Fraunhofer
AISEC

Jahresbericht 2023

Mit Sicherheit innovativ

#mitsicherheitinnovativ

Jahresbericht 2023

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,

die Bedrohung im Cyberraum erreichte im Jahr 2023 einen neuen Höchststand: Noch mehr als bislang wurden Schwachstellen in Software- und Hardware-Produkten ausgenutzt, die Angriffsmethoden spezifizierten sich weiter und die Bedrohungslage durch Ransomware ist besorgniserregend geblieben. Doch auch auf der abwehrenden und schützenden Seite verzeichnen wir wichtige Fortschritte. Mission des Fraunhofer AISEC ist und bleibt, exzellente IT-Sicherheitsforschung in anwendungsorientierte Lösungen für mehr Verlässlichkeit, Vertrauenswürdigkeit und Manipulationssicherheit von IT-basierten Systemen und Produkten zu überführen. In diesem Sinne entwickelte das Fraunhofer AISEC 2023 neue Lösungen für eine sichere digitale Transformation: zur sicheren Nutzung von Schlüsseltechnologien wie Künstlicher Intelligenz, zum sicheren autonomen Fahren, zur Plattformsicherheit und vertrauenswürdigen Datenverarbeitung, zum Cloud-Monitoring bis hin zu sicheren, zukunftsfähigen Netzen und kryptografischen Protokollen für quantensichere digitale Identitätsnachweise.

Den inhaltlichen Schwerpunkt unserer Arbeit bildete Vorlaufforschung in den Bereichen Trusted Hardware, generative KI sowie Cloud, digitale Identität und Embedded Security. Gezielt ging es um den Ausbau etablierter Angebote und Kompetenzen wie der Erstellung von Sicherheitskonzepten, von Risikoanalysen und der Durchführung von offensiven Tests. In Forschungsprojekten mit Unternehmen, Behörden und Einrichtungen und über die Weiterbildungen des Lernlabors Cybersicherheit trugen wir unser aktuelles Forschungswissen in die Praxis und zahlreiche Berufsgruppen. Denn um den Herausforderungen in der Cybersicherheit zu begegnen, gilt es eine Vielzahl von Beteiligten zu den Möglichkeiten im Aufbau einer Sicherheitskultur abzuholen.

Mit diesem Jahresbericht geben wir Ihnen Einblicke in unser Tun 2023 und zeigen Ihnen auf, wie eine sichere Partizipation an zukunftsweisenden Technologien gelingen kann.

Wir wünschen Ihnen eine aufschlussreiche Lektüre!

Herzliche Grüße

Prof. Dr. Claudia Eckert

Prof. Dr. Georg Sigl

Inhalt

Autonomer Truck nimmt Kurs auf die Autobahn

Fahrerlose Lkw transportieren eigenständig Waren von einem Logistikhof zum nächsten. Ein solches Szenario besitzt großes Potenzial, birgt aber Cybersicherheitsrisiken: Unbefugte könnten die Kontrolle übernehmen und das autonome Fahrzeug zu lebensbedrohlichen Entscheidungen verleiten. Für sichere Automatisierungskonzepte in der Logistik bringt das Fraunhofer AISEC seine Cybersicherheitsexpertise und Testfähigkeiten in die Entwicklung der Mobilität der Zukunft ein.

Im Forschungs- und Entwicklungsprojekt »ATLAS-L4« (Automatisierter Transport zwischen Logistikzentren auf Schnellstraßen im Level 4) wird mit dem Know-how von Wissenschaft, Industrie und Infrastrukturbetreibern die Basis für innovative Transportkonzepte gelegt. Das Ziel ist, erstmals autonom fahrende Lkw auf die Autobahn zu bringen – und zwar bis Mitte dieses Jahrzehnts.

Das Fraunhofer AISEC entwickelt mit MAN Truck & Bus, Knorr-Bremse, Leoni, Bosch, Fernride, BTC Embedded Systems, den Technischen Universitäten München und Braunschweig sowie TÜV SÜD, Autobahn GmbH und WIVW GmbH im vom Bundesministerium für Wirtschaft und Klimaschutz geförderten Verbundprojekt ein industrietaugliches Konzept für den Betrieb Level-4-automatisierter Lkw auf der Autobahn. Level 4 bezeichnet die Vorstufe zum autonomen Fahren, bei dem das Fahrzeug in der Lage ist, einen Großteil der Steuerung durch das System selbst zu übernehmen. Seit Januar 2022 haben die Partner die Subsysteme, Sensorik, das Bordnetz, die Lenkung und das Bremssystem konzeptioniert und erprobt. Auch das Control Center für die technische Aufsicht wurde erfolgreich in Betrieb genommen. Das Prototypenfahrzeug legte 2023 erfolgreich die ersten Kilometer zunächst auf der Teststrecke und anschließend auf der Autobahn zurück.

Ganzheitlicher Schutz vor Cyberangriffen

Das Fraunhofer AISEC stellt bei »ATLAS-L4« sicher, dass vollumfängliche und nachvollziehbare Security-Anforderungen erfüllt werden. Gemeinsam mit MAN führten die Sicherheitsexperten der Abteilung »Product Protection and Industrial Security« die Risikoanalyse für das autonome Fahrsystem durch. Dafür erweiterten sie ihre Methoden für Security-Risikoanalysen auf den Kontext automatisierter Lkw. Aufbauend darauf wurden Security-Maßnahmen wie authentische und verschlüsselte Kommunikation sowie funktionale Sicherheitsmaßnahmen wie Redundanz und Degradationskonzepte für das autonome Fahrsystem definiert. Diese sind entscheidend, um auf Cyberangriffe resilient reagieren zu können, die Systemintegrität zu wahren und die Sicherheit im Straßenverkehr zu gewährleisten.

Sicherer Betrieb auf Autobahnen

Darüber hinaus entstehen Konzepte für ein ganzheitliches Security-Management, die neben der Entwicklung weitere Bereiche des Fahrzeuglebenszyklus wie Produktion und Betrieb berücksichtigen. Diese werden im weiteren Projektverlauf verfeinert und in einem Werkzeugkasten umgesetzt. Damit können die Forschenden Risiken und Anforderungen in Bezug auf Cybersicherheit für den gesamten Fahrzeuglebenszyklus identifizieren und adressieren. Zusätzlich erstellt das Fraunhofer AISEC in »ATLAS-L4« die Risikoanalyse und das Schutzkonzept zum Control Center. Somit werden sämtliche Aspekte der Cybersicherheit für Level-4-automatisierte Lkw abgedeckt und eine industrietaugliche Grundlage für ihren sicheren Betrieb auf Autobahnen geschaffen.

Automotive Security am Fraunhofer AISEC

Das Fraunhofer AISEC bietet umfangreiche Expertise und Analysemöglichkeiten, um die Sicherheit von Fahrzeugen und ihrer Kommunikationssysteme zu bewerten sowie zu bewahren. Von der Entwicklung von sicheren Steuergeräten, Bordnetzarchitekturen und Car-to-X-Systemen (C2X) über Security-Maßnahmen für Fahrzeugelektronik bis hin zu Verfahren für sichere Remote-Software-Updates: Mit seiner Forschung treibt die Abteilung »Product Protection and Industrial Security« den Stand der Technik im Bereich Automotive Security voran und unterstützt bei der Entwicklung, Umsetzung sowie Integration sicherer Fahrzeugfunktionen, Anwendungen und Mehrwertdienste.

Kontakt

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

Weiterführende Informationen

Projekt »ATLAS-L4«

Abteilung »Product Protection and Industrial Security«

Cloudsicherheit mit Gütesiegel von morgen

Clouds sind skalierbar, kosteneffizient und flexibel – aber auch sicher? Spätestens seit dem EU Cybersecurity Act steht Sicherheit bei Cloud-Anbietern im Fokus. Das Gesetz sieht das Zertifizierungsschema »EU Cybersecurity Certification Scheme for Cloud Services« (EUCS) in Form eines europäischen Sicherheitskriterienkatalogs vor.

Mit »MEDINA« zur Cloud-Zertifizierung

Um Cloud-Anbietern von Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) und Software-as-a-Service (SaaS) eine künftige EUCS-Zertifizierung zu erleichtern, hat das Fraunhofer AISEC seine Expertise in das von der EU geförderte Projekt »MEDINA« eingebracht. Das internationale Konsortium aus Wissenschaft und Wirtschaft entwickelte einen modularen Baukasten, um die Konformität mit künftigen EUCS-Anforderungen und somit die Sicherheit von Clouds kontinuierlich und automatisiert messbar zu machen. »Die Werkzeuge und Prozesse von MEDINA geben Cloud-Anbietern die Möglichkeit zu prüfen, ob sie alle Compliance-Vorgaben erfüllen, und wenn nötig nachzubessern – ohne langwierige und kostenintensive manuelle Nachweissuche«, erklärt Christian Banse, Abteilungsleiter »Service and Application Security« am Fraunhofer AISEC.

Erfassung und Bewertung von Evidenzen mit dem »Clouditor«

Mit dem Assurance-Werkzeug »Clouditor« brachte das Fraunhofer AISEC ein Open-Source-Tool ins Projekt ein, das automatisiert und kontinuierlich die sichere Konfiguration von Cloud-Diensten und -Anwendungen hinsichtlich Sicherheitsaspekten wie Verschlüsselung, Identitäts- und Zugriffsmanagement und Logging prüft. Um Nachweise für die Erfüllung der EUCS-Vorgaben automatisiert zu sammeln und auszuwerten, erweiterte das Forschungsteam am Fraunhofer AISEC die Evaluation um EUCS-relevante Datenquellen wie unternehmensinterne Compliance-Vorgaben, Policies und Software-Anwendungen.

Die Forschenden übersetzten die EUCS-Regularien in technische Regeln, anhand derer »Clouditor« die Evidenzen automatisiert auswertet und einem Zertifizierungsstatus zuweist. Dadurch können Cloud-Anbieter erkennen, ob sie alle Anforderungen erfüllen oder zusätzliche Maßnahmen für die EUCS-Zertifizierung ergreifen müssen.

EUCS-konforme Software mit »Codyze«

Das AISEC-Analysetool »Codyze« wird vom Fraunhofer AISEC in MEDINA zur Konformitätsbewertung von Software eingesetzt. Es identifiziert automatisiert Verstöße gegen EUCS-Vorgaben im Quellcode von Software. Durch statische Code-Analyse in C, C++ und Java stellt Codyze sicher, dass die Software im Cloud-System z. B. Krypto-Protokolle wie TLS und Datenverschlüsselung korrekt implementiert wird, APIs den definierten Standards entsprechen und nur vertrauenswürdiger Code verwendet wird. So werden Compliance-Verstöße und Schwachstellen frühzeitig erkannt und korrigiert. »Unser Ziel ist es, Unternehmen und Institutionen je nach Anwendungsfall passende Tools zu geben, um ihre Sicherheit effizient zu prüfen und zu stärken«, erklärt Angelika Schneider, wissenschaftliche Mitarbeiterin der »Abteilung Service and Application Security«. »Die Technologien aus MEDINA helfen Industrie und öffentlicher Hand, ihre Cloud-Dienste sicherer zu machen und sich für zukünftige Herausforderungen aufzustellen.«
Das Fraunhofer AISEC nutzt die Ergebnisse aus MEDINA in den EU-finanzierten Folgeprojekten »EMERALD« zu Certification-as-a-Service-Angeboten (CaaS) in Cloud-Umgebungen sowie »COBALT« zur Etablierung eines domänenübergreifenden Zertifizierungsmodells.

Automatisierte Bewertung der Sicherheit und Privacy

Datensouveränität ist ein essentielles Kennzeichen zukunftsorientierter Industrie. Mit den Open Source Tools des Fraunhofer AISEC können Unternehmen und öffentliche Einrichtungen auf Basis von automatisierten Sicherheitsanalysen und -bewertungen einen sicheren Datenaustausch und resiliente, verteilte Systeme aufbauen.

Projekt »MEDINA«

Webseite »Clouditor«

Webseite »Codyze«

Abteilung »Service and Application Security«

Kontakt

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

Audio-Deepfakes verlässlich entlarven

Die am Fraunhofer AISEC entwickelte Plattform »Deepfake Total« unterstützt mithilfe einer Künstlichen Intelligenz bei der Erkennung von Audio-Deepfakes. Die Plattform bietet zudem Informationen und Materialien für die Sensibilisierung hinsichtlich Deepfakes sowie Datensätze für das Training und die Evaluierung von KI-basierten Audio-Deepfake-Erkennungsmodellen.

Plattform »Deepfake Total«

Cybersicherheit in der Ära generativer KI

Führende Expertinnen und Experten aus Wissenschaft und Industrie erforschen im Projekt »AIgenCY« Implikationen generativer Künstlicher Intelligenz (KI) für die Cybersicherheit. Im Experimentierlabor des Fraunhofer AISEC wird die Anwendbarkeit generativer KI-Technologien in praxisnahen Szenarien geprüft.

Projekt »AIgenCY«

Abteilung »Cognitive Security Technologies«

Kontakt

Dr. Philip Sperl
Abteilungsleiter
Cognitive Security Technologies
Tel. +49 89 3229986-141
philip.sperl@aisec.fraunhofer.de

Dr. Konstantin Böttinger
Abteilungsleiter
Cognitive Security Technologies
Tel. +49 89 3229986-163
konstantin.boettinger@aisec.fraunhofer.de

Künstliche Intelligenz und IT-Sicherheit

Künstliche Intelligenz wird immer leistungsfähiger. Das bietet Chancen und Risken für die Cybersicherheit. Forschende des Fraunhofer AISEC nehmen die Technologien genau unter die Lupe. Sie forschen zum Einsatz von KI in der Cybersicherheit ebenso wie zum Schutz von KI-Systemen vor Angriffen. Einen besonderen Schwerpunkt stellen neue Entwicklungen im Feld der generativen KI dar.

Das verblüffende Leistungsvermögen der generativen KI war das vorherrschende Digitalthema 2023. Allen voran Large Language Models (LLM), wie z. B. Generative Pre-trained Transformer (GPT), standen im Fokus der Aufmerksamkeit. Dabei handelt es sich um Sprachmodelle, die in einem rechenintensiven Trainingsprozess statistische Zusammenhänge aus Textdokumenten erkennen und selbstständig neue Texte erzeugen. Welche Chancen und Risiken mit generativer KI für die Cybersicherheit einhergehen, erarbeitet das 2023 gestartete Projekt »AIgenCY«, indem es in den nächsten drei Jahren Prognosen zum Einsatz generativer KI entwickelt. Für dieses vom Bundesministeriums für Bildung und Forschung geförderte Vorhaben haben sich 2023 KI- und Cybersicherheitsexperten von Fraunhofer AISEC, CISPA, TU Berlin, FU Berlin und des Heidelberger KI-Start-ups Aleph Alpha zusammengefunden.

KI-Angriffe auf Fahrzeuge abwehren

KI steht aber nicht erst seit den Entwicklungssprüngen in der generativen KI bei Cybersicherheitsexpertinnen und -experten hoch im Kurs. Für die IT-Sicherheit bringt sie auf unterschiedliche Weise große Veränderungen mit sich. KI kann zum einen genutzt werden, um IT-Sicherheit besser zu machen. Ein Beispiel ist die Anomalie-Erkennung durch die automatisierte Analyse großer Datensätze. Zum anderen kann KI auch selbst angegriffen werden. Durch Eingabe fehlerhafter Daten, sogenannter »Adversarial Examples«, kann man Algorithmen austricksen. Ein wichtiger Praxisfall sind Fahrzeuge, in denen zunehmend KI verbaut wird. Angreifende versuchen bewusst, die Systeme hinters Licht zu führen und Kontrolle über die Fahrzeuge zu erlangen. Das kann zu Risiken mit sicherheitsrelevanten Folgen führen. Um einen raschen und zuverlässigen Überblick über neue Angriffsvektoren und Vorgehensweisen zu erlangen, hat die Abteilung »Cognitive Security Technologies« ein Tool entwickelt, mit welchem das Risiko neuer Angriffe bewertet und Verteidigungsstrategien priorisiert werden können.

Deepfakes mit KI erkennen

Auch beim Thema Deepfakes spiegelt sich die Ambivalenz des Themas KI für die Cybersicherheit wider. »Deepfakes« sind täuschend echt wirkende Video- und Audiomanipulationen, die mit tiefen neuronalen Netzen erzeugt werden. »Die Risiken und Herausforderungen, die Deepfakes mit sich bringen sind erheblich, nicht nur für die Medien, sondern auch für Unternehmen und Einzelpersonen«, sagt Konstantin Böttinger, Co-Leiter der Abteilung »Cognitive Security Technologies«. Zugleich bietet KI aber auch das Rüstzeug, um Deepfakes verlässlich zu entlarven: 2023 veröffentlichte das Fraunhofer AISEC die Plattform »Deepfake Total«, die KI-gesteuert Audio-Deepfakes erkennt.

Die Effizienz von KI ist dabei stets stark von der Qualität der Trainingsdaten abhängig. Um dieser Herausforderung zu begegnen, hat die Abteilung »Cognitive Security Technologies« für die Bundesdruckerei und Logsight 2023 im Projekt »Datenatlas« an der Integrität und Verlässlichkeit von KI-Datensätzen geforscht. Das Team entwickelte Konzepte zur Pflege, Analyse und Bereinigung von Daten, die sicherstellen, dass KI-Trainingsdaten von hoher Qualität sind und ethischen sowie sicherheitstechnischen Anforderungen genügen.

Verwundbare Hardware: Die Achilles-Ferse des Internet of Things

Mikroelektronik bildet das Herzstück smarter Geräte – von Industrie- und Consumer-Produkten bis hin zu kritischen Infrastrukturen. Aus Kostengründen und mangelndem Gefahrenbewusstsein greifen gerade Hersteller von IoT-Produkten häufig zu Standard-Hardware, deren Absicherung bei der Produktentwicklung kaum berücksichtigt wird. Das macht sie zu einem attraktiven Ziel für Angreifende.

Sicherheit von Mikrocontrollern unter der Lupe

In der Studie »Hardware Attacks against Microcontrollers« im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) haben Hardware-Sicherheitsforschende des Fraunhofer AISEC die Verwundbarkeit von IoT-Geräten belegt. Nahezu alle untersuchten Mikrocontroller waren anfällig für Hardware-basierte Angriffstechniken, wie:

- Fehlerangriffe auf interne Abläufe durch Spannungs- und Clock-Glitching (d.h. Unterbrechung der Ausführung von Maschinenbefehlen) oder elektromagnetische Fehlerinjektion
- Seitenkanalangriffe anhand von Energieverbrauch oder elektromagnetischer Abstrahlung
- Angriffe auf Ausleseschutztechniken über Schwachstellen in Kommunikationsschnittstellen

Doch die Forschenden des Fraunhofer AISEC haben nicht nur den Nachweis der Anfälligkeit der Chips für Angriffe geliefert. In der Studie werden auch gezielte Schutzmaßnahmen vorgeschlagen, die Angriffe verhindern. Ein möglicher Ansatz ist, die Anfälligkeit des Codes gegen Fehlerangriffe mithilfe von Simulationen zu erkennen und an den anfälligen Stellen automatisiert Gegenmaßnahmen einzufügen. Die Schutzmaßnahmen können Software-basiert implementiert werden, ohne dass dazu Änderungen an der Hardware nötig sind.

Von der Schwachstelle zur Sicherheitslösung

Die Forschungsergebnisse unterstreichen die Notwendigkeit, die Sicherheit von Hardware stärker in den Fokus zu rücken. Dr. Matthias Hiller, Leiter der Forschungsabteilung »Hardware Security«, setzt daher auf Sicherheitsanalysen im Labor, die Absicherung und Integration von Mikrocontrollern und Secure Elements sowie den sicheren Einsatz von System-on-Chips und Hardware-Schnittstellen wie Field-Programmable Gate Arrays (FPGAs). Gepaart mit der Expertise und Erfahrung seines Teams sowie eigens entwickeltem Analyse- und Test-Tooling bietet das nach Common Criteria EAL7 zertifizierte Hardware-Sicherheitslabor des Fraunhofer AISEC die nötigen Voraussetzungen für die Entwicklung vertrauenswürdiger Hardware. Hier untersuchen die Forschenden des Fraunhofer AISEC komplexe System-on-Chips-Systeme umfassend auf Schwachstellen, entwirft individuelle Sicherheitslösungen und prüft ihre Effektivität auf dem Chip. »Durch die enge Verzahnung von Forschung und Anwendung fließen unsere Erkenntnisse unmittelbar in die Praxis ein, um zusammen mit unseren Partnern die Sicherheit von Hardware systematisch über den gesamten Produktlebenszyklus zu bewerten, zu gestalten und zu bewahren, was nicht zuletzt im Rahmen des EU Cyber Resilience Act eine essenzielle Grundlage darstellt«, erklärt Hiller.

Flyer zum Hardware Security Lab

Zertifiziertes Hardware Security Lab

Im Hardware Security Lab decken Sicherheitsforschende des Fraunhofer AISEC Sicherheitsmängel in Hardware auf und entwickeln entsprechende Schutzmaßnahmen.

Das Hardware Security Lab hat die Common Criteria Standort-Zertifizierung der höchsten Sicherheitsstufe, der EAL-Stufe 7 (Evaluation Assurance Level), abgeschlossen. Die Zertifizierung bestätigt, dass das Prüflabor und die Infrastruktur alle Anforderungen der Normen ISO/IEC 15408-1 :2009, -2 :2008, -3 :2008 sowie Common Criteria for Information Technology Security Evaluation (CC) erfüllen.

Kontakt

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

Weiterführende Informationen

Studie »Hardware Attacks against Microcontrollers«

Abteilung »Hardware Security«

Krypto-Protokoll für quantensicheren Pass entwickelt

Der Sicherheitschip auf unseren Personalausweisen und Reisepässen ist durch Quantencomputer bedroht. Das Kompetenzzentrum Post-Quanten-Kryptografie des Fraunhofer AISEC hat 2023 im Forschungsprojekt »PoQuID« Krypto-Protokolle entwickelt, die auch Angriffen durch Quantencomputer standhalten. Partner waren dabei Infineon und die Bundesdruckerei.

Seit 2005 sichert ein elektronischer Chip die deutschen EU-Reisepässe und seit 2010 die deutschen Personalausweise, mit denen sich Bürgerinnen und Bürger auch online authentisieren können (die Online-Ausweisfunktion). Im Chip sind die personenbezogenen Daten und biometrischen Merkmale wie das Passbild und zwei Fingerabdrücke gespeichert. Der Chip ist zudem mit einem Echtheitsnachweis versehen. Angriffen durch ausreichend leistungsstarke Quantencomputer, die in den kommenden zehn bis 15 Jahren erwartet werden, hält die dort eingesetzte Kryptografie jedoch nicht stand: Es wird davon ausgegangen, dass diese die dahinterliegenden mathematischen Problemstellungen in viel kürzerer Zeit lösen können als heutige Computer. Der Chip könnte dann als Sicherheitsmerkmal nicht weiter genutzt werden.

Zwei Sekunden für den Sicherheitscheck

Das Kompetenzzentrum Post-Quanten-Kryptografie des Fraunhofer AISEC hat den Chip im Forschungsprojekt »PoQuID« deshalb quantensicher gemacht. Partner des vom Bundesministerium für Wirtschaft und Klimaschutz geförderten Projekts waren Infineon und die Bundesdruckerei. »Wir haben das für Reisepässe geltende kryptografische Standard-Protokoll ›Extended Access Control (EAC)‹ so angepasst und weiterentwickelt, dass es quantenresistent ist und auch mit den beschränkten Ressourcen des Sicherheitschips performant läuft«, erläutert Prof. Dr. Marian Margraf, Co-Leiter des Kompetenzzentrums Post-Quanten-Kryptografie. »Wir haben in unseren Forschungsarbeiten nachgewiesen, dass das neue Protokoll dieselben Sicherheitsfunktionen umsetzt wie das bisherige. Es benötigt für die Berechnung lediglich zwei Sekunden, um das Sicherheitsmerkmal zu überprüfen und ist damit sowohl für die Grenzkontrolle von elektronischen Pässen als auch als Online-Ausweisfunktion geeignet.«

»Das Forschungsprojekt hat die Grundlagen geschaffen, die Sicherheit elektronischer Ausweisdokumente fit fürs Quantencomputer-Zeitalter zu machen. Bei der Markteinführung muss es jetzt schnell gehen«, so Margraf. Der Forscher rechnet mit einem internationalen Standardisierungsprozess von mindestens fünf Jahren. »Für Ausweisdokumente zuständige Behörden bzw. die Hersteller der Sicherheitschips müssen außerdem berücksichtigen, dass Ausweisdokumente bis zu zehn Jahre gültig sein können und erste, leistungsfähige Quantencomputer bereits für Mitte der 2030er Jahre prognostiziert sind.«

Kontakt

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

Kompetenzzentrum Post-Quanten-Kryptografie

Das Kompetenzzentrum Post-Quanten-Kryptografie bietet individuelle Beratung und Unterstützung bei der Umsetzung der Migration auf quantenresistente Architektur-Designs, Sicherheitsanalysen von PQC-Implementierungen und ein Informationsportal zur Post-Quanten-Kryptografie an.

Kompetenzzentrum Post-Quanten-Kryptografie

Seminar »Post-Quanten-Sicherheit«

Im Präsenz-Seminar »Post-Quanten-Sicherheit« des Lernlabors Cybersicherheit erlangen Teilnehmende umfassende Kenntnisse zur Funktionsweise eines Quantencomputers sowie einen Überblick über die Herausforderungen für die IT-Sicherheit.

Seminar »Post-Quanten-Sicherheit«

Kontakt

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

Weiterführende Informationen

Projekt »PoQuID«

Sicherheit für Betriebssysteme und Hardware-nahe Software

Die Abteilung »Secure Operating Systems« analysiert und entwickelt sichere Softwarearchitekturen und Techniken zum Schutz der Systemintegrität, Resilienz und zur Isolation von kritischen Komponenten und Daten.

Forschungsschwerpunkte liegen auf der Bewertung und Entwicklung von sicheren eigebetteten Systemen. Darunter fallen Confidential Computing, Software Security und Hardening, Fuzz-Testing, Code-Analysen, Entwicklung von Sicherheitsmaßnahmen und Kerntechnologien als Open-Source-Software für die Domänen Mobile, Embedded Systems, Edge Computing, Server und Cloud.

Kontakt

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

Weiterführende Informationen

Webseite zu »GyroidOS«

Abteilung »Secure Operating Systems«

GyroidOS: Sichere Virtualisierungslösung für die Speicherung, Verarbeitung und Kommunikation von Daten

Edge Computing, Künstliche Intelligenz oder IoT – das Speichern, Teilen und Bearbeiten von Daten ist wesentlicher Bestandteil der digitalen Wertschöpfungskette. Unternehmen stehen vor der Herausforderung, die Integrität, Vertraulichkeit und Verfügbarkeit von Daten zu schützen. Hier setzt »GyroidOS« an.

»GyroidOS« ist eine am Fraunhofer AISEC entwickelte Virtualisierungslösung auf Betriebssystemebene, die sich durch einen besonderen Fokus auf die IT-Sicherheit auszeichnet. Der zu Grunde liegende Linux-Betriebssystemkern verschafft GyroidOS eine Unabhängigkeit in Bezug auf Prozessorarchitekturen. Basierend auf Hardware-Funktionen ermöglicht die Lösung eine sichere Container-Isolierung und die Erstellung leichtgewichtiger sowie flexibler Ausführungsumgebungen, die auch für die Verarbeitung von Daten mit Geheimhaltungsstufe geeignet ist.

Schutz von Daten durch Isolierung von Anwenderkontexten

Durch die besondere Systemarchitektur von GyroidOS können Daten zusätzlich abgesichert werden. Besonders schützenswerte Anwendungen und Daten kommen in Ausführungsumgebungen zum Einsatz, die vom Core-Container isoliert und somit privilegiert sind. Im Core-Container befinden sich neben den kritischen Komponenten wie der Fernwartung und Update-Funktionalitäten das Administratorsystem, das gegenüber (Hacker-)Angriffen exponiert ist. Durch die Trennung von unprivilegierten Anwendungs-Containern vom Core-Container wird ein besonders hohes Sicherheitsniveau erreicht. Der Core-Container ist an dieser Stelle auch unprivilegiert, besitzt aber eine definierte Schnittstelle zur Steuerung der privilegierten Virtualisierungsschicht.

Sichere und vertrauliche Datenerfassung, -verarbeitung und -kommunikation

Vollständige Festplattenverschlüsselung, sicheres Booten mit Remote-Attestierung, Signierung von Komponenten wie Gast-Betriebssystemen, Kernel und Modulen, eine Secure-Element-Unterstützung für die Zwei-Faktor-Authentifizierung sowie weitere Security-Funktionen schützen die Speicherung, Verarbeitung und Kommunikation von Daten.

Die Open-Source-Software ist auf zahlreichen x86- und ARM-Plattformen einsetzbar. Zudem unterstützt GyroidOS Zertifizierungsprozesse nach den Industriestandards DIN SPEC 27070 und IEC 62443-4-2. Im Kontext der International Data Spaces verfügt GyroidOS als Teil des Trusted Connectors über das IDS-ready Label. Für eine Common Criteria Zertifizierung kann GyroidOS als Teil des zu zertifizierenden Produkts bzw. als Target of Evaluation (TOE) genutzt werden. Die Sicherheits-Features der Software eignen sich für die Umsetzung von TOE Security Functions.

Mit GyroidOS steht eine sichere, individuell konfigurierbare und flexible Lösung für die Ausführung von isolierten Anwendungen und Services zur Verfügung. Das Fraunhofer AISEC unterstützt bei der Implementierung der Open-Source-Software sowie mit kundenspezifischen Erweiterungen von GyroidOS.

Sicherheit für zukunftsfeste Infrastrukturen

Die Abteilung »Secure Infrastructure« des Fraunhofer AISEC am Standort Weiden unterstützt Kunden im Bereich der angewandten Kryptografie, bei der Migration auf quantensichere Architektur-Designs sowie der Untersuchung und Gestaltung von sicheren Netzprotokollen.

Abteilung »Secure Infrastructure«

Sichere und nutzerfreundliche digitale Systeme

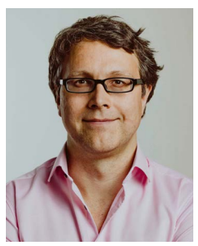
Ein Forschungsschwerpunkt der Abteilung »Secure Systems Engineering« am Standort des Fraunhofer AISEC in Berlin ist die Entwicklung von digitalen Systemen unter Berücksichtigung von Sicherheit, Datenschutz und Nutzerfreundlichkeit. Die entwickelten Sicherheitsarchitekturen unterstützen Unternehmen bei der Zertifizierung gemäß eIDAS, BSI-TR, ISO27000 oder Common Criteria.

Abteilung »Secure Systems Engineering«

Pressemitteilung zur Telematikinfrastruktur

Kontakt

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



Martin Seiffert
Senior Scientist
Secure Systems Engineering
Tel. +49 89 3229986-231
martin.seiffert@aisec.fraunhofer.de

Mehr Datensicherheit durch Zugriffskontrolle mit dem Zero-Trust-Konzept

Erfolgreich durchgeführte Cyberattacken oder eine versehentliche Offenlegung vertraulicher Daten durch interne Benutzende können für Unternehmen schwerwiegende Folgen haben. Mit dem Zero-Trust-Konzept liegt ein datenzentrierter Ansatz vor, der jeden Datenzugriff einer Prüfung unterzieht.

»Zero Trust« beschreibt ein Sicherheitskonzept, das weder einen vertrauenswürdigen internen Bereich noch a priori Vertrauensannahmen gegenüber Benutzenden, Geräten und Netzwerken vorsieht. Jeder Zugriff auf Ressourcen wird überprüft. Dabei beruhen Ressourcenauthentifizierungen und -autorisierungen auf einem dynamischen Regelwerk und werden vor dem Datenzugriff durchgesetzt. Dies ermöglicht eine vom Standort des Nutzenden oder vom Unternehmensnetzwerk unabhängige Kommunikation. Durch die genaue Überprüfung und Kontrolle aller Datenzugriffe können Unternehmen leichter Compliance-Vorgaben einhalten und die eigene Sicherheitslage verbessern.

Die Implementierung von »Zero Trust« bedarf der Berücksichtigung der bestehenden IT-Infrastruktur des Unternehmens sowie einer sorgfältigen Planung und Umsetzung. Durch die Entwicklung von anwendungsorientierten Sicherheitslösungen mittels des Zero-Trust-Konzepts trägt das Fraunhofer AISEC zu seiner Verbreitung in der Praxis bei. Die Gestaltung sicherer, auf »Zero Trust« basierender Kommunikation im Gesundheitswesen oder die Evaluation von Zero-Trust-Strategien im bayerischen Behördennetz sind Anwendungsbeispiele dieser Forschungsarbeit.

Telematikinfrastruktur 2.0: Sichere Kommunikation im Gesundheitswesen

Die Telematikinfrastruktur (TI) ist das zentrale Kommunikationsmittel im Gesundheitswesen. Um die TI sicher und zukunftsfähig zu machen, hat das Fraunhofer AISEC gemeinsam mit der Bundesdruckerei, CompuGroup Medical, genua GmbH und D-Trust GmbH im Auftrag der gematik die konzeptionellen Grundlagen für eine TI 2.0 gelegt. Neben einem auf Zero-Trust-Prinzipien basierenden Architekturkonzept und einem Migrationsplan wurde ein Demonstrator für die neue Sicherheitsarchitektur entwickelt. Die Machbarkeit der Architektur wurde mithilfe eines Proof of Concepts nachgewiesen. Durch einheitliche Zugriffsmechanismen für sämtliche Nutzergruppen wird eine gleichberechtigte Integration aller Akteure ermöglicht und der Benutzerkreis auf Versicherte sowie Leistungserbringer ohne festen Standort erweitert. Ausschlaggebend bei der Autorisierung einzelner Datenzugriffe ist, dass eingesetzte Endgeräte die an sie gestellten Sicherheitsanforderungen erfüllen.

Evaluation von Zero Trust im Behördennetz

Im Auftrag des Landesamts für Sicherheit in der Informationstechnik (LSI) hat das Fraunhofer AISEC untersucht, inwieweit »Zero Trust« im bayerischen Behördennetz umgesetzt ist und wie es zur Verbesserung der Sicherheitsinfrastruktur beitragen kann. Dabei wurden Werkzeuge entwickelt, um Anforderungen und Empfehlungen für Zero-Trust-Security abzuleiten. Anhand von drei Use Cases wurde ein Zero-Trust-Sicherheitskonzept evaluiert: »Zero Trust« bietet robuste Lösungen für die Verbesserung der Netzwerksicherheit im Behördennetz. Die Herausforderung besteht darin, die stark segmentierten Netze durch den neuen Zero-Trust-Ansatz nicht zu schwächen. Daher wurden in dem Projekt Herausforderungen für die Migration und Integration ins bestehende Netzwerk identifiziert. Empfehlungen zeigen auf, wie das Zero-Trust-Konzept in die Netzinfrastruktur sukzessiv implementiert werden kann, damit künftig die Vorteile von »Zero Trust« optimal genutzt werden können.

Wissenstransfer aus der Forschung in die Praxis

Mit zunehmender Digitalisierung wächst das Bedrohungspotenzial von Cyberattacken kontinuierlich. Das Lernlabor Cybersicherheit ist Teil der Weiterbildungseinrichtung Fraunhofer Academy und unterstützt Unternehmen sowie Behörden beim gezielten Aufbau von Kompetenzen in der IT-Sicherheit.

Das Lernlabor Cybersicherheit des Fraunhofer AISEC ist spezialisiert auf die Themen Embedded Systems, Internet of Things und Mobile Security. Die Schulungen vermitteln kompakt und praxisnah aktuelle Forschungsergebnisse sowie Methoden der IT-Sicherheit und können auf individuelle Interessen sowie Bedürfnisse angepasst werden.

Kontakt

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

Weiterführende Informationen

Lernlabor Cybersicherheit des Fraunhofer AISEC

Fraunhofer ACADEMY

Know-how bringt Sicherheit

Ist eine Sicherheitslücke geschlossen, wartet schon die nächste. So vielseitig sich der Schutz von IT-Systemen und somit Daten, Know-how und Produkten auch entwickelt – Unternehmen und Behörden kommen nicht umhin, sich fortlaufend mit Cybersicherheit zu befassen. Doch wie bleibt man einen Schritt voraus, wenn Fachkräfte rar sind?

Direkter Zugang zu anwendungsorientiertem Forschungswissen

Forschende des Fraunhofer AISEC teilen aktuelle wissenschaftliche Erkenntnisse und praktische Erfahrungen im Lernlabor Cybersicherheit, das Teil der Fraunhofer Academy ist. »Der erste Kontakt zur Weiterbildungseinrichtung entsteht oft über Forschungs- und Entwicklungsprojekte zwischen dem Fraunhofer AISEC und Partnern aus Industrie und öffentlicher Hand«, berichtet Vivija Čeprkalo-Simić, Projektleiterin des Lernlabor Cybersicherheit am Fraunhofer AISEC. Genauso erreichen sie Anfragen neuer Interessenten zu Risikoanalysen, Post-Quanten-Kryptografie (PQC), Blockchain-Technologien, Hardware-Sicherheit und Maschinellem Lernen (ML). »Bei Themen wie Advanced ML oder PQC werden wir für Trainings gebucht, die schlicht niemand sonst in dieser Fachtiefe anbietet«, erklärt Čeprkalo-Simić.

Im Beratungsgespräch stimmt sie das Lernziel ab: Wer braucht welches Wissen? Bedarf es einer Sensibilisierung für bestimmte Themen? Soll praktisches Security-Know-how oder ein strategisches Verständnis für eine Technologie vermittelt werden? Ist ein individuelles Schulungskonzept notwendig? Bei der Entwicklung der Lerninhalte stimmen sich Forschende und Trainer eng mit Lehrenden und Fachleuten für digitale Lerninhalte ab. Das anwendungsorientierte Forschungswissen wird dadurch verständlich und nachhaltig erlebbar aufbereitet.

IT-Sicherheit für konkrete Herausforderungen

Die Trainerinnen und Trainer vermitteln im Lernlabor Cybersicherheit das, woran sie forschen: z. B. Risikoanalysen für Automobilhersteller und Maschinenbauer, quantensichere Kryptografie für Finanzdienstleister, sichere FPGA-basierte Systeme für das Transportwesen und Machine Learning für die Telekommunikation. Aktuelle Forschungserkenntnisse werden in virtuellen Seminaren, webbasierten Trainings, In-House-Schulungen oder in den Security Labs am Fraunhofer AISEC vermittelt und direkt angewendet – in praxisnahen Simulationen, anhand von Trainings-Hardware oder in Hacking-Sessions, bei denen Teilnehmende selbst einmal in die Rolle des Angreifenden schlüpfen.

Das Konzept überzeugt. Viele Kunden streben langfristige Kooperationen an – nach dem Motto »Man lernt nie aus«. Das gilt auch für das Lernlabor selbst.

Cyberresilient in die Zukunft

Angesichts von Technologiesprüngen wie KI oder Quantencomputing müssen Fachleute auch darin geschult werden, IT-Systeme nicht nur widerstandsfähiger gegenüber Angriffen, sondern auch resilient im Fall erfolgreicher Angriffe zu machen. Im Fraunhofer-übergreifenden Projekt »CyRille« ist das Fraunhofer AISEC an der Entwicklung von Assessments und Weiterbildungen zum Thema Cyberresilienz beteiligt. Forschende unterstützen Unternehmen darin, ihre Produkte dahingehend weiterzuentwickeln, Angriffe zu erkennen und zu bewältigen. ». Unternehmen müssen wissen, wie sie selbst während eines Angriffs operativ bleiben, die Kontrolle über Prozesse und Produkte behalten und sich schnell von einem Angriff erholen. Über das Lernlabor Cybersicherheit, so Čeprkalo-Simić , können wir Erkenntnisse, Tools und Praktiken der Cyberresilienz in Unternehmen und die öffentliche Verwaltung bringen.«

1. Cybersicherheitstag – Forschung trifft Industrie

Im November fand erstmals ein Cybersicherheitstag am Fraunhofer AISEC statt. Unsere Expertinnen und Experten für Cybersicherheit präsentierten anhand von Demonstratoren Ergebnisse und Lösungen aus Forschungs- und Industrieprojekten. Kunden erhielten Einblicke in unsere Cybersecurity Labs und konnten sich in kompakten Expert Sessions über zentrale Themen der IT-Sicherheit informieren.

Zur Event-Webseite

TU München ehrt Prof. Dr. Eckert mit Heinz Maier-Leibnitz-Medaille

Die Leiterin des Fraunhofer AISEC, Prof. Dr. Claudia Eckert, erhielt am Dies Academicus der TUM für ihre herausragenden Arbeiten zu System- und Anwendungssicherheit sowie zu eingebetteten Systemen die höchste Auszeichnung der TUM, die Heinz-Maier-Leibnitz-Medaille. An ihrem Lehrstuhl Sicherheit in der Informatik an der TUM befasst sie sich mit dem Schutz von IT-Systemen. Als Mitglied verschiedener nationaler und internationaler industrieller Beiräte und wissenschaftlicher Gremien berät sie Unternehmen, Wirtschaftsverbände sowie die öffentliche Verwaltung in Fragen der IT-Sicherheit.

Zur Pressemitteilung

Türen auf mit der Maus 2023

Am »Türen auf mit der Maus«-Tag am Fraunhofer AISEC erlangten Kinder zwischen acht und 14 Jahren erste Einblicke in die Cybersecurity. Etwa 100 Gäste hatten an drei Stationen Gelegenheit, von einer Künstlichen Intelligenz erstellte Bilder und Töne zu erkennen, einen Safe zu knacken und beim Computerspiel »Charlie und die Quantenfabrik« Grundbegriffe zu Quantencomputern kennenzulernen.

Zur Event-Webseite

COSADE 2023 am Fraunhofer AISEC

Seit 2010 bietet der »International Workshop on Constructive Side-Channel Analysis and Secure Design COSADE« Wissenschaft und Industrie eine Plattform zur Präsentation aktueller Forschungsarbeit. 2023 organisierten die TUM und das Fraunhofer AISEC die 14. Edition der Workshop-Reihe. Die Themen reichten von Implementierungsangriffen über effiziente und sichere HW/SW-Implementierungen bis zu Hardware-intrinsischer Sicherheit und automatisierten Werkzeugen.

Zur Event-Webseite

Fraunhofer AISEC empfängt Vize-Premierminister Singapurs

Das Thema Cybersicherheit erstreckt sich über nationale Grenzen hinaus. Zur Förderung des Wissensaustauschs und zur Erschließung neuer Märkte in Asien arbeitet das Fraunhofer AISEC eng mit Forschungseinrichtungen in Singapur zusammen. Der Besuch hochrangiger Vertreterinnen und Vertreter der Regierung sowie der Forschungslandschaft Singapurs am Standort in Garching im Juni unterstrich die Bedeutung der internationalen Kooperation und setzte neue Impulse für die gemeinsame Forschung. Zu den Ehrengästen aus Regierung und Forschung zählten der singapurische Vize-Premierminister und Minister für Wirtschaftspolitik, Heng Swee Keat, sowie der Geschäftsführer der National Research Foundation Singapore, Beh Kian Teik.

Zur Pressemitteilung

Awareness für IT-Sicherheit

Der Faktor Mensch spielt in der IT-Sicherheit eine entscheidende Rolle. Um das Bewusstsein für den verantwortungsvollen Umgang mit IT-Systemen zu stärken, hat das Fraunhofer AISEC eine Poster-Kampagne zu Grundregeln der IT-Sicherheit entworfen. Die informativen Poster helfen, eine Sensibilisierung für das Thema Cybersicherheit zu entwickeln und stehen kostenlos zum Download zur Verfügung.

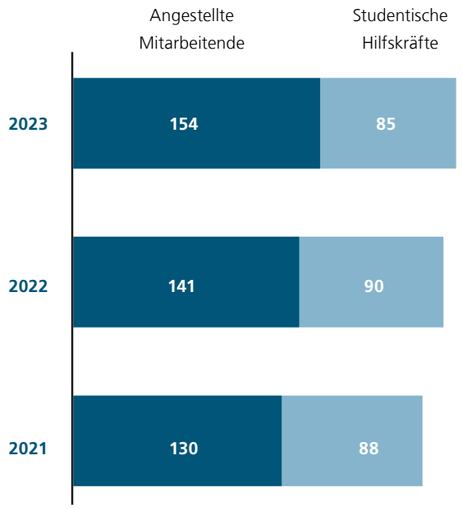
Zum Download

Unsere Mission:
Cybersicherheit bewerten, gestalten und bewahren

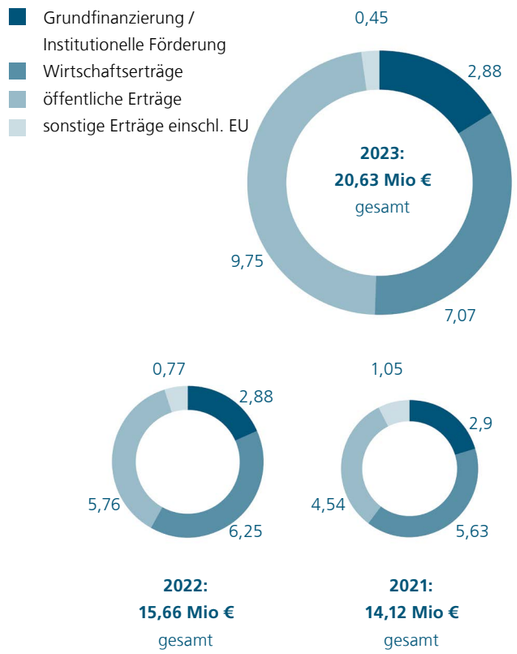
Das Fraunhofer AISEC überführt exzellente IT-Sicherheitsforschung in anwendungsorientierte Lösungen für mehr Verlässlichkeit, Vertrauenswürdigkeit und Manipulationssicherheit von IT-basierten Systemen und Produkten.

Zahlen und Daten

Zahl der Mitarbeitenden



Forschungsvolumen (in Mio €)



Unsere Forschungsabteilungen

Security von der Hardware bis in die Cloud

COGNITIVE SECURITY TECHNOLOGIES

Sicherheit für, mit und durch KI

SECURE SYSTEMS ENGINEERING

Sichere und nutzerfreundliche digitale Systeme

SECURE OPERATING SYSTEMS

Sicherheit von Hardwarenaher Software und Betriebssystemen

SERVICE AND APPLICATION SECURITY

Cloud-Sicherheit von Infrastrukturen, sichere verteilte Anwendungen

SECURE INFRASTRUCTURE

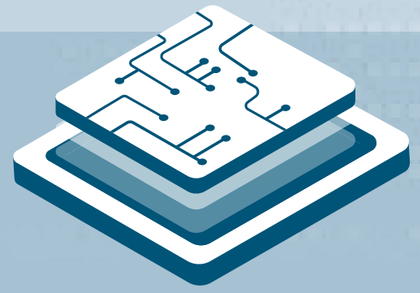
Anwendung kryptografischer Verfahren, sichere Netzprotokolle

PRODUCT PROTECTION AND INDUSTRIAL SECURITY

Produktschutz, Automotive Security, IoT, Industrial Security, Smart Building

HARDWARE SECURITY

Vertrauenswürdige Elektronik und sichere eingebettete Systeme



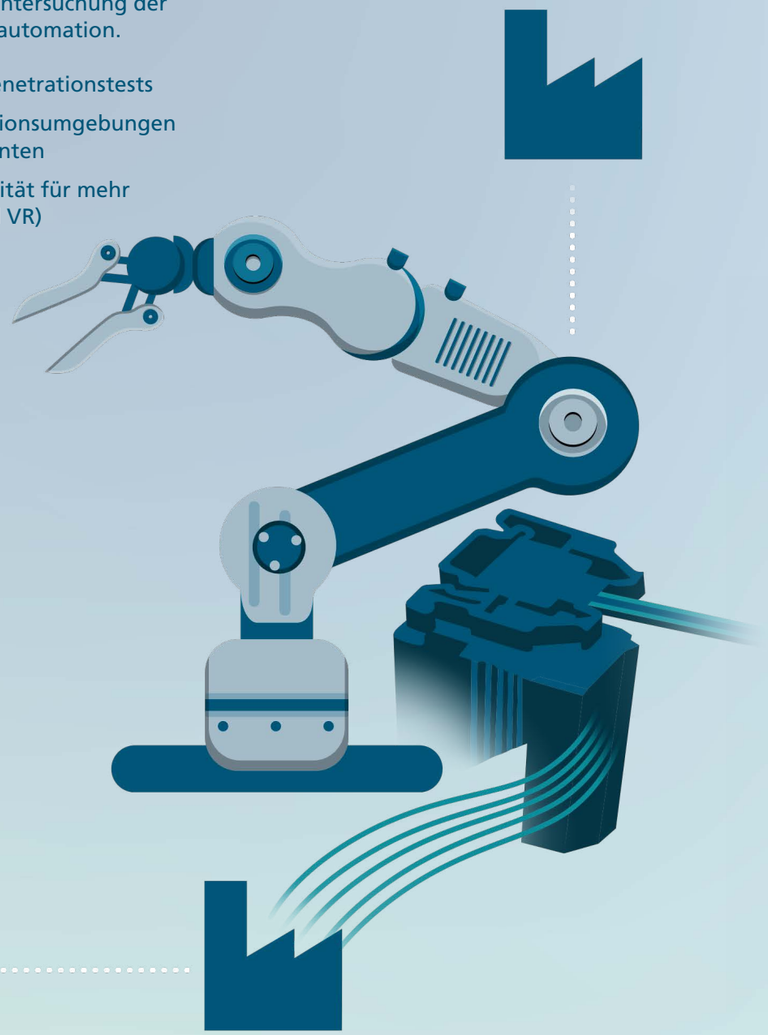
Laborlandschaft am Fraunhofer AISEC

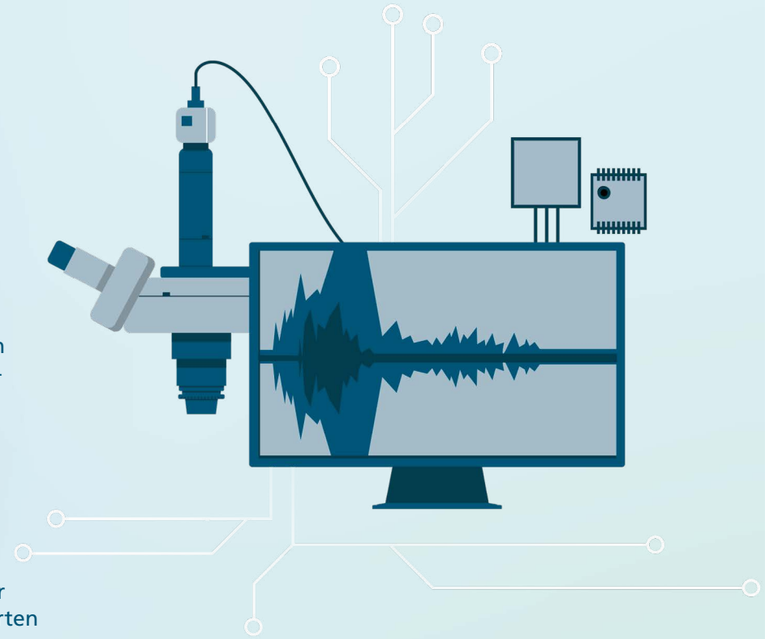
Maßgeschneiderte Lösungen, beruhend auf exzellenter Forschung

INDUSTRIAL SECURITY LAB

Das Angebotsspektrum der Industrial-Security-Labore reicht von Analysen für Industrie 4.0, Internet der Dinge und vernetzter Produktion bis hin zur Untersuchung der Sicherheit von 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 Sicherheits-Implementierungen.

- Hochpräzise EM-Messungen für die Seitenkanalanalyse
- Sicherheitsevaluierung eingebetteter Systeme gegenüber Hardware-basierten Angriffsvektoren
- Mehrere Laserstationen für Vorder- und Rückseiten-Fehlerinjektion
- Common Criteria Standort-Zertifizierung für die AEL-Stufe 7 (Evaluation Assurance

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
- Umgebung zertifiziert nach TISAX AL 3

Der Weg zum klimaneutralen Institut

Bis 2045 will das Fraunhofer AISEC klimaneutral sein. Mit diesem ehrgeizigen Ziel treibt Iris Karabelas als Beauftragte für Klimaneutralität und Nachhaltigkeit das Nachhaltigkeitsmanagement voran.

Wie klimaneutral ist das Fraunhofer AISEC?

Iris Karabelas: Wir sind auf einem guten Weg. Als Teil unserer Klimaschutzstrategie erfassen wir jährlich unsere Treibhausgasemissionen. Im Jahr 2022 haben wir 911 Tonnen CO_2-Äquivalente verursacht. Pro Kopf sind das 4,03 t CO_2 – im Vergleich zu Unternehmen gleicher Größe und Branche wenig. Das freut uns, aber die Bilanz zeigt auch: Unser Wärme- und Stromverbrauch sowie unsere Hardware verursachen einen Großteil unserer Emissionen.

Die Handlungsfelder sind also klar. Was passiert mit den Ergebnissen?

Iris Karabelas: Auf Basis unseres CO_2-Footprints haben wir Reduktionsmaßnahmen ermittelt und setzen diese nun Schritt für Schritt um. Beispielsweise beziehen wir inzwischen wie die anderen Fraunhofer-Institute auch zu 100 % grünen Strom. Perspektivisch wollen wir aber auch Lieferabhängigkeiten reduzieren und eigenen grünen Strom über eine Photovoltaik-Anlage produzieren sowie Fernwärme in unseren Energiemix integrieren.

Was wird abgesehen vom Bereich Strom und Wärme für den Klimaschutz getan?

Iris Karabelas: Da Emissionen bereits bei der Anfahrt zum Arbeitsplatz anfallen, fördert das Fraunhofer AISEC mobiles Arbeiten, bezuschusst ÖPNV-Tickets und unterstützt mit eigenen Ladesäulen die Nutzung von Elektroautos. Um CO_2-Emissionen durch eingekaufte Leistungen zu reduzieren, sind Nachhaltigkeitsstandards für Lieferanten inzwischen fester Bestandteil von Fraunhofer-Verträgen.

Uns ist außerdem wichtig, dass Nachhaltigkeit im Arbeitsalltag verankert ist. Daher bringen seit 2023 engagierte Mitarbeitende im AISEC-Zero-CO_2-Club klimaschützende Initiativen wie den Umstieg auf Recyclingpapier und das sichere, gemeinsame Nutzen von Hardware auf den Weg. Ebenso sensibilisieren sie die Belegschaft mit Aktions-tagen etwa zu nachhaltiger Ernährung und Mobilität sowie weiteren Maßnahmen für einen schonenden Umgang mit Ressourcen.

Wie wirkt sich das Engagement für Klimaneutralität auf Kunden aus?

Iris Karabelas: Wir stellen bei Projektanträgen und Vergabeverfahren immer häufiger fest, dass auch für unsere Kunden und Partner Nachhaltigkeit ein entscheidendes Kriterium ist. Durch unser Nachhaltigkeitsmanagement können wir nachweisen, dass wir ökologische Kundenanforderungen z. B. im Rahmen des Lieferkettensorgfaltspflichtengesetzes (LkSG) oder des weltweit anerkannten Nachhaltigkeitsstandards der Automobilbranche (Sustainability Assessment Questionnaire, SAQ 5.0) erfüllen. Das trägt dazu bei, dass wir ein attraktiver Forschungspartner und Arbeitgeber sind und bleiben.

Kontakt

Dr. Iris Karabelas
Beauftragte für Klimaneutralität
und Nachhaltigkeit
Tel. +49 89 3229986-1047
iris.karabelas@aisec.fraunhofer.de

Höchste Qualitätsstandards

Anpassungsfähig dank kontinuierlichem Qualitätsmanagement

Wissenschaftliche Exzellenz, systematische Verbesserung von Prozessen und adäquate Reaktionen auf Veränderungen und Wünsche unserer Kunden und Partner sind ausschlaggebend für unseren Erfolg. Dies gewährleistet ein kontinuierliches und wirkungsvolles Qualitätsmanagement am Fraunhofer AISEC.

TISAX®
(Trusted Information Security Assessment Exchange)

Für die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen gibt es in der Automobilindustrie definierte Standards. Die ENX Association unterstützt mit TISAX® im Auftrag des Verbandes der Automobilindustrie (VDA) die gemeinsame Akzeptanz von Informationssicherheitsprüfungen in der Automobilindustrie. Das Fraunhofer AISEC folgt dem Fragekatalog der Informationssicherheit des VDA und hat nach TISAX Assessment Level 3 umfangreiche Maßnahmen zum Schutz von Informationen von sehr hohem Schutzbedarf, von schutzbedürftigen Prototypenkomponenten, -bauteilen und -fahrzeugen und Bildaufnahmen schutzbedürftiger Objekte ergriffen und das Zertifikat nach TISAX Assessment Level 3 erhalten.

Common Criteria Site Certification

Die Common Criteria Site Certification ist ein internationaler IT-Sicherheitsstandard für vertrauenswürdige Software und Hardware. Seit 2024 gehört das Fraunhofer AISEC am Standort Garching zu einer ausgewählten Zahl von Laborinfrastrukturen, die offiziell zertifiziert sind, um Bewertungen von Hardware und Software auf Grundlage des Common Criteria-Standards durchzuführen. Das Fraunhofer AISEC hat die Common Criteria Standort-Zertifizierung für die EAL-Stufe 7 (Evaluation Assurance Level) abgeschlossen. Die Zertifizierung bestätigt, dass das Prüflabor und die Infrastruktur alle Anforderungen der Normen ISO/IEC 15408-1 :2009, -2 :2008, -3 :2008 sowie Common Criteria for Information Technology Security Evaluation (CC) erfüllen.

DIN EN ISO 9001:2015

Seit Dezember 2018 ist das Fraunhofer AISEC nach Din EN ISO 9001:2015, dem internationalen Qualitätsmanagement-Standard, zertifiziert. Für Partner und Kunden im In- und Ausland weisen wir damit unsere Leistungsfähigkeit, Effizienz und Serviceorientierung nach. Den hohen Standard unseres Ansatzes im Qualitätsmanagement bezeugen die sehr guten Ergebnisse der vergangenen Zertifizierungen durch die TÜV SÜD Management Service GmbH.

Unser Kuratorium

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

Dr. Astrid Elbe
Vice President Product Development,
Aviat Networks

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

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

Dr. Manfred Paeschke
Chief Visionary Officer,
Bundesdruckerei GmbH

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

Dr. Bettina Horster
Vorstand
VIVAI Software AG

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

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

Thomas Rosteck
Division President Connected Secure Systems, Infineon Technologies AG

Vera Schneevoigt
Geschäftsführende Gesellschafterin,
Guiding for Future GmbH

Dr. Stefan Wimbauer
stellv. Abteilungsleiter »Angewandte Forschung, Clusterpolitik«, Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie

Use Case: Zukunftsweisendes Condition Monitoring

Im Forschungsprojekt »AIQ-Bo« (»AI enhanced Intelligent Bolt«) zeigt der Fraunhofer CCIT den Mehrwert des Edge-Cloud-Continuums beispielhaft für die Anlagenüberwachung: Ein smarter Sensor erfasst Vibrationen an mechanischen Komponenten in Windkraftanlagen oder Brückenkränen und meldet Anomalien, um Schäden sowie Ausfälle zu verhindern.

Eine KI unmittelbar am Sensor wertet Vibrationsdaten lokal aus, erkennt eigenständig Abweichungen vom Normalbetrieb und meldet sie an die Cloud. Rechenintensive Aufgaben wie das Training des KI-Algorithmus oder Anpassungen des Modells erfolgen in der Cloud, von der aus die KI in der Edge aktualisiert wird. Die Vorverarbeitung der Daten direkt im Edge-Device reduziert den Datentransfer erheblich und macht das System äußerst energieeffizient. Die Cloud besticht durch ihre Skalierbarkeit und Kosteneffizienz.

Projekt »AIQ-Bo«

Vom Sensor zur Cloud und zurück: Technologien für die digitale Transformation

Das Internet der Dinge (IoT) verändert die technologischen Anforderungen grundlegend. Ausschließlich entweder auf dezentrale Datenverarbeitung oder auf Netzwerk-Computing in fernen Rechenzentren zu setzen, greift zu kurz. Um das volle Potenzial der digitalen Transformation zu heben, bedarf es neuer Technologien, mit denen Edge- und Cloud-Computing zu einem kontinuierlichen Datenraum verschmelzen. So wird Rechenkapazität dynamisch dort genutzt, wo es am effizientesten ist.

Nahtloser Datenfluss im Edge-Cloud-Continuum

Für Prozesse, die in Sekundenbruchteilen abgeschlossen sein müssen, werden Rechenleistung und Speicherplatz der Edge genutzt – d. h. lokaler Sensoren, Maschinen oder Endgeräte. Daten werden in Echtzeit dort analysiert, gefiltert oder komprimiert, wo sie erzeugt werden. Das minimiert Latenzzeiten, entlastet das Netzwerk und stellt auch ohne Internetverbindung die Funktionalität sicher. Zeitunabhängige und rechenintensive Aufgaben wie Simulationen oder das Training eines KI-Algorithmus erfolgen dagegen in der Cloud. Hier sind Speicherplatz und Rechenleistung skalierbar und die Kosten überschaubar. Die dynamische Nutzung von Edge und Cloud erfolgt automatisch, abhängig von Datenaufkommen und Anforderungen. Wichtig für diesen dynamischen Datenfluss innerhalb des Edge-Cloud-Continuums sind Datenraum-Konnektoren wie der Eclipse Dataspace Connector EDC. Sie machen es möglich, dass Daten nachhaltig aufbereitet, abgerufen und geteilt werden, um neues Wissen zu generieren.

Angewandte Spitzenforschung aus einer Hand

Mit dem Fraunhofer AISEC als Sprecherinstitut bringt der Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT angewandte Spitzenforschung mehrerer Fraunhofer-Institute zusammen, um Technologien für das Edge-Cloud-Continuum voranzutreiben: Von vertrauenswürdiger IoT-Technik für Sensoren und Kommunikationsmodule über intelligente und sichere Datenräume bis hin zu innovativen Methoden des maschinellen Lernens. »Die maßgeschneiderten Lösungen des Fraunhofer CCIT ermöglichen Unternehmen, ihre Prozesse und Produkte zukunftsfähig zu gestalten und ihr Innovationspotential voll auszuschöpfen«, erklärt Michael Fritz, Geschäftsstellenleiter des Fraunhofer CCIT. Neben der Technologieentwicklung bieten die Forschenden des Fraunhofer CCIT umfassende Unterstützung bei der Integration einzelner Komponenten für das reibungslose Zusammenspiel von Edge und Cloud.

Kontakt

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

Weiterführende Informationen

Webseite Fraunhofer CCIT

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 Vertrauens-würdigkeit von digitalen Anwendungen erhöhen.

Sicherheitsrelevante Schwachstellen sowohl in Hardware als auch in Soft-ware finden und schließen.

In modern ausgestatteten Cybersicherheitslaboren forschen.

Neueste Forschungs-ergebnisse 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 voran-treiben und sich schnell weiterentwickeln.

Auszeichnungen der Fraunhofer-Gesellschaft als Arbeitgeber

1. PLATZ
Attraktivste Arbeitgeber
2023
Für Absolventen
Forschung
trendence

Most Attractive Employers Germany universum 2023

Most Attractive Employers Germany universum 2023

glassdoor BESTE ARBEITGEBER 2022

Dr.-Ing. Nisha Jacob Kabakci

Leiterin der Forschungsgruppe »Physical Analysis and Countermeasures«

»Neueste Hardware und besonders FPGAs faszinieren mich. Für ihre Absicherung blicke ich unter die Oberfläche: Ich prüfe Sicherheitseigenschaften, entwickle Sicherheitsstrategien und ermögliche ihre sichere Nutzung durch Wirtschaft und Gesellschaft.«

In ihrer Heimatstadt, der Großstadt Bangalore in Indien, ergreifen Frauen häufig einen technischen Beruf. Von ihrer großen Familie bekommt sie viel Rückenwind als sich Nisha Kabakci an der Visvesvaraya Technological Universität für den Bachelorstudiengang der Elektrotechnik einschreibt. Ihr Entdeckergeist und ihre Weltoffenheit führen sie nach dem Bachelorstudium in die Schweiz. An der USI Università della Svizzera italiana in Lugano studiert sie Embedded Systems im Masterstudiengang. In einer Vorlesung zur IT-Sicherheit wird sie auf Kryptografie aufmerksam. Bereits in ihrem zweiten Master-Jahr absolviert sie ein einjähriges Praktikum an der Nanyang Technological University (NTU) in Singapur. Schwerpunkt des Praktikums liegt auf kryptografischen Verfahren und ihrer Implementierung auf kleinen Microcontrollern. So kommt sie zum ersten Mal mit angewandter IT-Sicherheit in Berührung.

»Beim Absichern von Hardware-Systemen sehe ich einen direkten Effekt meiner Arbeit. Zudem hat meine Tätigkeit eine hohe gesellschaftliche Relevanz. Dies hat mich bestärkt, mir eine Karriere in der IT-Sicherheit aufzubauen«, sagt Nisha Jacob Kabakci. Sie schreibt wissenschaftliche Artikel, besucht Konferenzen und sucht aktiv nach einer Arbeitsstelle, die eigene Forschungsvorhaben und gleichzeitig Praxis in der IT Security ermöglicht. Fündig wird sie beim Fraunhofer AISEC. Sie wird wissenschaftliche Mitarbeiterin im Bereich Embedded Systems Security am Fraunhofer AISEC und nimmt zugleich ihre Promotion an der TUM bei Georg Sigl am Lehrstuhl für Sicherheit in der Informationstechnik auf, die sie 2020 erfolgreich abschließt.

Auf Entdeckungstour im Hardware Security Lab

Von Projekt zu Projekt untersucht sie am Fraunhofer AISEC eingebettete Systeme – insbesondere integrierte Schaltkreise wie Field-Programmable Gate Arrays (FPGAs) und FPGA Sytem on Chips – auf ihre Sicherheit, entdeckt Schwachstellen und entwickelt Maßnahmen zur Absicherung und Risikominimierung. »Meine Arbeit ist sehr abwechslungsreich, spannend und gleichzeitig herausfordernd. Ich schätze unsere offene Kultur und die gegenseitige Unterstützung der Kolleginnen und Kollegen«, erzählt sie. Als Leiterin der Gruppe »Physical Analysis and Countermeasures« setzt sie auf Pluralität, gegenseitiges Zuhören und gemeinsame Ziele.

Im Hardware Security Lab des Fraunhofer AISEC untersucht sie zusammen mit ihrem Team physikalische Angriffe: Vermeintlich sichere Chips werden dort einer Seitenkanalanalyse unterzogen. Dabei liest eine Sonde mirkometer-weise elektromagnetische Impulse des Chips aus und entlockt ihm seinen kryptografischen Schlüssel. Für Fault-Injection-Angriffe werden Laser zur Manipulation eines Chips eingesetzt, sodass er unter falschen Voraussetzungen weiterrechnet. Gleiche Ergebnisse erzielen Glitching-Angriffe, die die Versorgungsspannung oder Taktfrequenz für Bruchteile von Sekunden verändern. Mit dem Wissen um vorhandene Schwachstellen unterstützt Kabakci Kunden und öffentliche Institutionen bei der Entwicklung neuer Sicherheitslösungen. Die Common-Criteria-Zertifizierung des Hardware Security Lab ermöglicht neuartige Projekte mit besonderem Schutzniveau. Durch gebäudetechnische und personelle Sicherheitsvorkehrungen ergeben sich für sie neue Arbeitsprozesse und Aufgaben. Kabakci freut sich auf kommende Herausforderungen und neue Erkenntnisgewinne, um Hardware noch besser abzusichern.

Ferdinand Jarisch

Doktorand in der Abteilung »Product Protection and Industrial Security«

Maßnahmen der Cybersecurity sind nur dann erfolgreich, wenn sie auf das System zugeschnitten sind. Dafür muss man das System verstanden haben und seine Schwachstellen kennen, und genau das ist mein Job am Fraunhofer AISEC.«

Ferdinand Jarisch hat Physik an der TUM studiert. Im Master vertiefte er sich in die Quantenoptik. Sein Weg in Richtung Grundlagenforschung schien vorgezeichnet. Doch dann lernte Jarisch in einer Vorlesung die Quantenkryptografie kennen – und war sofort begeistert. Insbesondere der abhörsichere Austausch von Schlüsseln zur Absicherung von Kommunikation durch Quantenphysik beeindruckte ihn. Hier verband sich seine Leidenschaft Rätsel zu lösen und tief in Systeme einzutauchen mit seinem Wunsch zu programmieren und zu coden: Bereits während des Studiums hatte er ein Programm gescripted, das Tickets für Sneak-Premieren auf den besten Plätzen im Kinosaal reservierte. Die Häufigkeit seiner Teilnahmen an Hacking-Contests wie Capture-The-Flag-Events (CTF) stieg mit der Studiendauer stetig an. Escape Games und Geocaching verfestigten sich zu Hobbies. Jarisch hatte seine Berufung gefunden: Rätsel knacken für die Cybersecurity. Diese Fähigkeit wollte er nun auf ein professionelles Level heben – und fand dabei schnell das Fraunhofer AISEC.

Cybersecurity für Automotive und Industrie

Jarisch ist direkt am aktuellen Geschehen dran und kennt die Herausforderungen seiner Kunden aus Automotive und Industrie. Der Schwerpunkt seiner Forschung ist das automatisierte Finden von Schwachstellen in eingebetteten Systemen. Die kleinen Superhirne machen das Internet of Things (IoT) immer relevanter und sind das Herz von vielen intelligenten Geräten, z. B. im Smart Home oder der Smart Factory. Beim Pentesting für Automotive taucht Jarisch mit seinen Kolleginnen und Kollegen in die IT-Systeme von Fahrzeugen ein, versucht diese zu verstehen und Schwachstellen zu finden. Dazu gehören beispielsweise die Möglichkeit zur Manipulation der Kilometeranzeige oder das Umgehen digitaler Bezahldienste. Gleichzeitig müssen Unternehmen immer wieder neue Regularien beachten, z. B. dass Cybersecurity-Eigenschaften schon in der Produktionsphase eingebaut werden. Jarisch hat diese Vorgaben für seine Kunden im Blick, prüft Fahrzeug-Prototypen vor dem Release oder erstellt Security-Konzepte, die Systeme so designen, dass sie möglichst sicher sind. Dabei hat er die zentralen digitalen Fahrzeug-Technologien auf dem Schirm, wie Anwendungen, die Kommunikation mit dem Backend des Herstellers oder zwischen Fahrzeugen und deren Umgebung.

Für den Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA) erstellt er seit 2018 eine Studie zur Produktpiraterie, die wichtige Erkenntnisse liefert, wie Unternehmen sich vor dem Raub ihres geistigen Eigentums schützen können. Neben seiner wissenschaftlichen Arbeit ist Jarisch Vertreter des Fraunhofer AISEC beim Wissenschaftlichen Technischen Rat (WTR) von Fraunhofer, der als unternehmensinternes Beratungsorgan den Fraunhofer-Vorstand berät. Seine
Fähigkeit knifflige Situation schnell und souverän zu lösen, setzt Jarisch seit 2008 auch für das Technische Hilfswerk (THW) ein. Als gut ausgebildete THW-Führungskraft war er bereits bei Auslandseinsätzen in Moldau, Haiti und Guatemala.

Barbora Hrdá

Doktorandin in der Abteilung »Secure Operating Systems«

In einem naturwissenschaftlichen Gymnasium, umgeben von hauptsächlich männlichen Lehrern und Mitschülern, beschreibt sich Barbora Hrdá als zurückhaltendes Mädchen mit Migrationshintergrund. Zwar weiß sie um ihre Stärke in der Mathematik, ist sich aber nicht sicher, ob diese für ein technisches Studium reichen würde.

Als gebürtige Pragerin folgt sie ihren kulturellen Wurzeln und studiert Slavistik und Theaterwissenschaft an der LMU. Sie beendet das Bachelorstudium mit sehr guten Noten. Doch die Frage nach ihrer eigentlichen Berufung bleibt. Auf dem Jakobsweg von León nach Finisterre befreit sie sich von fremden Zuschreibungen. »Für mich selbst muss es richtig sein«, erkennt sie und schreibt sich kurz darauf für den interdisziplinären Informatikstudiengang »Computing in the Humanities« an der Universität Bamberg ein. Die Freude an Mathematik, Logik, Statistik, Programmieren und Entwickeln von Softwaresystemen bestätigt ihr, auf dem richtigen Weg zu sein. Ihr erfolgreich absolvierter Masterabschluss erfüllt sie mit Stolz und neuem Selbstvertrauen. »Ich muss mich nicht verstecken. Wenn ich etwas nicht weiß, dann lerne ich es«, so geht sie nun die Dinge an.

In der Zeit als IT-Trainee in einem Unternehmen gefällt es ihr, Neues auszuprobieren und an unterschiedlichen Aufgaben zu wachsen. Genau dies fehlt ihr jedoch in ihrem ersten Job. Mit dem Wunsch, ihre eigenen Ideen einzubringen und mit ihrer Tätigkeit einen positiven gesellschaftlichen Impact zu bewirken, bewirbt sie sich bei Fraunhofer.

Wertschätzung und Raum für Entfaltung

Bereits beim Vorstellungsgespräch am Fraunhofer AISEC wird sie ernst genommen. Dieses Gefühl der Wertschätzung ist ihr bis heute geblieben. Nach vier Jahren am Fraunhofer AISEC blickt sie auf eine steile Lernkurve und spannende Projekte zurück. Sie startet im Bereich Mobile Security und Virtualisierungstechnologien. Heute spezialisiert sie sich auf die IT-Sicherheit von Quantencomputing-Plattformen. Sie beschäftigt sich mit Schutzmechanismen für diese Zukunftstechnologie und nutzt hierfür klassische sowie quantenmechanische Ansätze. »Das erfordert eine ganz andere Art zu Denken und viel Kreativität«, sagt sie. Sie analysiert Datenströme, entwickelt Ideen und konzeptioniert Sicherheitstools, die das Spektrum von Security-Maßnahmen spezifisch für den Bereich des Quantencomputings erweitern. Dabei untersucht sie beispielsweise Verschlüsselungsmöglichkeiten zwischen einem klassischen Client und einem Quantenserver. Damit legt sie den Grundstein für eine sichere Nutzung von Quantencomputern durch Wirtschaft und Gesellschaft. Für sie zählen Neugierde, Freude am Lernen, Gestaltungsfreiheit und die gesellschaftliche Relevanz ihrer Arbeit.

Aktuell verfolgt Barbora ihr Promotionsprojekt zur Integrität und Vertraulichkeit von Daten für Quantencomputing as a Service. Ihre wissenschaftlichen Erkenntnisse finden direkte Anwendung in Kundenprojekten und bieten so einen echten Mehrwert für Wirtschaft und Gesellschaft.

Mache das, was dir am Herzen liegt – dieses Prinzip gilt auch für die Berufswahl. Wissbegierde, das Einbringen eigener Ideen und ein positiver Effekt für Wirtschaft und Gesellschaft sind bei meiner Arbeit das A&O.«

Martin Seiffert

Senior Scientist in der Abteilung »Secure Systems Engineering«

Wir strukturieren den Werkzeugkasten und helfen bei der Auswahl der richtigen Werkzeuge, um digitale Systeme sicher zu gestalten und zu betreiben.«

Auf seinem Smartphone speichert Martin Seifert unterschiedliche elektronische Nachweise, mit denen er sich für Online-Dienste identifiziert. Der digitale Personalausweis erleichtert ihm beispielsweise die Steuererklärung. Auch Krankenkassen-Apps probiert der Berliner aus. Er ist neugierig, wie seine Arbeit praktisch wirkt.

Nach seinem Diplom in Informatik und seiner Tätigkeit als wissenschaftlicher Mitarbeiter sowie Doktorand an der Freien Universität Berlin forscht Seiffert seit 2018 in der Abteilung »Secure Systems Engineering« am Fraunhofer AISEC an Informationssicherheit und sicheren digitalen Identitäten. Zusammen mit Industriepartnern und öffentlichen Einrichtungen wie im Innovationswettbewerb »Schaufenster Sichere Digitale Identitäten« des Bundesministeriums für Wirtschaft und Klimaschutz unterstützt der Informatiker bei der Konzeption sicherer eID-Lösungen und digitaler Ökosysteme sowie bei deren Evaluation hinsichtlich internationaler Standards, nationaler Richtlinien und europäischer Verordnungen wie z. B. der eIDAS-Verordnung (Electronic Identification and Trust Services). Sein Ziel ist, Informationssicherheit ganzheitlich im Einklang mit weiteren Anforderungen wie Privatsphäre, Nutzbarkeit, Interoperabilität und Skalierbarkeit umzusetzen.

Digitale Identitäten in vertrauenswürdiger Umgebung

In einem sicheren Ökosystem entscheiden neben digitalen Identitäten weitere Faktoren darüber, ob ein Zugriff auf sensible Daten gewährt wird. Mit diesem Verständnis haben Seiffert und sein Team ein Konzept für die künftige Sicherheitsarchitektur der Telematik-Infrastruktur entwickelt. Im Informationsnetz des Gesundheitswesens können bisher nur ausgewählte Stakeholder wie Praxen, Krankenhäuser, Apotheken und Krankenkassen mit proprietärer Hardware auf Patientendaten oder eRezepte zugreifen. Für zukunftsfeste Gesundheitsdienste setzt der Logik-orientierte Seiffert auf Zero Trust: Jeder einzelne Zugriff wird geprüft, authentisiert und autorisiert – anhand einer eID auf einem Smartphone in Kombination mit Faktoren wie Ort und Zeit des Zugriffs. Dass trotz eines so datenhungrigen Ansatzes die Privatsphäre der Nutzenden gewahrt bleibt, ist dem Forscher ein besonderes Anliegen, sowohl für die Millionen von Menschen, deren privateste Daten durch seine Arbeit beeinflusst werden (mehr Infos zur Telematikinfrastruktur auf Seite 21) als auch persönlich.

Mit Logik und Struktur zur besten Lösung

Seiffert sieht seine Stärke im Verständnis für Struktur. Der Analytiker betont: »Wenn wir große Digitalisierungsvorhaben voranbringen wollen, müssen wir verstehen, welche Instrumente uns bei wegweisenden Entscheidungen helfen können.« Sein Forschungsbereich fußt auf umfangreicher Erfahrung und Know-how. In hochkomplexen Systemen den Überblick zu bewahren, ist eine anspruchsvolle Aufgabe, bei der Seiffert seinen Kunden regelmäßig mit Leidenschaft unter die Arme greift. Mit seinem Team bereitet er Lösungsoptionen so systematisch und verständlich auf, dass sie messbar und damit vergleichbar werden. Sein Hang zur Methodik erlaubt ihm fundierte Entscheidungen zugunsten guter, praktikabler Lösungen – nicht perfekter Lösungen, denn nach denen sucht man in seinem dynamischen Fachgebiet vergeblich.

Publikationen

Alexander Küchler, Leon Wenning, Florian Wendland: »AbsIntIO: Towards Showing the Absence of Integer Overflows in ARM Binaries«. In: Proceedings of ACM Asia Conference on Computer and Communications Security. ASIA CCS '23. 2023.

Anna-Magdalena Krauß, Sandra Kostic, Rachelle A. Sellung: »A more User-Friendly Digital Wallet? User Scenarios of a Future Wallet«. Open Identity Summit 2023. DOI: 10.18420/OID2023_06. Bonn: Gesellschaft für Informatik e.V. pp. 73-84. Regular Research Papers. Heilbronn, Germany. 15.-16. June 2023.

Anna-Magdalena Krauß, Sandra Kostic, Rachelle A. Sellung: »Ist das die Wallet der Zukunft?« HMD 60, 344–365 (2023).

Bernhard Lippmann, et al.: »VEFIDES: Designing Trustworthy Supply Chains Using Innovative Fingerprinting Implementations«. In: Design, Automation & Test in Europe Conference & Exhibition (DATE). 2023.

Carl Riehm, Christoph Frisch, Florian Burcea, Matthias Hiller, Michael Pehl, Ralf Brederlow: »Structured Design and Evaluation of a Resistor-Based PUF Robust Against PVT-Variations«. In: International Symposium on Design and Diagnostics of Electronic Circuits and Systems (DDECS). 2023.

Christian Banse, Immanuel Kunz, Nico Haas, Angelika Schneider: »A Semantic Evidence-based Approach to Continuous Cloud Service Certification«. In: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. SAC '23. New York, NY, USA: Association for Computing Machinery, 2023.

Dariush Wahdany, Carlo Schmitt, Jochen L. Cremer: »More than accuracy: end-to-end wind power forecasting that optimises the energy system«. In: Electric Power Systems Research. 2023.

Felix Oberhansl, Tim Fritzmann, Thomas Pöppelmann, Debapriya Basu Roy, Georg Sigl: »Uniform instruction set extensions for multiplications in contemporary and postquantum cryptography OFP+23«. In: Journal of Cryptographic Engineering (2023).

Hendrik Meyer zum Felde, Jean Luc Reding, Michael Lux: »Decentralized Geolocation and Time Enforcement for Usage Control«. In: 8th IEEE European Symposium on Security and Privacy Location. Privacy Workshop. 2023.

Immanuel Kunz, Konrad Weiss, Angelika Schneider, Christian Banse: »Privacy Property Graph: Towards Automated Privacy Threat Modeling via Static Graph-based Analysis«. In: Proceedings on Privacy Enhancing Technologies. 2023.

Johannes Geier, Lukas Auer, Daniel Mueller-Gritschneder, Uzair Sharif, Ulf Schlichtmann: »CompaSeC: A Compiler-Assisted Security Countermeasure to Address Instruction Skip Fault Attacks on RISC-V«. In: Proceedings of the 28th Asia and South Pacific Design Automation Conference. ASPDAC'23. New York, NY, USA: Association for Computing Machinery, pp. 676–682, 2023.

John Morris, Stefan Tatschner, Michael P. Heinl, Patrizia Heinl, Thomas Newe, Sven Plaga: »Cybersecurity as a Service«. In: Cybersecurity Vigilance and Security Engineering of Internet of Everything. Ed. by Kashif Naseer Qureshi, Thomas Newe, Gwanggil Jeon, Abdellah Chehri. Cham: Springer Nature Switzerland, 2024, pp. 141–161.

Konrad Hohentanner, Florian Kasten, Lukas Auer: »HWASanIO: Detecting C/C++ Intra-object Overflows with Memory Shading«. In: Proceedings of the 12th ACM SIGPLAN International Workshop on the State Of the Art in Program Analysis. 2023, pp. 27–33.

Konrad Hohentanner, Philipp Zieris, Julian Horsch: »CryptSan: Leveraging ARM Pointer Authentication for Memory Safety in C/C++«. In: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. SAC '23. New York, NY, USA: Association for Computing Machinery, 2023.

Konrad Hohentanner, Philipp Zieris, Julian Horsch: »CryptSan: Leveraging ARM Pointer Authentication for Memory Safety in C/C++«. In: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. SAC '23. New York, NY, USA: Association for Computing Machinery, 2023. ISBN: 9781450395175/23/03.

Konrad Hohentanner, Philipp Zieris, Julian Horsch: »CryptSan: Leveraging ARM Pointer Authentication for Memory Safety in C/C++ Hohentanner2023 CryptSan«. In: Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. SAC '23. New York, NY, USA: Association for Computing Machinery, 2023.

Marc Fischlin, Jonas von der Heyden, Marian Margraf, Frank Morgner, Andreas Wallner, Holger Bock: »Post-Quantum

Security for the Extended Access Control Protocol«. In: 8th Security Standardisation Research Conference, SSR 2023, Lyon, France. 2023.

Martin Schanzenbach, Christian Grothoff, Bernd Fix: »The GNU Name System« RFC 9498. Nov. 2023.

Maximilian Richter, Magdalena Bertram, Jasper Seidensticker, Marian Margraf: »Cryptographic Requirements of Verifiable Credentials for Digital Identification Documents«. SDIM/COMPSAC 2023.

Maximilian Kaul, Alexander Küchler, Christian Banse: »A Uniform Representation of Classical and Quantum Source Code for Static Code Analysis«. In: 2023 IEEE International Conference on Quantum Computing and Engineering. QCE '23. 2023, pp. 1013–1019.

Michael P. Heinl, Simon Gölz, Christoph Bösch: »Remote Electronic Voting in Uncontrolled Environments: A Classifying Survey«. In: ACM Comput. Surv., 2023.

Michael P. Heinl, Maximilian Pursche, Nikolai Puch, Sebastian Peters, Alexander Giehl: »From Standard to Practice: Towards ISA/IEC 62443conform Public Key Infrastructures«. In: SAFECOMP 2023: 42nd International Conference on Computer Safety, Reliability and Security. Toulouse, France: Springer International Publishing, 2023, pp. 196–210.

Nicolas Müller, Jochen Jakobs, Jennifer Williams, Philip Sperl, Konstantin Böttinger: »Localized Shortcut Removal«. In: The 2nd XAI4CV Workshop at CVPR 2023 (2023).

Nicolas Müller, Jochen Jochen, Jennifer Williams, Konstantin Böttinger: »Localized Shortcut Removal«. In: 2nd XAI4CV Workshop at CVPR. 2023.

Nicolas Müller, Philip Sperl, Konstantin Böttinger: »Complex valued neural networks for antispoofing«. In: Interspeech 2023 (2023).

Philipp Fuxen, Rudolf Hackenberg, Michael P. Heinl, Mirko Ross, Heiko Roßnagel, Christian H. Schunck, Raphael Yahalom: »Lock-in Thermography for the Localization of Security Hard Blocks on SoC Devices«. In: Open Identity Summit 2023. Ed. by Heiko Roßnagel, Christian H. Schunck, Jochen Günther. Gesellschaft für Informatik e.V., 2023.

Philipp Fuxen, Rudolf Hackenberg, Michael P. Heinl, Mirko Ross, Heiko Roßnagel, Christian H. Schunck, Raphael Yahalom: »MANTRA: A Graphbased Unified Information Aggregation Foundation for Enhancing Cybersecurity Management in Critical Infrastructures«. In: Open Identity Summit 2023. Ed. by Heiko Roßnagel, Christian H. Schunck, Jochen Günther. Gesellschaft für Informatik e.V., 2023.

Sandra Kostic, Maija Poikela: »Der Wandel von Vertrauen in eine digitale Identität? – Einblicke in eine Nutzerstudie«. HMD 60, 322–343 (2023).

Sandra Kostic, Maija Poikela: »The State or Private Enterprise? — The Shift in Users' Preference for the Provider of an Identity Wallet". SOUPS 2023 - Symposium on Usable Privacy and Security. 7. Aug. 2023

Stefan Tatschner, Sebastian Peters, David Emeis, John Morris, Thomas Newe: »A Quic(k) Security Overview: A Literature Research on Implemented Security Recommendations«. In: ARES 2023. Benevento, Italy: ACM, 2023.

Stefan-Lukas Gazdag, Sophia Grundner Culemann, Tobias Heider, Daniel Herzinger, Felix Schärtl, Joo Yeon Cho, Tobias Guggemos, Daniel Loebenberger: »Quantumresistant MACsec and IPsec for Virtual Private Networks«. In: Günther, F., Hesse, J. (eds) Security Standardisation Research. SSR 2023. Lecture Notes in Computer Science, vol 13895. Springer, Cham.

Stefan-Lukas Gazdag, Sophia Grundner Culemann, Tobias Heider, Daniel Herzinger, Felix Schärtl, Joo Yeon Cho, Tobias Guggemos, Daniel Loebenberger: »8th Security Standardisation Research Conference, SSR 2023, Lyon, France, April 2023«. In: Security Standardisation Research. Ed. by F. Günther, J. Hesse. Vol. 13895. Lecture Notes in Computer Science. Berlin, Heidelberg, 2023, pp. 1–21.

Sebastian Sitaru, Georg Bramm, Alexander Zink, Matthias Hiller: »Cybersecurity in digital healthcare – challenges and potential solutions«. In: Die Dermatologie (2023).

Stefan-Lukas Gazdag, Sophia Grundner-Culemann, Tobias Heider, Daniel Herzinger, Felix Schärtl, Joo Y. Cho, Tobias Guggemos, Daniel Loebenberger: »Quantum-resistant MACsec and IPsec for Virtual Private Networks«. In: 8th Security Standardisation Research Conference, SSR 2023, Lyon, France. 13895, 1–21. 2023

Simon Ott, Monika Kamhuber, Joana Pecholt, Sascha Wessel: »Universal Remote Attestation for Cloud and Edge Platforms«. In: Proceedings of the 18th International Conference on Availability, Reliability and Security. ARES '23. Benevento, Italy: Association for Computing Machinery, 2023.ISB N: 9798400707728.

Tobias Holl, Katharina Bogad, Michael Gruber: »Whiteboxgrind – Automated Analysis of Whitebox Cyptography«. In: Constructive Side-Channel Analysis and Secure Design. Ed. by E. B. Kavun, M. Pehl. COSADE 2023. Springer Nature Switzerland, 221–240, 2023.

Tudor Soroceanu, Nicolas Buchmann, Marian Margraf: »On Multiple Encryption for Public-Key Cryptography«. Cryptography. 2023; 7(4):49.

Publikationen

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, Pia Kinzler,
Tobias Steinhäußer (Leitung)

Layout
Maria Schwab-Kloe

Grafiken
Daniela Miedaner

Druck
Zimmermann GmbH Druck & Verlag

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

Cover
Gezielte elektromagnetische Messungen auf einem
freigelegten Chip im Hardware Lab des Fraunhofer AISEC.

Bildquellen
Cover: Oliver Bodmer
Seite 4: Bernd Müller, Andreas Heddergott
Seite 9: MAN, Andreas Heddergott
Seite 10: Freepik, Fraunhofer AISEC
Seite 13: Oliver Bodmer
Seite 14: Freepik, Fraunhofer AISEC
Seite 17: Andreas Heddergott, Creative Commons/TECNALIA
Seite 18: Gene Glover, AllEyesOnYou.de, Freepik
Seite 21: Adobe Stock, AllEyesOnYou.de, Oliver Bodmer
Seite 22: Oliver Bodmer, Andreas Heddergott
Seite 24: Oliver Bodmer
Seite 26: HGEsch
Seite 32: Andreas Heddergott/TUM, Oliver Rösler, Adam
Bacher, Bundesdruckerei GmbH, Rene Bertrand, Bundesdruckerei GmbH
Seite 33: Werner Bartsch; Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie; Hessian.AI
Seite 34: Fraunhofer CCIT
Seite 35: Fraunhofer-Gesellschaft
Seite 38: Oliver Bodmer
Seite 41: Oliver Bodmer
Seite 42: Oliver Bodmer
Seite 45: Gene Glover
Alle übrigen Abbildungen: © Fraunhofer AISEC

Folgen Sie uns!

Cybersecurity-Blog des Fraunhofer AISEC

LinkedIn

XING

X