttinger: »R2-AD2: Detecting Anomalies by Analysing the Raw Gradient.« InEuropean Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML-PKDD 2022).

Bodo Selmke, Maximilian Pollanka, Andreas Duensing, Emanuele Strieder, Hayden Wen, Michael Mittermair, Reinhard Kienberger, Georg Sigl: »On the application of Two-Photon Absorption for Laser Fault Injection attacks Pushing the physical boundaries for Laserbased Fault Injection«. In: IACR Trans. Cryptogr. Hardw. Embed. Syst. 2022.4 (2022), pp. 862–885. DOI: 10.46586/tches.v2022.i4.862-885.

Bodo Selmke, Emanuele Strieder, Johann Heyszl, S. Freud., T. Damm: »Breaking Black Box Crypto-Devices Using Laser Fault Injection«. In: Foundations and practice of security. 14th International Symposium, FPS 2021 (2022). DOI 10.1007/978-3-031-08147-7_6.

Alexander Wagner, Felix Oberhansl, Marc Schink: »To Be, or Not to Be Stateful: Post-Quantum Secure Boot using Hash-Based Signatures«. In: Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security (2022), pp. 85-94.

Konrad Weiss, Christian Banse: »A Language Independent Analysis Platform for Source Code.« (2022). arXiv: 2203.08424 [cs.CR]. DOI 10.48550/arXiv.2203.08424.

Felix Wruck, Vasil Sarafov, Florian Ralph Jakobsmeier, Michael Weiß: »GyroidOS: Packaging Linux with a Minimal Surface«. In: SaT-CPS 2022, ACM Workshop on Secure andTrustworthyCyber-Physical Systems. Proceedings (2022). DOI 10.1145/3510547.3517917.

Impressum

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

Lichtenbergstr. 11
85748 Garching bei München
Telefon +49 89 3229986-0
www.aisec.fraunhofer.de

Redaktion
Maria Schwab-Kloe, Wiebke Ramm, Ramona Ursic, Tobias Steinhäußer (Leitung)

Redaktionelle Mitarbeit
Andreas Kunkel

Layout
Maria Schwab-Kloe

Grafiken
Daniela Miedaner

Druck
Flyeralarm GmbH

Kontakt
Fraunhofer-Institut für Angewandte und
Integrierte Sicherheit AISEC
Lichtenbergstr. 11
85748 Garching bei München
Telefon +49 89 3229986-170
marketing@aisec.fraunhofer.de

Bildquellen
Titelbild: HGEsch
Seite 4: Bernd Müller, Andreas Heddergott
Seite 8/9: Oliver Bodmer
Seite 11: Bernd Müller, Andreas Heddergott
Seite 12/13: Oliver Bodmer
Seite 14: Oliver Bodmer
Seite 15: Andreas Heddergott
Seite 16/17: Freepik/@kanawatTH
Seite 18/19: Andreas Heddergott
Seite 20/21: Adobe/agsandrew
Seite 22: Fraunhofer AISEC
Seite 23: AllEyesOnYou.de, Oliver Bodmer
Seite 24/25: Oliver Bodmer
Seite 26/27: Oliver Bodmer
Seite 28/29: Oliver Bodmer
Seite 30: Fraunhofer AISEC
Seite 31: Andreas Heddergott
Seite 32: Adobe Stock
Seite 33: Merck/Thomas Pirot für manager magazin
Seite 34: HGEsch
Seite 35: Daniela Miedaner (Grafik)
Seite 36/37: Daniela Miedaner (Grafik)
Seite 38/39: Daniela Miedaner (Grafik)
Seite 40: Andreas Heddergott/TUM, Oliver Rösler, Adam Bacher, Bundesdruckerei GmbH, Rene Bertrand, Bundesdruckerei GmbH
Seite 41: Werner Bartsch; Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie; Hessian.AI
Seite 42: Fraunhofer CCIT
Seite 43: Fraunhofer-Gesellschaft
Seite 44: Claudia Grosser
Seite 45: Udo Geisler Photographie
Seite 46: Fraunhofer-Verbund IUK-Technologie/Sasha Marie Runge
Seite 49: Oliver Bodmer
Seite 51: Oliver Bodmer
Seite 52: Oliver Bodmer
Seite 55: Freepik/@Serg Nivens
Seite 56: Freepik
Alle übrigen Abbildungen: © Fraunhofer AISEC

Folgen Sie uns!

Cybersecurity-Blog des Fraunhofer AISEC

LinkedIn

XING

Twitter