Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC | Jahresbericht 2024

Jahresbericht 2024

Mit Sicherheit innovativ

#mitsicherheitinnovativ

Jahresbericht 2024

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 digitale Transformation unserer Gesellschaft schreitet weiter voran – und mit ihr wachsen die Herausforderungen für eine sichere digitale Zukunft. Neue gesetzliche Vorgaben wie der Cyber Resilience Act, NIS-2 und die Maschinenverordnung IEC 62443 setzen wichtige Impulse für mehr Cybersicherheit. Doch wie lassen sich regulatorische Anforderungen konkret umsetzen, ohne Innovationen auszubremsen?

Am Fraunhofer AISEC entwickeln wir wissenschaftlich fundierte, praxisnahe Lösungen, die Unternehmen und öffentliche Einrichtungen unterstützen, Sicherheitsstandards zu erfüllen, Risiken zu minimieren und ihre digitalen Geschäftsmodelle zu stärken.

Im Zentrum unserer Arbeit standen 2024 unter anderem automatisierte Cloud-Zertifizierungen, quantensichere und kryptoagile Fernfreigaben für Werkzeugmaschinen, der Aufbau von Resilienz gegenüber generativer KI sowie vertrauenswürdige Mikroelektronik.

Besonderes Augenmerk lag auf der Post-Quanten-Kryptografie, mit der wir vernetzte Systeme – vom autonomen Fahrzeug bis zur digitalen Identität – langfristig absichern. Gleichzeitig bringen wir im Lernlabor Cybersicherheit unser Wissen in die Praxis, um die Resilienz von Unternehmen und öffentlichen Organisationen gegenüber Cyberangriffen zu stärken. Denn nachhaltige Sicherheit entsteht durch Wissensvermittlung, vorausschauende Maßnahmen und Zusammenarbeit, die zukünftige Herausforderungen adressiert.

Mit gezielter Vorlaufforschung, wissenschaftlicher Exzellenz und marktgerechter Umsetzung von IT-Sicherheitslösungen sichert und stärkt das Fraunhofer AISEC die globale Wettbewerbsfähigkeit von Unternehmen insbesondere aus unserer Region, Deutschland und Europa.

Wir wünschen Ihnen eine anregende Lektüre!

Herzliche Grüße

Prof. Dr. Claudia Eckert

Prof. Dr. Georg Sigl

Inhalt

CRA, NIS-2 & Co. – neue Regularien für mehr Cybersicherheit nutzen

Regelwerke wie der Cyber Resilience Act (CRA), die NIS-2 und IEC 62443 Maschinenverordnung setzen neue Maßstäbe für das Sicherheitsniveau von digitalen Produkten und Infrastrukturen. Das Fraunhofer AISEC zeigt auf, wie Unternehmen durch die Umsetzung von Mindeststandards regulatorische Anforderungen erfüllen, Sicherheit aufbauen und ihre digitalen Geschäftsmodelle zukunftssicher machen.

Die Digitalisierung in Deutschland und Europa schreitet voran, doch mit ihr wächst auch die Angriffsfläche für Cyberkriminelle. Die Zahl der Cyberangriffe steigt rasant – laut einer Bitkom-Studie zur Cybersicherheitslage in Deutschland von 2024 meldeten 91 Prozent der deutschen Unternehmen Vorfälle von Datendiebstahl, Spionage oder Sabotage, mit einem geschätzten wirtschaftlichen Schaden von 267 Milliarden Euro. Besonders betroffen sind kritische Infrastrukturen, die zunehmend Ziel von aus dem Ausland gesteuerten Angriffe werden. Die Bedrohungslage wird durch neue Angriffsmethoden mithilfe künstlicher Intelligenz noch verschärft.

Vor diesem Hintergrund zielen die neuen Anforderungen an die Cybersicherheit, wie der Cyber Resilience Act (CRA), NIS-2-Richtlinie oder die Maschinenverordnung IEC 62443, auf die Stärkung des Vertrauens in digitale Produkte und die Förderung des europäischen Binnenmarkts sowie digitaler Geschäftsmodelle ab.

CRA, NIS-2 und IEC 62443 als neue Leitplanken

Der CRA legt erstmals europaweit einheitliche Anforderungen für die Cybersicherheit digitaler Hardware- und Software-Produkte fest. Hersteller, Einführer und Händler müssen umfassende Sicherheitsmaßnahmen implementieren, darunter Risikobewertungen, Schwachstellenmanagement und Inventarlisten für Softwarekomponenten (sogenannte Software Bill of Materials). Unternehmen, die gegen diese Vorschriften verstoßen, riskieren hohe Geldstrafen und den Verlust des Marktzugangs.

Die NIS-2-Richtlinie erweitert den Geltungsbereich der Cybersicherheitsanforderungen auf zahlreiche Sektoren, darunter Gesundheitswesen, Verkehr und Energie. Sie verpflichtet Unternehmen zur Einführung eines Cyber-Risikomanagements und zur Meldung von Sicherheitsvorfällen. Verstöße können mit Bußgeldern von bis zu zehn Millionen Euro geahndet werden.

Ergänzend definiert die IEC 62443-Norm Sicherheitsanforderungen für industrielle Automatisierungs- und Steuerungssysteme. Sie legt Standards für sichere Produktentwicklungsprozesse und den »Secure-by-Design«-Ansatz fest, um Risiken bereits in der Entwurfsphase zu minimieren.

Die Einhaltung dieser Vorschriften nehmen Unternehmen, insbesondere KMUs, als sehr herausfordernd wahr. Die Vielzahl an Anforderungen erscheint komplex und ihre Umsetzung ressourcenintensiv.
Mit intelligenter Automatisierung kann die Einhaltung regulatorischer Vorgaben jedoch effizient und ressourcenschonend gestaltet und die eigene Cybersicherheit nachhaltig gestärkt werden. »Es gibt bereits heute eine Vielzahl an Technologien und Maßnahmen, die wirksam gegen viele Angriffe schützen. Mit den neuen EU-Regelwerken stehen nun für Unternehmen hilfreiche Leitplanken zur Verfügung, um Mindeststandards zu realisieren«, erläutert Prof. Dr. Claudia Eckert, Institutsleiterin des Fraunhofer AISEC.

Mindeststandards umsetzen und wirksamen Schutz aufbauen

Ein Schlüsselelement für eine effektive Umsetzung der verschiedenen Regularien ist die Erstellung eines Mappings zwischen den vielfältigen Anforderungen, um Überschneidungen zu identifizieren und Effizienzpotenziale zu nutzen. Dies reduziert redundante Maßnahmen und schafft eine Sicherheitsgrundlage auf Basis der identifizierten Mindeststandards. »Mit diesen sichern Unternehmen nicht nur ihre Marktzugänge, beispielsweise zum EU-Binnenmarkt mittels der CE-Kennung, oder vermeiden Sanktionen bei Gesetzesverstößen, sie schützen sich auch vor Missbrauch, Datenverlust und Spionage«, sagt Eckert.

Als zentrale Gemeinsamkeiten in den zu erfüllenden Anforderungen identifiziert Eckert:

- das Aufsetzen von Risk-Assessment-Prozessen
- die Implementierung eines Schwachstellenmanagements zum Beispiel mit Patches und Updates über den gesamten Produktlebenszyklus
- die Sicherstellung von Business Continuity etwa mittels eines Back-up- und Krisenmanagements
- die Gewährleistung der Sicherheit der digitalen Lieferkette beispielsweise anhand der Erfassung der genutzten Hard- und Softwarekomponenten mit der Software Bill of Materials (SBOM)
- das Aufsetzen eines Informationssicherheits-Managementsystems (ISMS), in dem etwa Zugriffsrechte sicher verwaltet werden und klare Regeln zum Umgang mit Passwörtern sowie E-Mails verankert sind
- die Umsetzung eines kontinuierlichen Berichts- und Meldewesens, zum Beispiel mit regelmäßigen Konformitätsnachweisen und einer kontinuierlichen Dokumentation der getroffenen Vorkehrungen sowie ihrer Wirksamkeit
- die Realisierung von angemessenen Sicherheitsmaßnahmen entsprechend dem Stand der Technik, etwa gemäß Zero-Trust, Multi-Faktor-Authentifizierung etc.

Automatisierung als Erfolgsfaktor

(Teil-)automatisierte Tools ermöglichen es, die Einhaltung dieser Maßnahmen kontinuierlich zu überwachen, zu dokumentieren und Konformitätsnachweise zu erstellen. Mit KI-Lösungen lässt sich die Geschwindigkeit der Cyberabwehr deutlich erhöhen und der Aufwand für effektiven Schutz minimieren.

Das Fraunhofer AISEC unterstützt Unternehmen mit technologie- und anwendungsorientierten Sicherheitslösungen, z. B. als Open-Source-Tools, die die Umsetzung regulatorischer Anforderungen basierend auf (teil-)automatisierten Technologien erleichtern. Die am Fraunhofer AISEC entwickelten Werkzeuge unterstützen entlang der identifizierten Mindeststandards wie der Risikobewertung, dem Schwachstellenmanagement, beim Supply Chain und Policy Management und der Erklärung der Konformität. Das Fraunhofer AISEC stärkt so die Verlässlichkeit, Vertrauenswürdigkeit und Manipulationssicherheit von IT-basierten Systemen und Produkten und ermöglicht Unternehmen, Vertrauen in die Sicherheit ihrer Produkte aufzubauen. Dies ist ein entscheidender Faktor, um digitale Geschäftsmodelle nachhaltig zu stärken und Wettbewerbsvorteile auf dem deutschen und europäischen Binnenmarkt zu sichern.

Kontakt

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

Weiterführende Informationen

Spotlight »Cyber Resilience Act«

Pressemitteilung zu »CRA, NIS-2 & Co.«

Assets identifizieren, Schutz aufbauen und Konformität erreichen

Auswahl der Open-Source-Tools des Fraunhofer AISEC

RISK-ASSESSMENT

»QuBA« (Questionnaire-Based Assessment) ist eine fragebogenbasierte, schnell und einfach durchführbare Risk-Assessment-Methode zugeschnitten auf einfache Produkte mit einheitlichem Schutzbedarf. (Kontakt: Daniel Angermeier, daniel.angermeier@aisec.fraunhofer.de)

SCHWACHSTELLENMANAGEMENT

Das **Analyse-Tool »Codyze«** prüft Softwarecode automatisiert auf die Einhaltung geltender Regularien für Kommunikation, Verschlüsselung, Compliance und Zertifizierung. Dabei erkennt es potenzielle Sicherheitslücken und empfiehlt konkrete Maßnahmen zur Behebung.
(Kontakt: Chistian Banse, christian.banse@aisec.fraunhofer.de)

Der **»Clouditor«** checkt kontinuierlich die sichere Konfiguration von Cloud-Diensten auf Cloud-Plattformen. Anhand definierter Kataloge kontrolliert er Sicherheits- und Compliance-Anforderungen sowie die Datenverschlüsselung, das Zugriffsmanagement und die Datenschutzkonformität.
(Kontakt: Chistian Banse, christian.banse@aisec.fraunhofer.de)

Die **Library »kotlin-csaf«** ermöglicht das Parsen, Importieren und Validieren von CSAF-Dokumenten. Mithilfe der Bibliothek kann die Implementierung des Providers automatisiert auf ihre Korrektheit geprüft werden. (Kontakt: Chistian Banse, christian.banse@aisec.fraunhofer.de)

SUPPLY CHAIN MANAGEMENT

Das **Open-Source-Framework »Connector Measurement Component (CMC)«** erfasst alle verwendeten Softwarekomponenten und ermöglicht den Aufbau attestierter Kommunikationsnetze in heterogenen, cloud-basierten Infrastrukturen unabhängig der eingesetzten Hardware.
(Kontakt: Sascha Wessel, sascha.wessel@aisec.fraunhofer.de)

POLICY MANAGEMENT

Die **Plattform »GyroidOS«** schützt mit zahlreichen Sicherheitsfunktionen die Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Software und trägt maßgeblich zur Erfüllung der Sicherheitsanforderungen bei. Zudem unterstützt sie Zertifizierungsprozesse nach den Industriestandards DIN SPEC 27070 und IEC 62443-4-2 sowie gemäß Common Criteria.
(Kontakt: Sascha Wessel, sascha.wessel@aisec.fraunhofer.de)

ERKLÄRUNG DER KONFORMITÄT

Mit **»Confirmate«** können automatisierte Konformitätsprüfungen von Software-Komponenten erfolgen. Das Tool kombiniert statische Code-Analyse mit einer Compliance-Auswertung und überprüft die Konformität von Drittanbieter-Software anhand von Schwachstellendatenbanken.
(Kontakt: Chistian Banse, christian.banse@aisec.fraunhofer.de)

Webseite zu »Codyze«

»Clouditor« auf GitHub

»kotlin-csaf« auf GitHub

»CMC« auf GitHub

Webseite zu »GyroidOS«

Pressemitteilung zu »Confirmate«

Sichere Fernaktivierung für Werkzeugmaschinen – quantensicher und zukunftsfähig

Wie lassen sich Werkzeugmaschinen sicher aus der Ferne aktivieren? Das Projekt »PoQsiKom« hat dafür eine kryptoagile, quantensichere Technologie entwickelt, die auch zukünftigen Bedrohungen standhält. Ein speziell gesicherter Chip ermöglicht die verlässliche Überprüfung und Aktivierung von Sicherheitseinrichtungen über Landesgrenzen hinweg.

In der Industrie sind Werkzeugmaschinen in der Regel über Jahrzehnte hinweg im Einsatz, weshalb ihre Sicherheit langfristig gewährleistet sein muss. Da Quantencomputer in Zukunft in der Lage sein könnten, klassische Verschlüsselungsverfahren zu brechen, ist es essenziell, bereits heute auf quantensichere Kommunikation zwischen verschiedenen Komponenten in der Betriebstechnik umzurüsten, um sensible Produktionsdaten und Steuerungsprozesse dauerhaft zu schützen.

Der wachsende Trend zur intelligenten Fertigung führt zu einer verstärkten Kommunikation zwischen verschiedenen Komponenten in der Betriebstechnik. Da die Kommunikation zunehmend über die Grenzen der eigenen Vertrauensdomäne hinweg stattfindet, z. B. bei der internationalen Zusammenarbeit, reichen authentifizierte und gesicherte Kommunikationsverbindungen nicht mehr aus. Es ist auch erforderlich, die auf den Geräten generierten und ausgetauschten Daten auf Vertrauenswürdigkeit zu überprüfen.

Sicherheitsprimitiv gewährt Vertrauenswürdigkeit kritischer Daten

Im Projekt »PoQsiKom« (Post-Quanten-sichere Kommunikation für Industrie 4.0) wurde ein Konzept entwickelt, das das sichere Aktivieren der Schutzbereiche von Werkzeugmaschinen aus der Ferne ermöglicht. Grundlage hierfür ist ein Chip mit kryptoagiler, quantensicherer Security-Technologie, der flexibel eingesetzt werden kann und auch zukünftigen Bedrohungen standhält.

Sicherheitseinrichtungen von Werkzeugmaschinen wurden bisher über lokal, direkt verkabelte Terminals von physisch anwesenden Personen aktiviert. Der Sicherheitsbereich der Werkzeugmaschine ist durch Lichtschranken geschützt. Beim Unterbrechen der Lichtschranken, z. B. durch dritte Personen, Tiere oder Gegenstände, wird die Maschine gestoppt. Der Weiterbetrieb der Maschine ist nur nach die Aktivierung durch eine geschulte Person zulässig. Bisher musste dies durch persönliche Kontrolle vor Ort erfolgen. Im Gegensatz zur persönlichen Kontrolle gibt es beim Fernzugriff höhere Ansprüche an die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit der verwendeten Daten.

Durch die Implementierung von kryptografischen Bausteinen, auch Sicherheitsprimitive genannt, in jedem einzelnen Gerät ist die Aktivierung der Sicherheitseinrichtungen jetzt auch im Fernbetrieb über Landesgrenzen hinweg möglich. Der kryptoagile und quantensichere Security-Chip bildet den Vertrauensanker und ist bereits beim Design der Geräte integriert. Ein echtzeitfähiges und gegen Malware gehärtetes Betriebssystem verhindert Kompromittierungen der Daten während der Verarbeitung. Zudem garantiert die Sicherheitstechnologie den korrekten und unveränderten Zustand entfernter Systeme.

Forschung und Wirtschaft Hand in Hand

Im Projekt »PoQsiKom« verantwortet die TU München die FPGA-basierte Hardware-Plattform für den Vertrauensanker und zusammen mit der Siemens AG die Umsetzung der kryptografischen Post-Quanten-Algorithmen. Das Fraunhofer AISEC ist für die Absicherung des echtzeitfähigen Betriebssystems zuständig, während die Siemens AG die Entwicklung und Standardisierung der GTA API leitet. Das Hochtechnologieunternehmen TRUMPF entwickelt ein Konzept zur Freigabe von Sicherheitseinrichtungen über das Internet und setzt dies mit dem im Projekt entwickelten Vertrauensanker zur sicheren Kommunikation in einem Demonstrator um.

Kontakt

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

Weiterführende Informationen

Projekt »PoQsiKom«

Abteilung »Product Protection and Industrial Security«

Automatisierte Zertifizierung von Cloud-Diensten und -Anwendungen

Im EU-Projekt »EMERALD« entwickelt das Fraunhofer AISEC zusammen mit Partnern einen automatisierten Zertifizierungsprozess von Cloud-Diensten und -Anwendungen für Cloud-Anbieter und Auditoren und stärkt so die Akzeptanz sowie das Vertrauen in Cloud-Dienste.

Je digitaler unsere Welt wird, desto stärker wächst der Einsatz von Cloud-Diensten. Cloud-Anbieter und Auditoren stehen vor der Herausforderung, eine Vielzahl von Sicherheits-, Datenschutz- und Regulierungsanforderungen zu erfüllen bzw. zu prüfen. Standards wie das European Cybersecurity Certification Scheme for Cloud Services (EUCS) und der Cloud Computing Compliance Criteria Catalogue (C5) des Bundesamts für Sicherheit in der Informationstechnik (BSI) erfordern erhebliche Ressourcen, um die Vorgaben umzusetzen. »Cloud-Anbieter benötigen sichere und effiziente Zertifizierungsprozesse, die Nachweise automatisiert erbringen, interoperabel sind und flexibel auf unterschiedliche Anforderungen angepasst werden können«, sagt Christian Banse, Abteilungsleiter Service Application Security am Fraunhofer AISEC.

Mit »EMERALD« Zertifizierung als Service ermöglichen

Das EU-Projekt »EMERALD« (Evidence Management for Continuous Certification as a Service in the Cloud) strebt an, den Weg zu einem effizienten »Certification-as-a-Service« (CaaS) zu ebnen, der die Einhaltung der Sicherheitsanforderungen von Cloud-Diensten und -Anwendungen verlässlich überprüft und flexibel neue regulatorische Anforderungen berücksichtigt. Dafür soll das Technology Readiness Level (TRL) der im Vorgängerprojekt »MEDINA« entwickelten Technologien von TR5 (Validierung in relevanter Umgebung) auf TR7 (Prototyp in operativer Umgebung) angehoben werden.

Für Anbieter von Cloud-Diensten entwickelt »EMERALD« Prozesse, die Zertifizierungen vorbereiten, verwalten, überwachen und eine schlanke Rezertifizierung ermöglichen. Auditoren profitieren von Prozessen zur Unterstützung von Audits und einem neuen Konzept für die Benutzerinteraktion, das die Durchführung von Audits vereinheitlicht und vereinfacht. Zudem entwickelt »EMERALD« für Cybersicherheits- und Normierungs-behörden neuartige Strategien und Methoden zur Erstellung von Cybersicherheitsanforderungen und -metriken, die flexibel auf Änderungen reagieren können und interoperabel sind, um auf andere Systeme übertragen zu werden.

Security-Tools »Clouditor« und »Codyze« weiterentwickeln

Das Fraunhofer AISEC bringt in das Projekt seine bereits entwickelten Security-Werkzeuge »Clouditor« und »Codyze« ein. »Clouditor« ist ein Tool zur automatisierten Sicherheits- und Compliance-Analyse von Cloud-Infrastrukturen. Es scannt Cloud-Ressourcen, identifiziert potenzielle Sicherheitsrisiken sowie Compliance-Verstöße und gibt Empfehlungen zur Behebung dieser Probleme. Im Rahmen von »EMERALD« wird »Clouditor« weiterentwickelt, um das Gesamtsystem von Cloud-Diensten und -Anwendungen zu analysieren. »Codyze« dient der statischen Code-Analyse und überprüft automatisiert Sicherheitslücken und Schwachstellen in Software – beispielsweise die korrekte Umsetzung von Verschlüsselung oder Authentifizierung. Bereits im Vorgänger-Projekt »MEDINA« wurden Informationen über die notwendigen Nachweise für eine Zertifizierung automatisiert ermittelt. »EMERALD« will diese Erkenntnisse nun verknüpfen, um Aussagen über das Gesamtsystem von Cloud-Diensten und -Anwendungen zu erhalten.

Security-Tools für automatisiertes Monitoring von Cloud-Diensten und Software

Projekt »EMERALD«

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

Spezialteam von Forschungseinrichtungen und Universitäten

Das vom Bundesministerium für Bildung und Forschung (BMBF) unterstützte Projekt »AIgenCY« vereint unter der Federführung des Fraunhofer AISEC Spezialistinnen und Spezialisten des CISPA – Helmholtz-Zentrums für Informationssicherheit, der Technischen Universität Berlin und der Freien Universität Berlin und kooperiert mit dem Pionier-Unternehmen für KI, Aleph Alpha, aus Heidelberg.

Projekt »AIgenCY«

Abteilung »Cognitive Security Technologies«

Kontakt

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

Prof. Dr.-Ing. habil. Gerhard Wunder
Abteilungsleiter
Cognitive Security Technologies
Tel. +49 89 3229986-1067
gerhard.wunder@aisec.fraunhofer.de

Generative KI im Cyberraum – Chancen nutzen, Gefahren abwehren

Wie beeinflusst generative KI die Cybersicherheit – und wie können wir uns schützen? Das Forschungsprojekt »AIgenCY« untersucht Chancen und Risiken KI-generierter Inhalte und entwickelt Abwehrstrategien gegen neue Bedrohungen.
Unter Leitung des Fraunhofer AISEC arbeiten führende Forschungsinstitute und Unternehmen an Lösungen für eine sichere digitale Zukunft.

Mit dem Forschungsprojekt »AIgenCY – Chancen und Risiken generativer KI in der Cybersicherheit« nehmen führende Expertinnen und Experten aus Wissenschaft und Industrie die Herausforderung an, die Implikationen generativer Künstlicher Intelligenz für die Cybersicherheit zu erforschen.

Die rasant fortschreitenden Entwicklungen in der generativen KI, insbesondere in neuronalen Netzwerken, revolutionieren die Erstellung von digitalen Inhalten. Systeme sind mit generativer KI in der Lage, authentische Texte, visuelle Inhalte und komplexe Programmcodes zu generieren und zu verfeinern. Diese Fähigkeiten eröffnen neue Chancen, bergen aber auch signifikante Risiken. »AIgenCY« widmet sich daher der Aufgabe, potenzielle Bedrohungen durch KI-generierte Inhalte zu erkennen und robuste Abwehrstrategien zu entwickeln, um die digitale Souveränität Deutschlands zu festigen und kritische Infrastrukturen zu schützen – gleichzeitig soll so Deutschland als Innovationsstandort gestärkt werden.

Im Zuge des Projekts wird ein Experimentierlabor eingerichtet, das die Anwendbarkeit generativer KI-Technologien in praxisnahen Szenarien erforscht. Das Labor wird unter anderem genutzt, um Angriffsszenarien und Konzepte zur Erhöhung der Robustheit von Systemen gegen Angriffe in realistischen Szenarien untersuchen zu können.

»Mit dem Projekt ›AIgenCY‹ haben wir die Chance, die Weichen für eine sichere digitale Zukunft zu stellen und KI-Innovationen im Sinne einer resilienten Gesellschaft voranzutreiben«, betont Prof. Dr. Claudia Eckert, Institutsleiterin des Fraunhofer AISEC. »Mit einer Förderung von fünf Millionen Euro durch das BMBF über die nächsten drei Jahre ist ›AIgenCY‹ auf einem guten Weg, dieses zukunftsrelevante Forschungs- und Innovationsfeld maßgeblich mitzugestalten.«

Von Anomalieerkennung bis Watermarking

Das Forschungsteam konzentriert sich auf folgende Kernthemen:

- Malware-Bekämpfung: Analyse der Generierung fortschrittlicher Malware durch KI und Entwicklung entsprechender Gegenmaßnahmen

- Verhinderung von Social Engineering, Desinformation und betrügerischen Kampagnen: Steigerung der Wachsamkeit und Verbesserung der Erkennung automatisierter Angriffe

- Informationssammlung und -aufbereitung: Verständnis für präventive Angriffsstrategien und deren Abwehr

- Erklärbarkeit und Inferenz: Interpretation der Entscheidungsfindung generativer KI-Modelle und Identifikation systemischer Schwachstellen

- Watermarking und Anomalieerkennung: Rückverfolgung der Datenherkunft und Erkennung ungewöhnlicher Muster, die auf mögliche Angriffe hinweisen.

Vertrauenswürdige Mikroelektronik: Schlüsseltechnologie für digitale Wertschöpfung

Mikroelektronik ist eine Schlüsseltechnologie der Digitalisierung. Das Fraunhofer AISEC forscht mit Partnern an vertrauenswürdiger Mikroelektronik und fördert so die Wettbewerbsfähigkeit und technologische Souveränität.

Smartphones, industrielle Fertigung oder medizinische Diagnostik sind ohne Mikrochips undenkbar. Umso wichtiger ist es, dass Elektronik zuverlässig und vertrauenswürdig ist. Angesichts wachsender Cyberbedrohungen, denen z. B. durch EU-Regularien wie dem Cyber Resilience Act (CRA) Rechnung getragen wird, ist es für Unternehmen nötig, Produkte und Lieferketten auch auf der Hardware-Ebene abzusichern.

Initiative für vertrauenswürdige Elektronik

In Zusammenarbeit mit dem Verband der Elektrotechnik, Elektronik und Informationstechnik e.V. (VDE) und der Forschungsplattform »Velektronik« wurde 2024 die VDE-Fachgruppe »Vertrauenswürdige Elektronik« ins Leben gerufen. Sie dient als zentrale Anlaufstelle, um vertrauenswürdige Elektronik im Verbund von Industrie, Forschung und Behörden in Deutschland voranzutreiben. Ziel ist, gemeinsam das Bewusstsein für vertrauenswürdige Elektronik zu schärfen, Industriestandards mitzugestalten und neue Sicherheitsansätze zu entwickeln. Prof. Dr. Georg Sigl, Institutsleiter des Fraunhofer AISEC, fungiert als Sprecher der Initiative.

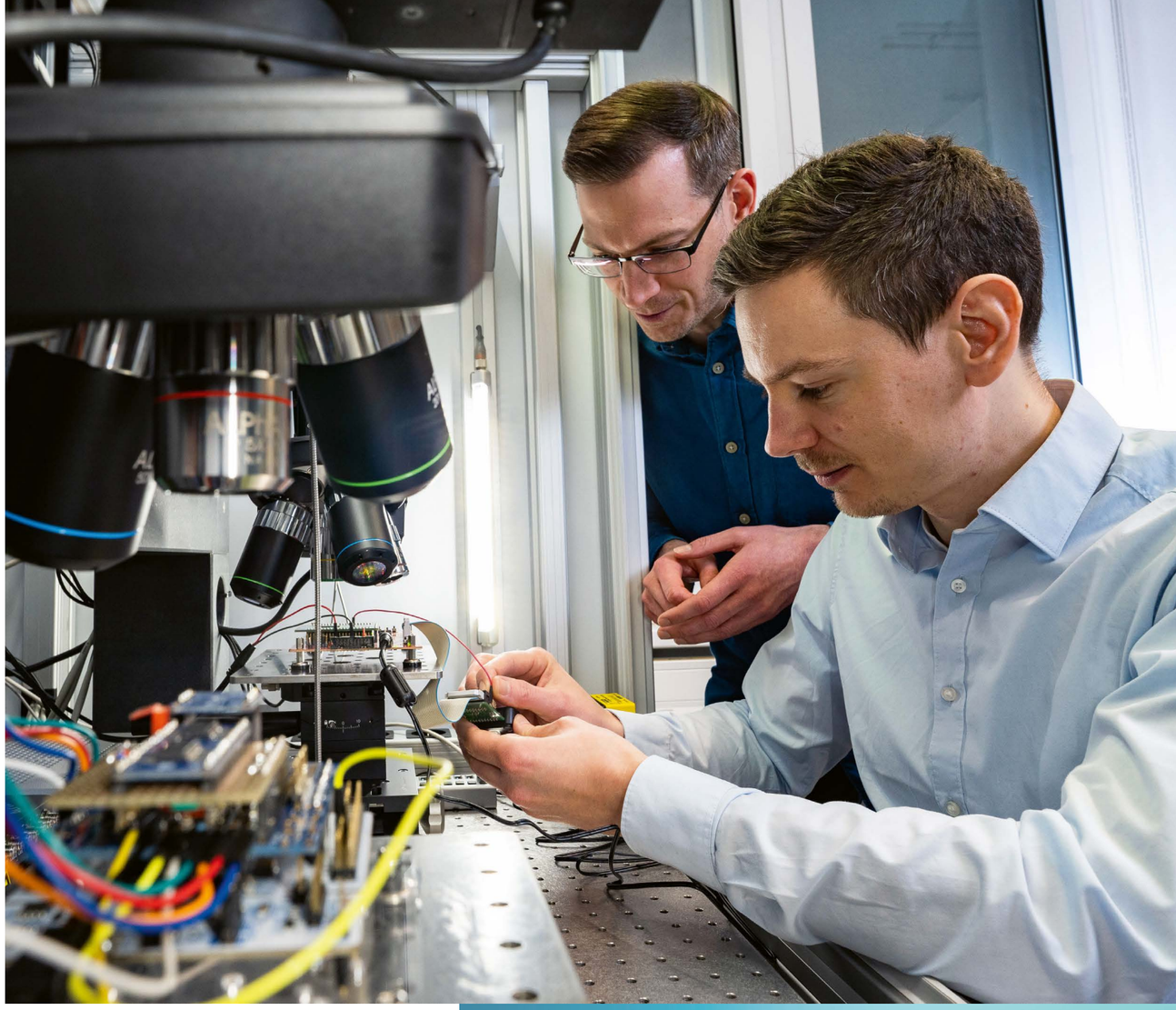
Im Zentrum steht der Informationsaustausch zu neuen Forschungserkenntnissen und Best Practices zwischen Hochschulen, Industrie, Prüflaboren und Behörden. Die Fachgruppe beobachtet gesetzliche Vorschriften wie NIS-2 und CRA, analysiert neue Sicherheitsvorfälle im Bereich der vertrauenswürdigen Elektronik und initialisiert Projekte, die zur Weiterentwicklung sicherer Elektronik beitragen.

Bayerisches Chip-Design-Center als Innovationsmotor

Ein weiteres Schlüsselprojekt zur Stärkung der Halbleiterindustrie ist das Bayerische Chip-Design-Center (BCDC), gefördert vom Bayerischen Staatsministerium für Wirtschaft, Landesentwicklung und Energie. Das BCDC soll Bayern als Innovationsstandort für Chipdesign stärken und kleinen und mittleren Unternehmen (KMU) sowie Start-ups den Zugang zur strategisch wichtigen Technologie erleichtern.

Die Forschenden am Fraunhofer AISEC entwickeln neue Sicherheitsarchitekturen für vertrauenswürdige Elektronik und gehärtete Prozessoren, die auf offenen RISC-V-Designs basieren. Durch die enge Verknüpfung von Hardware und Software werden geschützte Umgebungen geschaffen, die auf Mechanismen wie Trusted Execution Environments und Confidential Computing beruhen. Zudem sorgen verifizierte Bootvorgänge, sichere Firmware-Updates und architekturbasierte Sicherheitsmaßnahmen für einen robusten Schutz vor Angriffen auf Software-Schwachstellen.

Durch den aktiven Beitrag zur VDE-Fachgruppe und zum BCDC stärkt das Fraunhofer AISEC die Wettbewerbsfähigkeit und technologische Souveränität der bayerischen, deutschen und europäischen Halbleiterindustrie und etabliert vertrauenswürdige Elektronik als Schlüsseltechnologie für eine sichere digitale Transformation.



Kontakt

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

Fraunhofer AISEC als Netzwerkpartner zur Förderung vertrauenswürdiger Hardware

Pressemitteilung zur VDE-Fachgruppe

Pressemitteilung zum Bayerischen Chip-Design-Center (BCDC)

Pressemitteilung zum Zentrum Trusted Electronic Bayern (TrEB)

Abteilung »Hardware Security«

Vernetzte und automatisierte Fahrzeuge für das Quantenzeitalter

Um die Sicherheit von vernetzten und automatisierten Fahrzeugen langfristig zu gewährleisten, erforscht das vom BMBF geförderte Projekt »PARFAIT« den Einsatz von Post-Quanten-Kryptografie (PQC) und Krypto-Agilität. Das Fraunhofer AISEC erforscht dabei Sicherheitsstrategien für Fahrzeugkomponenten, analysiert Schwachstellen und optimiert Verschlüsselungsverfahren.

Die zunehmende Vernetzung und Automatisierung von Fahrzeugen erhöht das Risiko von Cyberangriffen. Zudem könnten künftige Quantencomputer heutige Verschlüsselungen brechen. Deshalb fordert die UNECE-Richtlinie R155 seit 2022 ein langfristiges Sicherheitskonzept für Fahrzeugzulassungen. Um diese Vorgaben zu erfüllen, müssen Post-Quanten-Kryptografie (PQC) und Krypto-Agilität frühzeitig in die Entwicklung digitaler und elektronischer Fahrzeugkomponenten einfließen.

Ziel des vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Projekts »Post-Quanten-Kryptografie für Automotive-Komponenten (PARFAIT)« ist es deshalb, sichere Verfahren und Methoden für den Einsatz der Post-Quanten-Kryptografie und Krypto-Agilität für den Automobilbereich zu erforschen. Das Fraunhofer AISEC ist einer der Cybersecurity-Partner unter den acht beteiligten Einrichtungen aus Wirtschaft und Wissenschaft.

Sicherheitsstrategien für Fahrzeugkomponenten, Schwachstellenanalyse und optimierte Verschlüsselungsverfahren

Das Fraunhofer AISEC hilft, kryptografische Sicherheitsziele für Fahrzeuge zu identifizieren, etwa für Secure Boot, Updates und Diagnosen, die mit PQC abgesichert werden sollen. Zudem analysiert es »store now, decrypt later«-Szenarien zur Umsetzung eines Angreifendenmodells als Grundlage für spätere Sicherheitslösungen.

Das Fraunhofer AISEC bewertet aktuelle Technologien und ordnet sie passenden Anwendungsfällen zu. Es prüft, welche Verfahren sich für eine sichere Migration eignen und entwickelt Migrationsstrategien für verschiedene Fahrzeugarchitekturen. Dabei berücksichtigt es Systemanforderungen und den Wechsel von klassischen zu PQC-basierten Lösungen.

Die Forschenden des Fraunhofer AISEC analysieren die PQC-Algorithmen aus den NIST-Wettbewerben hinsichtlich Performance und Speicherbedarf. Sie erweitern die PQDB-Datenbank um Low-End-Devices und Automotive-Mikrocontroller, sodass passende Algorithmen für Steuergeräte ausgewählt werden können. Das Fraunhofer AISEC erweitert Protokolle aus dem Automobilumfeld um PQC und prüft Schwächen bestehender Verfahren und Protokolle. Es untersucht Hybridisierungsstrategien, um PQC in bestehende Systeme zu integrieren, und bewertet die besten Lösungen für Performance, Sicherheit und Kompatibilität. Zudem analysiert es die Eignung moderner kryptografischer Ansätze wie Proxy Re-Encryption für den Einsatz im Automobilbereich.

Glossar

Krypto-Agilität *bezeichnet die Fähigkeit von IT-Systemen, kryptografische Algorithmen und Protokolle flexibel auszutauschen.*

Proxy Re-Encryption (PRE) *ist eine kryptografische Technik, die es ermöglicht, verschlüsselte Daten von einem Sender an einen Empfänger weiterzugeben, ohne dass der Vermittler (Proxy) den Klartext der Daten kennt*

Starker Verbund für die Zukunftsfähigkeit der Automobilbranche

Die Verbundpartner von PARFAIT sind: DENSO AUTOMOTIVE Deutschland GmbH, Fraunhofer AISEC, Freie Universität Berlin, Hochschule Darmstadt, Hochschule RheinMain, Infineon Technologies AG, Technische Universität Darmstadt und Vitesco Technologies Germany GmbH.

Projekt »PARFAIT«

Kontakt

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

Weiterführende Informationen

Kompetenzzentrum Post-Quanten-Kryptografie

Gemeinsam für sichere, nutzerfreundliche und universell einsetzbare digitale Identitäten

Zur Umsetzung der novellierten eIDAS-Verordnung in Deutschland hat das Bundesministerium des Inneren und für Heimat (BMI) die SPRIND GmbH beauftragt, ein Konzept für das EUDI-Wallet-Ökosystem in Deutschland sowie die staatliche EUDI-Wallet zu entwickeln. BMI und SPRIND setzen dieses Vorhaben gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesdruckerei, PwC und Fraunhofer AISEC um.

Kontakt

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

Weiterführende Informationen

Pressemitteilung des BMI zu EUDI-Wallets

Abteilung »Secure Systems Engineering«

Cybersecurity-Expertise für die digitale EUDI-Wallet in Deutschland

Einfach nutzbare und sichere elektronische Identitäten (eID) sind essenzielle Bausteine für den Zugang zu digitalen Diensten. Ab 2027 sollen EUDI-Wallets ein vertrauenswürdiges, europaweit interoperables Ökosystem für digitale Identitäten und Nachweise schaffen. Das Fraunhofer AISEC ist Cybersecurity-Partner.

Laut der im Mai 2024 in Kraft getretenen novellierten eIDAS-Verordnung müssen alle EU-Mitgliedstaaten bis Ende 2026 mindestens eine europäische Brieftasche für digitale Identitäten (EUDI-Wallet) zertifizieren und bereitstellen. Sie ermöglicht es Nutzerinnen und Nutzern, sich per Smartphone auszuweisen, eine Vielzahl von Dokumenten als Identitätsnachweise zu speichern, Transaktionen zu autorisieren und mit der qualifizierten elektronischen Signatur (QES) zu unterschreiben – ohne zusätzliche Hardware. Der Online-Ausweis ist die Grundlage für die Übertragung der Personenidentifizierungsdaten in die Wallet. Dabei unterstützt die Wallet auch das pseudonyme Authentisieren gegenüber allen Diensten, für die eine Identifizierung einer natürlichen Person nicht notwendig ist. Auch nicht-staatliche Anbieter wie Unternehmen oder Forschungseinrichtungen werden die Möglichkeit haben, eigene EUDI-Wallets anerkennen zu lassen.

Bei der Entwicklung der EUDI-Wallet wird besonderer Wert auf Akzeptanz und Nutzerfreundlichkeit gelegt. Die zukünftigen Benutzeroberflächen werden intuitiv gestaltet und alle Funktionen sollen leicht zugänglich sein, um eine hohe Zufriedenheit und Verbreitung bei den Nutzerinnen und Nutzern zu gewährleisten. Durch ausführlichen Input im Rahmen des transparenten Konsultationsprozesses wird kontinuierlich an Verbesserungen gearbeitet, um ein reibungsloses Nutzungserlebnis zu garantieren. Durch den Fokus auf die User Experience schafft das Projekt wichtige Grundlagen für die breite Akzeptanz in der Bevölkerung und somit für vollständig digitale und effiziente Prozesse in Gesellschaft, Wirtschaft und Verwaltung.

Fokus auf Sicherheit

Für die Identifizierungsfunktion der Wallet wurden verschiedene Architekturoptionen beschrieben und hinsichtlich Informationssicherheit, Privatheit, Nutzbarkeit und Skalierbarkeit verglichen. Nach intensiver Prüfung wurde für die Umsetzung der staatlichen Wallet die Architektur-Variante gewählt, welche mit den bereits heute bei den Bürgerinnen und Bürgern verfügbaren Smartphones funktioniert. Sie kombiniert Hardware-Sicherheitsanker in der Cloud mit signierten Daten und ermöglicht es so, Schlüssel mit dem höchsten Schutzbedarf in sicherer Hardware zu speichern und damit das Risiko der Beobachtbarkeit von Transaktionen zu minimieren.

Das Fraunhofer AISEC ist Cybersecurity-Partner und unterstützt das Projekt mit Expertise im Design sicherer Architekturen von elektronischen Identitäten, bei der Risikoanalyse, beim Thema Usable Security and Privacy (Cybersecurity, bei deren Entwicklung die Nutzenden von Anfang an intensiv mit eingebunden werden) und Mobile Security.

Die Entwicklung der staatlichen Wallet erfolgt in einem transparenten und öffentlichen Konsultationsprozess mit allen Stakeholdern und der Öffentlichkeit. Der Rollout soll schrittweise mit erweitertem Funktionsumfang bis 2027 erfolgen. Die EUDI-Wallet gilt als größtes digitalpolitisches Projekt der EU, mit dem Ziel, bis 2030 mindestens 80 Prozent der EU-Bürgerinnen und -Bürger mit einer digitalen Identität auszustatten.

Wissenstransfer aus der Forschung in die Praxis

Das Lernlabor Cybersicherheit ist ein Verbund aus acht Fraunhofer-Instituten und zehn Fachhochschulen. Als Teil der Weiterbildungseinrichtung Fraunhofer Academy unterstützt es Unternehmen sowie Behörden beim gezielten Aufbau von Kompetenzen in der IT-Sicherheit.

Lernlabor
Cybersicherheit

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

Wissen schafft Sicherheit

Angriffe frühzeitig bemerken, handlungsfähig bleiben und schnell zum Normalbetrieb zurückkehren – Cyberresilienz ist angesichts der steigenden Zahl an Angriffen und gesetzlichen Standards unverzichtbar. Wer sich nicht auskennt, riskiert erhebliche Schäden. Das Fraunhofer AISEC unterstützt im Lernlabor Cybersicherheit mit aktuellem Forschungswissen.

Check der eigenen Cyberresilienz

Der erste Schritt zur Widerstandsfähigkeit gegen Cyberbedrohungen ist eine Standortbestimmung:

- Nutzt Ihr Unternehmen Schutzmechanismen zur Datenübertragung und -speicherung?
- Wird Ihr Netzwerk kontinuierlich auf Angriffe überwacht?
- Existieren Notfallpläne, um den Geschäftsbetrieb im Ernstfall aufrechtzuerhalten?
- Werden regelmäßig Backups durchgeführt?

Mit dem Online-Fragebogen des Lernlabor Cybersicherheit erhalten Organisationen ein erstes Feedback, wo sie in Sachen Cyberresilienz stehen. Spezifischer Handlungsbedarf wird im persönlichen Workshop erarbeitet – abgestimmt auf Branche, Geschäftsmodell und Regulatorik. Eine Einheitslösung gibt es nicht: Während Einrichtungen der kritischen Infrastruktur wie Stromversorger trotz eines Cyberangriffs handlungsfähig bleiben müssen, liegt der Fokus für Automobilzulieferer auf einer schnellen Wiederherstellung des Normalbetriebs nach einem Angriff.

Direkter Zugang zu anwendungsorientiertem Forschungswissen

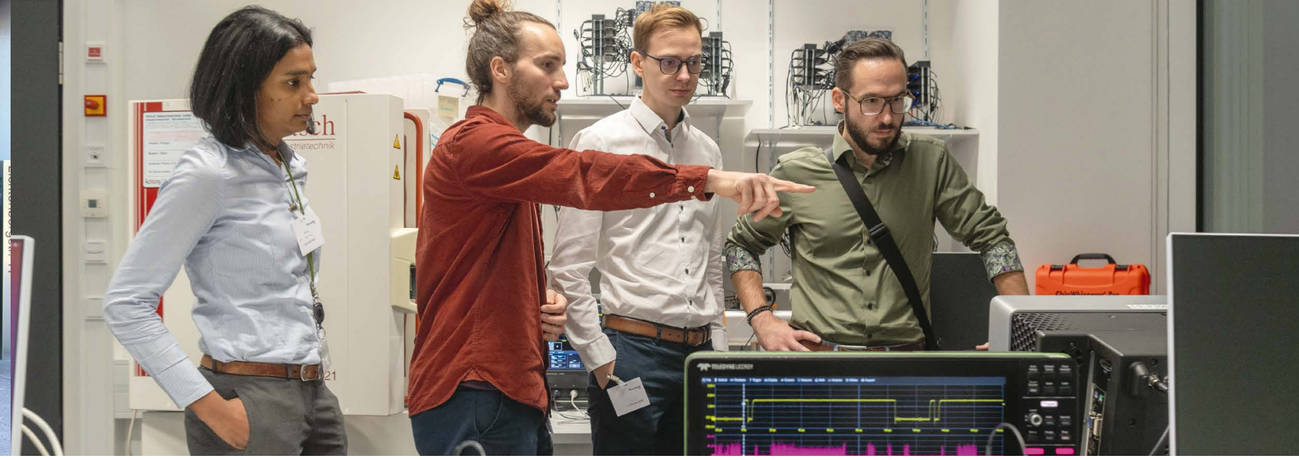
Abhängig vom individuellen Bedarf schulen die Trainerinnen und Trainer des Fraunhofer AISEC im Lernlabor Cybersicherheit gezielt die Kompetenzen, die die Organisation benötigt. Ob für Product Owner, Softwareentwickler*innen oder IT-Sicherheitsbeauftragte: Maßgeschneiderte Inhouse-Schulungen integrieren sich nahtlos in den Arbeitsalltag und befähigen die Teilnehmenden, Maßnahmen direkt umzusetzen.

Von der Wissenschaft in die Praxis

Zwei Praxisbeispiele zeigen, wie Wissenschaftler ihr Fachwissen weitergeben:

- **Dr. Nicolas Müller** vermittelt, wie Machine-Learning-Modelle widerstandsfähiger gegenüber Angriffen, Manipulation und Datenlecks gemacht werden. Mit diesem Wissen können z. B. Banken und Zahlungsdienstleister ihre KI-Modelle so absichern, dass verdächtige Transaktionen zuverlässig erkannt werden – ohne dass Betrüger das System überlisten können.
- **Albert Stark** zeigt Methoden, eingebettete Systeme so zu gestalten, dass selbst im Falle eines Angriffs grundlegende Funktionalitäten z. B. in Industrieanlagen weiterlaufen. Ein solcher Minimalbetrieb ist z. B. bei Windrädern, Ölraffinerien oder Hochöfen entscheidend, deren Betrieb schwer oder teuer zu stoppen ist.

»Die Stärke unserer Trainings liegt in der verständlichen und praxisnahen Aufbereitung hochspezialisierter Themen«, erklärt Vivija Čeprkalo-Simić, Projektleiterin des Lernlabor Cybersicherheit am Fraunhofer AISEC. »Für Advanced Machine Learning oder Post-Quanten-Kryptografie kommen Unternehmen gezielt zu uns, denn Trainings in dieser Fachtiefe gibt es sonst nirgendwo.« Wer strategisch in dieses Know-how investiert, schützt nicht nur seine Systeme und Daten, sondern wappnet sich auch für neue Herausforderungen.



3. Netzwerkevent »PQC-Update«: Migrate now to be secure later

Zur Pressemitteilung

Beim 3. PQC-Update des Fraunhofer AISEC hat sich die deutschsprachige PQC-Community am 13. und 14. Mai 2024 über den aktuellen Entwicklungsstand der Post-Quanten-Kryptografie (PQC) ausgetauscht. Mehr als 100 Expertinnen und Experten aus Behörden, Unternehmen, Hochschulen und Forschungseinrichtungen, die am jährlichen Netzwerktreffen des Kompetenzzentrums Post-Quanten-Kryptografie teilgenommen haben, waren sich einig: Der Einsatz von leistungsstarken Quantencomputern ist nur eine Frage der Zeit. Deshalb müsse aufgrund der massiven Konsequenzen sofort gehandelt und auf quantensichere Verschlüsselungsverfahren migriert werden. Gleichzeitig müssen PQC-Algorithmen selbst weiter verbessert werden, was einige der Vorträge anschaulich zeigten. PQC müsse zudem noch viel agiler, intensiver und schneller umgesetzt werden als bisher, um der drohenden Gefahr zu begegnen. Denn das Damokles-Schwert »Store now and decrypt later« schwebt über allem.

1. Nachhaltigkeitswettbewerb: Auf dem Weg zum klimaneutralen Institut

Bis 2045 will das Fraunhofer AISEC klimaneutral sein. Zu unserer Klimaschutzstrategie tragen zahlreiche Maßnahmen bei. Beispielsweise zahlen der Bezug von 100 Prozent grünen Stroms, die Bezuschussung des ÖPNV-Tickets und eigene Ladesäulen vor dem Institutsgebäude auf dieses Ziel ein. Seit 2023 engagieren sich Mitarbeitende im AISEC-Zero-CO_2-Club für klimaschützende Initiativen und sensibilisieren die Belegschaft mit Aktionen. Im Sommer 2024 fand erstmalig ein Nachhaltigkeitswettbewerb am Fraunhofer AISEC statt, bei dem Ideen für die Reduktion von CO_2 gesucht wurden. Die Vorschläge zur Vermeidung vorschneller Entsorgung funktionsfähiger IT- und Elektrogeräte für Testaufbauten im Labor, zur Systematisierung von Labor-Lagerbestand sowie zur Durchführung von nachhaltigen Events mit Fokus auf vegetarischer und veganer Bewirtung und Müllreduktion wurden prämiert. Zusammen mit zahlreichen weiteren Einreichungen werden diese Vorschläge sukzessiv umgesetzt, um anerkannte Nachhaltigkeitsstandards zu erfüllen und die CO_2-Emissionen des Fraunhofer AISEC dauerhaft zu senken.

Cybersicherheitstag mit Fokus auf CRA, NIS-2 & Co.

Zur Pressemitteilung

Die neuen EU-Regularien zur Cybersicherheit setzen die digitalisierte und vernetzte Wirtschaft unter Handlungsdruck: Die NIS-2-Richtlinie und der Cyber Resilience Act (CRA) verpflichten Unternehmen, für ein ausreichend hohes Sicherheitsniveau zu sorgen. Angesichts der Vielzahl der Sicherheitsanforderungen, die es nachweislich effektiv zu erfüllen gilt, stellt dies oft eine Herausforderung dar.

Auf dem 2. Cybersicherheitstag gaben Wissenschaflerinnen und Wissenschafler des Fraunhofer AISEC den rund 80 Teilnehmenden aus Industrie und Wirtschaft einen Einblick, welche Gemeinsamkeiten sich in den Regelwerken identifizieren lassen, wie daraus Mindeststandards zu entwickeln sowie (teil-)automatisierte Lösungen einzusetzen sind. Die Umsetzung von Mindesstandards lohnt auch, um ein angemessenes Sicherheitsniveau aufzubauen und gleichzeitig Marktzugänge zu sichern.

Schutz vor Cyberangriffen gewinnt an Bedeutung

Zur Pressemitteilung

Laut der vom Fraunhofer AISEC erstellten Studie für den VDMA »Industrial Security und Produktpiraterie 2024« gewinnt der Schutz vor Cyberangriffen für Unternehmen im Maschinen- und Anlagenbau immer mehr an Bedeutung. Gleichzeitig ist die Bekämpfung von Produkt- und Markenpiraterie enorm wichtig. Knapp ein Viertel der befragten Unternehmen war in den letzten zwei Jahren von signifikanten Cybersicherheitsvorfällen betroffen. Die Unternehmen reagieren auf diese Bedrohung: 96 Prozent der befragten Firmen gaben an, ihre Betriebsstätte mit mindestens einer Cybersicherheits-Maßnahme abzusichern. Hinsichtlich der Richtlinie NIS-2 für den cybersicheren Betrieb von Informationssystemen glauben 24 Prozent der Unternehmen, nicht von der Richtlinie betroffen zu sein – jedoch ergab eine VDMA-Analyse, dass rund 90 Prozent es tatsächlich sind.

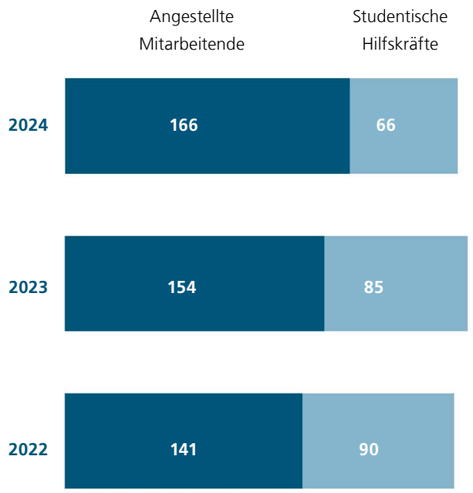
An der Studie haben sich gut 100 VDMA-Mitglieder beteiligt.

Unsere Mission:
Cybersicherheit bewerten, gestalten und bewahren

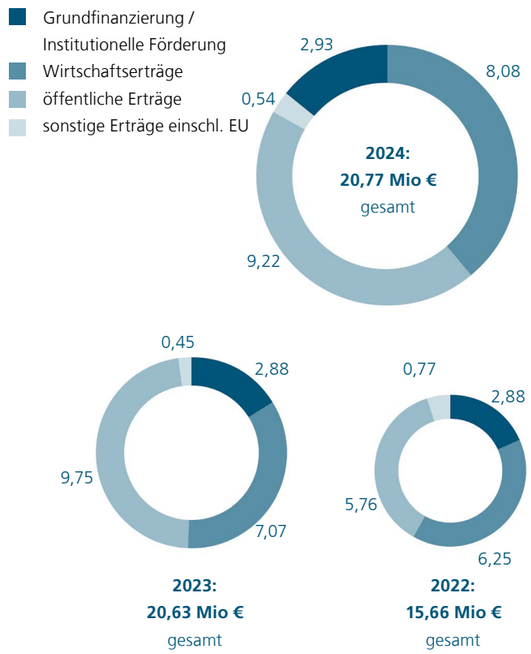
Das Fraunhofer AISEC überführt exzellente IT-Sicherheitsforschung in anwendungsorientierte Lösungen für mehr Verlässlichkeit, Vertrauenswürdigkeit und Manipulationssicherheit von IT-basierten Systemen und Produkten.

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

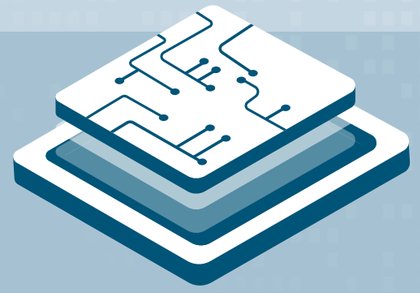
Anwendung kryptografischer Verfahren, sichere Netzprotokolle

PRODUCT PROTECTION AND INDUSTRIAL SECURITY

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

HARDWARE SECURITY

Vertrauenswürdige Elektronik und sichere eingebettete Systeme



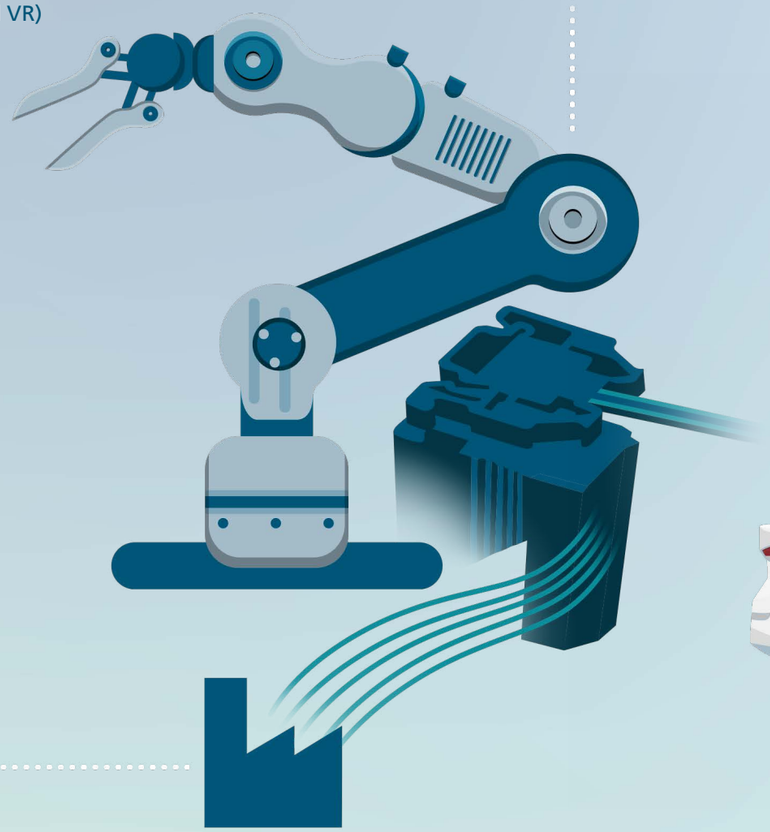
Laborlandschaft am Fraunhofer AISEC

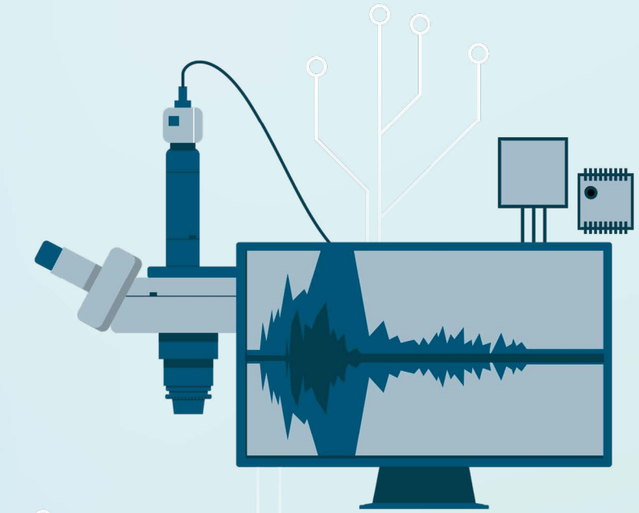
Maßgeschneiderte Lösungen, beruhend auf exzellenter Forschung

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)

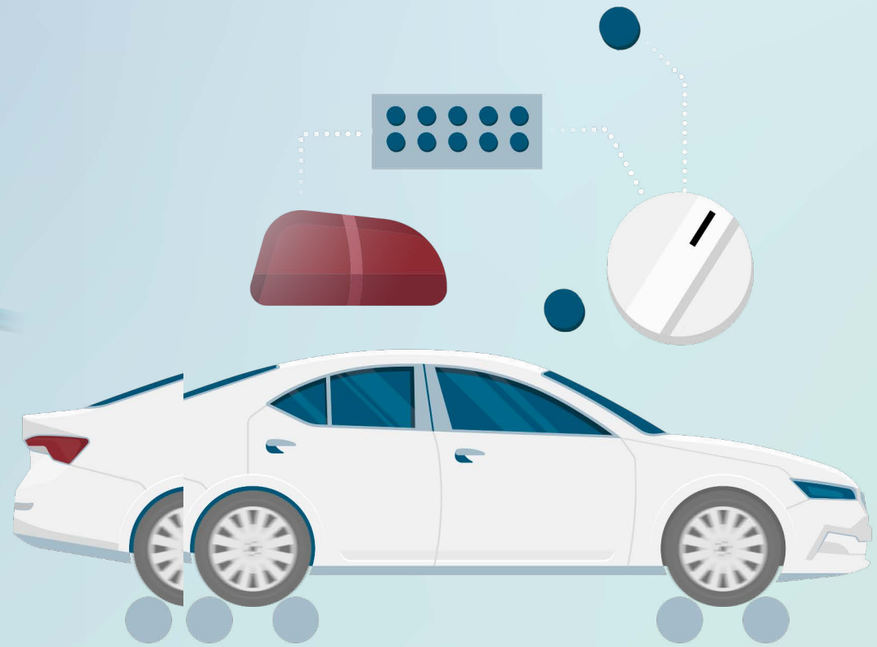




HARDWARE SECURITY LAB

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 EAL-Stufe 7 (Evaluation Assurance Level)



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

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
Verwaltungsrätin, XXtalents Jobbörse by LEADING WOMEN

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

Fraunhofer CCIT: Forschung für das Edge-Cloud-Continuum

Im Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT arbeitet die Fraunhofer-Gesellschaft an kognitiven Internet-Technologien entlang der gesamten Datenverarbeitungskette. Dazu bündelt der Fraunhofer CCIT die Kompetenzen von unterschiedlichen Fraunhofer-Instituten aus der Mikroelektronik, der Informations- und Kommunikationstechnik und der Produktion. Die gemeinsamen Forschungs- und Entwicklungsarbeiten konzentrieren sich auf Technologielösungen im Bereich Edge-Cloud-Continuum.

Edge Cloud Continuum for Production (ECC4P)

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

Edge Cloud Continuum for Production: Effizienz durch KI-gestütztes Datenmonitoring

Angesichts steigender Anforderungen an Effizienz, Ressourcen und Produktionssicherheit steht die industrielle Fertigung vor großen Herausforderungen: Sie muss Qualitätsschwankungen minimieren, Ausschuss reduzieren und Maschinen optimal auslasten. Produktionsanlagen liefern bereits wertvolle Messwerte dafür, doch deren Erfassung, sichere Verarbeitung und Nutzung erfordern leistungsfähige Infrastrukturen.

Mit Edge Cloud Continuum for Production (ECC4P) entwickelt der Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT eine Lösung, die genau hier ansetzt: Produktionsprozesse wie Fräsen, Bohren oder Wälzschleifen werden mit durchgängigem Monitoring und durch intelligente Datenverarbeitung optimiert – vom Sensor bis zur Cloud. Dabei bündelt ECC4P die Expertise der Fraunhofer-Institute IWU, IIS, ISST, IAIS und AISEC zu Sensorik, KI-gestützter Datenanalyse, sicheren Datenräumen und Edge-Cloud-Architekturen.

Vom Sensor in die Cloud und zurück

ECC4P kombiniert die Vorteile der lokalen Datenverarbeitung an der Maschine (Edge Computing) mit der skalierbaren Rechenleistung der Cloud. Kritische Abweichungen wie Vibration oder Temperaturanstieg erkennt die Edge sofort und Maschinen reagieren automatisch. Gleichzeitig analysiert die Cloud große Datenmengen aus verschiedenen Maschinenstandorten KI-gestützt, um Verschleißmuster zu identifizieren und Wartungsintervalle zu optimieren. So lassen sich ungeplante Stillstände vermeiden und Werkzeuge länger nutzen.

»ECC4P bietet dem produzierenden Gewerbe im Maschinenbau eine wissenschaftlich fundierte, praxisnahe Lösung zur effizienteren, flexibleren und sicheren Fertigung. Die intelligente Verbindung von Edge- und Cloud-Technologien schafft neue Möglichkeiten zur Optimierung, Automatisierung und Qualitätssicherung«, erklärt Michael Fritz, Leiter der Geschäftsstelle Fraunhofer CCIT.

Das Fraunhofer AISEC als Sprecher-Institut des Fraunhofer CCIT bringt seine Expertise in der automatisierten Sicherheitsprüfung von ECC4P ein. So werden die Edge- und Cloudinfrastrukturen kontinuierlich und automatisiert analysiert, um Schwachstellen zu identifizieren und aktuelle Sicherheitsstandards einzuhalten.

Modulare Infrastruktur für die Produktion der Zukunft

ECC4P ist als modulares Baukastensystem konzipiert und lässt sich flexibel in bestehende Produktionsumgebungen integrieren. Wesentliche Bestandteile sind:

- **Smart-Sensoren** für spezifische Fertigungsprozesse: smartGRIND (Schleifen), smartTOOL (Fräsen, Bohren), smartNOTCH (Metallumformung)
- **Software-Infrastruktur der Edge** für echtzeitfähige Erfassung und Synchronisierung hochfrequenter Messsignale
- **LinkedFactory**: flexible Datenarchitektur zur Verwaltung von produkt-, prozess- und maschinenbezogenen Informationen
- **Anwendungsspezifische KI-Algorithmen** zur prozessparallelen Datenauswertung
- **Eclipse-Dataspace-Konnektoren (EDC)** für einen einfachen, sicheren und souveränen Datentransfer
- **MLOps-Pipeline** zur kontinuierlichen Optimierung anwendungsspezifischer KI-Modelle
- **Automatisierte Prüfungen von Security-Compliance-Regeln** für Edge und Cloud

Stephan Klein

Geschäftsführer bei Governikus GmbH & Co. KG

Welche Rolle spielt die Governikus im Kontext der Verwaltungsdigitalisierung?

Governikus ist an vielen Stellen vertreten, meist als Softwarelieferant für Infrastrukturen und Basisangebote. So entwickeln wir z. B. vier der 15 Produkte des IT-Planungsrates oder wirken wesentlich daran mit. Mit der AusweisApp, die wir im Auftrag des Bundes entwickeln, stellen wir Bürgerinnen und Bürgern eine App zur Verfügung, die jährlich millionenfach genutzt wird. Eins haben alle Entwicklungen gemeinsam: Das Thema benutzbare Sicherheit spielt eine große Rolle.

Bei welchen Themen haben Sie auf die Kompetenz des Fraunhofer AISEC zurückgegriffen?

Hier möchte ich den Aspekt »benutzbare Sicherheit« hervorheben. Schon zu Beginn der Entwicklung der AusweisApp haben wir uns entschieden, das Thema Usability und User Experience systematisch in den Prozess zu integrieren. Hier konnte das Fraunhofer AISEC optimal unterstützen. Benutzbare Sicherheit (Usable Security) als ein entscheidender Faktor für den Schutz digitaler Anwendungen traf genau auf die Bedürfnisse, die wir bei der Entwicklung der AusweisApp identifiziert hatten. Um die Akzeptanz der Nutzenden zu erhalten, hatten wir besondere Ansprüche an die Verständlichkeit und Praktikabilität. Diese erfüllt das Fraunhofer AISEC durch interdisziplinäre Ansätze. Die Erkenntnisse aus der Psychologie, Mensch-Computer-Interaktion und IT-Sicherheit werden kombiniert und ganzheitlich betrachtet. Inzwischen nutzen mehrere Millionen Bürgerinnen und Bürger die AusweisApp. Mindestens alle zwei Sekunden findet ein Identifizierungsvorgang statt: Dies trägt und wird fortgeführt.

Das zweite größere Thema unserer Zusammenarbeit betrifft das einheitliche Unternehmenskonto. Governikus entwickelt das erweiterte Postfach des Unternehmenskontos (»OZG-PLUS-Postfach«). Hier standen wir vor der Herausforderung, kryptografisch abgesicherte Kommunikation zwischen Verwaltung und Organisationen umzusetzen, die jeweils durch Gruppen von Menschen repräsentiert werden können. Im Austausch mit dem Fraunhofer AISEC haben wir eine Lösung auf Basis der sogenannten Proxy Re-Encryption umgesetzt, die jetzt dazu genutzt werden kann, Ende-zu-Ende Verschlüsselung auch zwischen Gruppen von Menschen umzusetzen.

Was sind die entscheidenden Gründe für die Zusammenarbeit mit dem Fraunhofer AISEC?

Die Zusammenarbeit mit dem Fraunhofer AISEC ist vor allem durch die engagierte und inspirierende Art der Kolleginnen und Kollegen geprägt. Lösungen werden gemeinsam erarbeitet, in Frage gestellt und verbessert. Das ist ein kontinuierlicher Prozess, der besonders gut zu der Produktentwicklung passt, wie Governikus sie umsetzt. Das Fraunhofer AISEC verfügt über ausgeprägte Expertise im Bereich Kryptografie, Security und benutzbare Sicherheit, die in der Zusammenarbeit auf praktische Fragestellungen treffen. Neben der Implementierung moderner kryptografischer Verfahren zählen auch Pflege der entstandenen Bibliotheken sowie Prüfungen, Beratungen und Bewertungen im Hinblick auf die Anforderungen zur Sicherheit, Benutzbarkeit und Vertraulichkeit dazu.

Ingo Münch

Cybersecurity Specialist, SICK AG

Herr Münch, bitte stellen Sie die SICK AG kurz vor. Welche Relevanz haben die neuen EU-Regularien wie die NIS-2-Richtlinie und der Cyber Resilience Act (CRA) für Ihr Unternehmen?

Die SICK AG entwickelt Automatisierungs- und Sensorlösungen für Kunden auf der ganzen Welt. Am Firmensitz in Waldkirch, nördlich von Freiburg im Breisgau, und in unseren insgesamt 60 Tochtergesellschaften und Beteiligungen beschäftigen wir mehr als 12.000 Menschen weltweit. Im Geschäftsjahr 2023 betrug der Umsatz 2,3 Milliarden Euro. Mehr als tausend Lösungen sind im SICK-Portfolio direkt vom CRA betroffen. Industrielle Cybersicherheit spielt bei uns grundsätzlich eine wichtige Rolle und die Risikoanalyse mit der »QuBA« ist ein wesentliches Element im SICK Security Development Lifecycle.

Sie haben »QuBA« 2024 auf dem Cybersicherheitstag des Fraunhofer AISEC vorgestellt. Bitte beschreiben Sie die Methode und ihre Funktionsweise kurz.

Die »QuBA« ermöglicht eine schnelle und einfache Bewertung des Risikolevels von Einzelkomponenten und Sensorprodukten im Kontext ihrer spezifischen Anwendung. Der Risikostatus von weniger komplexen Produkten mit einheitlichem Schutzbedarf lässt sich so anhand eines Excel-basierten Fragebogens schnell in ein bis zwei Stunden ermitteln. Der Fragebogen enthält ca. 30-40 gezielte Fragen zur Risikoermittlung, basierend auf standardisierten Bedrohungsszenarien und Angriffspfaden. Das schlanke, standardisierte Modell beinhaltet den kompletten Katalog unserer SICK Baseline Security Requirements, die an die technischen Sicherheitsanforderungen der IEC62443-4-2 angelehnt sind, und unterstützt damit auch gleich die Risikominimierung. Die »QuBA« ist ein umfassendes Tool, das sich einfach an Änderungen der Anforderungslage anpassen lässt.

Welchen Mehrwert hat die Methode für SICK?

Auch SICK-Produkte müssen die Vorgaben der neuen EU-Regularien erfüllen. Beispielsweise ist die Einhaltung der Anforderungen aus dem CRA Voraussetzung für die Erklärung der Konformität zur CE-Kennzeichnung. Die »QuBA« ermöglicht es uns, alle relevanten Geräteeigenschaften und Anwendungsdetails unserer Produkte zu analysieren und daraufhin zu prüfen, ob die neuen Anforderungen erfüllt werden bzw. was noch zu tun ist, um diese zu erfüllen. Konkret erzeugt die »QuBA« eine Liste von notwendigen und möglichen Maßnahmen zur Risikominderung, die wir dann gemeinsam mit unseren Produktmanagern begutachten und erforderliche Maßnahmen auswählen. Die »QuBA« bietet so einen einheitlichen Weg für das CRA-konforme Risiko-Profiling für alle Produktgruppen. Mit etwas Training und ersten Erfahrungen kann sie auch rasch von Dritten durchgeführt werden.

Welche Hürden gibt es noch zu überwinden und wie geht es 2025 weiter mit »QuBA«?

Die Diversität des SICK-Produktportfolios und die individuellen Anwendungsfälle erzeugen über tausend anstehende Risiko-Assessments im SICK-Konzern. Individuelle Assessments kosten auch viel Zeit. An diesen Punkten optimieren wir gerade.

SICK steht im Austausch mit Zertifizierungsstellen bezüglich einer Zertifizierung der »QuBA« als für den CRA geeignetes Instrument für den Teil des Risko-Profilings und verfolgt die Idee, die »QuBA« zukünftig für die allgemeine Nutzung im Rahmen einer Open-Source-Lizensierung zur Verfügung zu stellen.

Fraunhofer AISEC – A great place to work

Zehn Gründe am Fraunhofer AISEC zu arbeiten

Die Vielfalt der Cybersicherheitsforschung in abwechslungsreichen Projekten und unterschiedlichen Anwendungsfeldern erfahren.

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

Im Team Herausforderungen angehen und gemeinsam technologische und gesellschaftliche Innovationen fördern.

Bewahren und Schaffen von IT-Sicherheit durch das Finden und Beheben von Schwachstellen.

In modern ausgestatteten Cybersicherheitslaboren forschen.

Neueste Forschungsergebnisse und IT-Lösungen in die Praxis bringen.

Praktisch arbeiten und gleichzeitig im gewünschten Themenfeld promovieren.

Know-how aufbauen, eigene Ideen einbringen und damit die Forschung und Industrie vorantreiben.

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

Den Stand der Cybersicherheit mit wissenschaftlicher Exzellenz in hohem Tempo weiterentwickeln.

Auszeichnungen der Fraunhofer-Gesellschaft als Arbeitgeber

YOUNG PROFESSIONAL Most Attractive EMPLOYERS GERMANY universum 2024

STUDENT Most Attractive EMPLOYERS GERMANY universum 2024

2. PLATZ
Attraktivste Arbeitgeber 2024
Für Akademiker_innen
Forschung / Ingenieurwissenschaften
trendence

2. PLATZ
Attraktivste Arbeitgeber 2024
Für Studierende
Forschung / Informatik
trendence

Johanna Baehr

Wissenschaftliche Mitarbeiterin in der Abteilung »Hardware Security«

»Beim Reverse Engineering identifiziere ich aus sieben Millionen Logikgattern eines Chips die funktionalen Einheiten und verstehe so das gesamte Chip-Design – ein Gefühl, als würde die Sonne durch die Wolken brechen.«

Das Außergewöhnliche ist für Johanna Baehr schon immer ein Teil des Alltags. Ihre Kindheit in Australien, geprägt von den Forschungsarbeiten ihrer Mutter – einer Biologin, die Insekten und Spinnen entdeckte und nach ihrer Tochter benannte – weckte früh forschende Neugierde und Spaß an gelebter Wissenschaft in Baehr.

Während ihrer Schulzeit zeigte Baehr ein ausgeprägtes Talent für Mathematik und Physik und wurde in diesen Fächern Klassenbeste. In ihrem Studium der Elektrotechnik an der Technischen Universität München (TUM) sah sie die Möglichkeit, Mathematik und Physik zusammenzubringen und gleichzeitig applikations- und praxisnah zu arbeiten. Aufgrund ihrer analytischen Fähigkeiten und ihrem Blick fürs Kleine genauso wie fürs Große zeichnete sich zunächst eine Karriere im Bereich Data Science als Consultant bei einer großen Versicherungsgesellschaft ab – abseits der Forschung.

Der Wendepunkt kam während ihrer Masterarbeit. Im Thema Reverse Engineering entdeckte sie ihre berufliche Leidenschaft: Das Untersuchen von Hardware-Elementen auf ihre Bestandteile und die Entschlüsselung und Rückführung von komplexen, physikalischen Systemen in grundlegende funktionale Komponenten wurde treibende Kraft ihrer Forschung. »Das ist wie eine Schatzsuche, bei der sich einzelne Puzzlestücke zu einem Gesamtbild zusammensetzen. Total faszinierend!«, sagt Baehr.

Verlässliche Aussagen zur Vertrauenswürdigkeit von Elektronik

Diese Begeisterung führte sie zur Promotion am Lehrstuhl von Prof. Dr. Georg Sigl, in der sie sich auf Graph-basierte Verfahren im Reverse Engineering spezialisierte und KI-gestützte Methoden zur Datenauswertung entwickelte. Ziel ihrer Arbeit ist es, selbst fehlerhafte oder unvollständige Daten so zu analysieren, dass verlässliche Aussagen über die Sicherheit von Hardware möglich sind – ein wesentlicher Beitrag zur vertrauenswürdigen Elektronik.

Am Fraunhofer AISEC fand Baehr den idealen Ort, um ihre wissenschaftlichen Interessen mit praktischer Relevanz für Wirtschaft und Gesellschaft zu verbinden. In Projekten für die Industrie und die öffentliche Hand sowie im Rahmen von Initiativen für Hardware-Sicherheit wie der VDE-Fachgruppe »Vertrauenswürdige Elektronik«, dem Trusted Electronic Bayern Center (TrEB) und dem Bayerischen Chip-Design-Center (BCDC) kann sie ihre Forschungsergebnisse zu unmittelbarem gesellschaftlichem Nutzen einbringen. Reale Herausforderungen zu lösen, die einen konkreten Bedarf decken, ist ihr in ihrem Arbeitsalltag enorm wichtig. Neue Ansätze auszutesten, eigenverantwortlich zu handeln und sich kontinuierlich neues Wissen anzueignen, schätzt sie an ihrer Arbeit am Fraunhofer AISEC besonders. Baehr übernimmt gerne die Rolle der vielseitigen Gestalterin, die ihr breites Fachwissen und ihre Initiative gezielt bei Projekten, Konferenzen und Messen einsetzt.

Ein zentrales Anliegen ist Baehr zudem die Förderung des wissenschaftlichen Nachwuchses. Beispielsweise durch ihr Engagement bei dem »Türen auf mit der Maus«-Event am Fraunhofer AISEC macht sie junge Menschen auf spannende Berufsperspektiven in der IT-Sicherheit aufmerksam. Dabei legt sie besonderen Wert darauf, auch Mädchen für Wissenschaft und Technik zu begeistern. Denn Cybersicherheit ist für Baehr nicht nur rational und abstrakt, sondern spielerisch, kreativ und innovativ.

Wolfgang Studier

Leiter der Forschungsgruppe »Identity Management« in der Abteilung »Secure Systems Engineering«

»Digitale Identitäten sind der Schlüssel für eine erfolgreiche Digitalisierung in Deutschland. Ich trage dazu bei, indem ich sichere, datenschutzkonforme und benutzerfreundliche digitale Identitätslösungen entwickle.«

Von der Eröffnung eines Bankkontos bis zur Beantragung eines Führerscheins setzen zahlreiche digitale Services eine benutzerfreundliche und sichere digitale Identität voraus. Ohne sie bleibt die Digitalisierung in vielen Bereichen Stückwerk. Davon ist Wolfgang Studier überzeugt. Als Leiter der Gruppe »Identity Management« in der Abteilung »Secure Systems Engineering« am Fraunhofer AISEC entwickelt er Lösungen für eine sichere digitale Identität.

Seine Begeisterung für die IT beginnt mit Multi-User-Dungeon-Spielen im Teenager-Alter, bei denen er erstmals programmiert und im kollaborativen Arbeiten eine digitale Welt formt. Am Bachelorstudium der Angewandten Informatik an der Hochschule Offenburg schätzt er den starken Praxisanteil bei der Softwareentwicklung und Programmierung. In seiner Bachelorarbeit, die er bei Rohde & Schwarz Cybersecurity absolviert, baut er ein Verschlüsselungsgerät für VoIP-Telefonie. Sein Fokus auf IT-Sicherheit schärft sich weiter im Masterstudium der Informatik an der FU Berlin und als Teil einer Arbeitsgruppe für Kryptografie und digitale Identitäten am Lehrstuhl von Prof. Dr. Marian Margraf.

Mission: Cybersicherheit der deutschen EUDI-Wallet

Mit der Übernahme der Abteilungsleitung »Secure Systems Engineering« des Fraunhofer AISEC am Standort Berlin durch Professor Margraf wechselt auch Studier in die Fraunhofer-Familie. Seine Forschungsarbeit zu zukunftsträchtigen Sicherheitstechnologien richtet er flexibel gemäß den realen gesellschaftlichen und wirtschaftlichen Bedarfen aus – dabei ist die gesellschaftliche Relevanz seines Berufs für ihn essenziell. Hauptaugenmerk von Studier und seinem Team liegt aktuell auf dem Projekt »EUDI-Wallet«. Das zielt gemäß der eIDAS-Verordnung (eIDAS 2.0) der Europäischen Union darauf ab, für Deutschland bis 2027 mindestens eine European Digital Identity Wallet (EUDI-Wallet) bereitzustellen. Studier entwickelt hierzu ein Architekturkonzept sowie ein Konzept für die IT-Sicherheit der gesamtdeutschen EUDI-Wallet. Herausfordernd ist vor allem die Umsetzung sehr hoher Sicherheits- und Datenschutzanforderungen, der Interoperabilität mit den digitalen ID-Lösungen anderer EU-Mitgliedstaaten und einer positiven User Experience.

Für Studier ist Cybersicherheit Teamarbeit. Am Fraunhofer AISEC kann er auf die Unterstützung seiner Co-Teamleiter und seines Abteilungsleiters bauen. Darüber hinaus setzt Studier auf eine klare Struktur und einen Umsetzungsplan, um innovative Lösungen für komplexe Sicherheitsprobleme effizient und nachhaltig zu lösen.

Das Thema digitale Identität wird ihn auch in den kommenden Jahren begleiten, denn auch in seinem Promotionsvorhaben möchte er diesen Themenkomplex weiter ausbauen. »Wir haben hier eine große Chance, die Digitalisierung entscheidend voranzubringen,« sagt er. Mit Leidenschaft und einem Bewusstsein für die gesellschaftliche Relevanz seiner Forschung gestaltet er die digitale Zukunft Deutschlands.

Hannah Schmid

Leiterin der Forschungsgruppe »Embedded Software Analysis« in der Abteilung »Product Protection and Industrial Security«

Embedded Security steckt voller Potenzial, und das ist auch gut so – sonst wäre mein Job ja langweilig.«

Hannah Schmid weiß nach ihrem Informatik-Master 2017 genau, was sie will: mit Profis lernen. Allzu oft sind Verantwortliche für IT-Sicherheit in Unternehmen die einzigen in ihrem Bereich. Am Fraunhofer AISEC findet die Absolventin der TU München stattdessen »ein ganzes Haus voller Cybersecurity-Expertinnen und -Experten« – die ideale Umgebung, um sich fachlich weiterzuentwickeln. Über Abteilungsgrenzen hinweg treibt sie die Forschung zur Absicherung eingebetteter Systeme in der Automobilbranche voran. 2024 geht Schmid den nächsten Schritt und gründet die Forschungsgruppe »Embedded Software Analysis« – und das in einer besonderen Lebensphase: Sie erwartet ihr erstes Kind. Babyglück und Führungsverantwortung sind für die Informatikerin kein Widerspruch, sondern eine Aufgabe, die sie – genau wie ihre Forschung – mit Weitsicht, Pragmatismus und Effizienz angeht.

Smarte Methoden für sichere Software

Gemeinsam mit ihrem Team entwickelt Schmid Werkzeuge für effiziente Analysen von Software in Steuergeräten, Sensoren und anderen eingebetteten Systemen. Zwar gibt es bereits eine Vielzahl an Analyse-Tools, doch nicht jedes ist mit jeder Codebasis kompatibel, und viele liefern eine Flut an Ergebnissen, die manuell geprüft werden müssen. Für eine effiziente Prüfung setzt Schmid auf moderne Technologien:

- **Künstliche Intelligenz** erkennt automatisch Muster und potenzielle Schwachstellen in großen Codebasen.

- Die Kombination von **statischer und dynamischer Analyse** bietet Synergieeffekte für mehr Präzision der Ergebnisse.

- **Code Property Graphs** verknüpfen syntaktische, semantische und datenflussbezogene Informationen einer Software in einer einheitlichen Darstellung – die ideale Basis für tiefgehende Sicherheitsanalysen.

So entstehen Prüfwerkzeuge, die umfassende, aber präzise Ergebnisse liefern. Denn jede Fehlermeldung bedeutet manuellen Aufwand – und im schlimmsten Fall bleibt eine echte Sicherheitslücke unentdeckt.

Forschung in der Anwendung

Die praktische Relevanz steht für Schmid an erster Stelle. Ihr Tooling, wie der modulare Werkzeugkasten »Woodpecker«, kommt direkt in der Industrie zum Einsatz. Mit ihrem Team schult und berät sie Entwicklerinnen und Entwickler im Umgang mit Analyse-Werkzeugen und führt selbst Sicherheitsanalysen durch. »Wir bekommen konkrete Problemstellungen aus der Industrie und entwickeln passgenaue Lösungen«, erklärt die Informatikerin. Diese enge Verzahnung von Wissenschaft und Praxis macht ihre Arbeit so wirkungsvoll: Ihre Methoden und Tools entstehen nicht im Elfenbeinturm, sondern werden an realen Herausforderungen gemessen – und funktionieren deswegen auch mit fragmentiertem Code, fehlenden Abhängigkeiten oder lückenhafter Dokumentation.

»Jeder neue Code ist wie ein Puzzle – welche Bausteine greifen ineinander? Wie wurde die Funktion umgesetzt?«, beschreibt Schmid begeistert. Denn Sicherheitslücken schließt nur, wer tief in den Code eintaucht. Deckt eines ihrer Werkzeuge eine Schwachstelle auf, die zuvor nur durch mühsame manuelle Analyse gefunden werden konnte, weiß sie: »Das macht einen echten Unterschied!«

Pascal Debus

Leiter der Forschungsgruppe »Quantum Security Technologies« in der Abteilung »Cognitive Security Technologies«

Ob für Angriffe oder Schutzmechanismen – Quantencomputer werden die IT-Sicherheit neu definieren. Jetzt ist die Zeit, die Weichen für Quantensicherheit zu stellen.«

Als Pascal Debus Physik studierte, war Quantencomputing ein Nischenthema. In den frühen 2010er-Jahren experimentierte die Forschung mit wenigen Qubits; Algorithmen wie die von Shor und Grover schienen das gesamte Feld abzudecken. Heute ist ein regelrechter Hype um die Supercomputer entfacht. Größer, schneller, besser lautet die Devise.

Doch Quantencomputer sind komplex. Ihre Umsetzung, von Chip bis Cloud, erfordert Expertise aus unterschiedlichsten Disziplinen: Elektrotechnik, Informatik sowie theoretische und experimentelle Physik. In diesem Spannungsfeld spielt Pascal Debus seine Vielseitigkeit aus. Mit einem Bachelor- und Masterabschluss in Physik von der ETH Zürich und Abschlüssen in Mathematik und BWL sowie Erfahrung als Softwareentwickler wird er zum Brückenbauer in einem boomenden Forschungsfeld.

Quantencomputing trifft Cybersicherheit

Trotz des Hypes um Quantencomputer gerät ein entscheidender Aspekt oft in den Hintergrund: Sicherheit. Hier setzt Debus an. Seit 2022 forscht er mit seinem Team »Quantum Security Technologies« zur Sicherheit für und mit Quantencomputing. Die immense Rechenleistung der Technologie lässt sich gezielt für die IT-Sicherheit nutzen – etwa in der Software-Verifikation oder im Quantum Machine Learning (QML) zur Anomalieerkennung.

So erforscht Debus mit SAP, wie QML beim Cloud-Monitoring helfen kann: Quantenalgorithmen werten Protokolldaten aus, um ungewöhnliche Abweichungen – etwa plötzliche Leistungseinbrüche oder verdächtige Zugriffsversuche – effizient zu erkennen. Während herkömmliche Algorithmen an der Komplexität dieser Daten scheitern, kann das quantengestützte System verdächtige Vorfälle erkennen und frühzeitig Alarm schlagen.

Schutz ab dem ersten Qubit

»Jetzt ist die Zeit, Quantencomputing vor Angriffen zu schützen,« mahnt Debus. Neben der Absicherung des gesamten Tech-Stacks eines Quantencomputers – von der Hardware bis zur Cloud – nach dem Prinzip »Security by Design« liegt sein Fokus auf der Sicherheit von QML.

Mit der d-fine GmbH untersucht er im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) die potenziellen Angriffsflächen von QML. Besonders riskant sind »adversarial attacks« – gezielte Manipulationen, die die Ergebnisse von Quantenalgorithmen verfälschen. Um sie abzuwehren, überträgt Debus bewährte Sicherheitskonzepte aus der klassischen IT auf QML und entwickelt neue quantenspezifische Schutzmechanismen.

Obwohl das Bewusstsein für Quantensicherheit wächst, bleibt viel zu tun. Und das ist gut so, denn Stillstand ist für den dreifachen Familienvater keine Option – und an Herausforderungen mangelt es in seinem dynamischen Forschungsfeld nicht.

Publikationen

Banse, C.; Schneider, A.; Kunz, I.: »owl2proto: Enabling Semantic Processing in Modern Cloud Micro-Services«. In: 16th International Conference on Knowledge Engineering and Ontology Development, 2024.

Bauer, T. J.; Aßmuth, A.: »Securing Confidential Data For Distributed Software Development Teams: Encrypted Container File«. In: International Journal On Advances in Security, vol. 17, no. 1 and 2, 2024, pp. 11–28.

Binder, A. M.; Kunz, I.: »Using Static Code Analysis for GDPR Compliance Checks«. In: European Symposium on Research in Computer Security. Springer, 2024.

Bramm, G.; Önen, M.; Schanzenbach, M.; Komarov, I.; Morgner, F.; Tiebel, C.; Cadavid, J.: »UPCARE: User Privacy-preserving Cancer Research Platform«. In: Proceedings of the 21st International Conference on Security and Cryptography, 2024, pp. 52–63. ISBN: 978-3-88579-744-9. DOI: 978-989-758-709-2.

Choorod, P.; Bauer, T. J.; Aßmuth, A.: »Distinguishing Tor From Other Encrypted Network Traffic Through Character Analysis«. In: Proceedings of the 15th International Conference on Cloud Computing, GRIDs, and Virtualization (Cloud Computing 2024), Venice, Italy: May 2024, pp. 8–12.

Gavrilan, I.; Oberhansl, F.; Wagner, A.; Strieder, E.; Zankl, A.: »Impeccable Keccak: Towards Fault Resilient SPHINCS+ Implementations«. In: IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2024.2, 2024, pp. 154–189. DOI: 10.46586/tches.v2024.i2.154-189.

Kao, C-Y.; Ghanmi, I.; Ben Ayed, H.; Kumar, A.; Böttinger, K.: »Near Real-Time Detection and Rectification of Adversarial Patches«. In: Future of Information and Communication Conference. Springer, 2024, pp. 174–196.

Geier, J.; Auer, L.; Mueller-Gritschneder, D.; Sharif, U.; Schlichtmann, U.: »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 '24), Association for Computing Machinery, New York, USA, 2024, pp. 676–682. DOI: 10.1145/3566097.3567925.

Hager-Clukas, A.; Hohentanner, K.: »DMTI: Accelerating Memory Error Detection in Precompiled C/C++ Binaries with ARM Memory Tagging Extension«. In: Proceedings of the 2024 ACM Asia Conference on Computer and Communications Security (ASIA CCS '24). Singapore, Singapore: ACM, July 2024. ISBN: 979-8-4007-0482-6/24/07. DOI: 10.1145/3634737.3637655.

Kasten, F.; Zieris, P.; Horsch, J.: »Integrating Static Analyses for High-Precision Control-Flow Integrity«. In: Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses. RAID '24, Padua, Italy: Association for Computing Machinery, 2024, pp. 419–434. ISBN: 9798400709593. DOI: 10.1145/3678890.3678920.

Kasten, F.; Zieris, P.; Horsch, J.: »Integrating Static Analyses for High-Precision Control-Flow Integrity«. In: Proceedings of the 27th International Symposium on Research in Attacks, Intrusions and Defenses. RAID '24. Padua, Italy: Association for Computing Machinery, 2024, pp. 419–434. ISBN: 9798400709593. DOI: 10.1145/3678890.3678920.

Lange, F.; Kunz, I.: »Evolution of Secure Development Lifecycles and Maturity Models in the Context of Hosted Solutions«. In: Journal of Software: Evolution and Process, 2024.

Ludwig, A.; Heinl, M. P.; Giehl, A.: »MINERVA: Secure Collaborative Machine Tool Data Utilization Leveraging Confidentiality-Protecting Technologies«. In: Open Identity Summit 2024. Ed. by Heiko Roßnagel, Filipe Sousa, Christian H. Schunck. Gesellschaft für Informatik e.V., 2024.

Morris, J.; Tatschner, S.; Heinl, M. P.; Heinl, P.; Newe, T.; Plaga, S.: »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. ISBN: 978-3-031-45162-1. DOI: 10.1007/978-3-031-45162-1_9.

Müller, N. M.; Evans, N.; Tack, H., Sperl, P.; Böttinger, K.: »Harder or Different? Understanding Generalization of Audio Deepfake Detection«. In: Interspeech 2024, 2024.

Müller, N. M.; Kawa, P.; Choong, W. H.; Casanova, E.; Gölge, E.; Müller, T.; Syga, P.; Sperl, P.; Böttinger, K.: »MLAAD: The Multi-Language Audio Anti-Spoofing Dataset«. In: International Joint Conference on Neural Networks (IJCNN), 2024.

Müller, N. M.; Kawa, P.; Hu, S.; Neu, M.; Williams, J.; Sperl, P.; Böttinger, K.: »A New Approach to Voice Authenticity«. In: Interspeech 2024, 2024.

Müller, N. M.; Roschmann, S.; Khan, S.; Sperl, P.; Böttinger, K.: »Shortcut Detection with Variational Autoencoders«. In: International Joint Conference on Neural Networks (IJCNN), 2024.

Näther, C.; Herzinger, D.; Gazdag, S-L.; Steghöfer, J-F.; Daum, S.; Loebenberger, D.: Migrating Software Systems towards Post-Quantum-Cryptography – A Systematic Literature Review. In: IEEE, June 2024. DOI: 10.48550/arXiv.2404.12854

Orthen, B.; Braunsdorf, O.; Zieris, P.; Horsch, J.: »SoftBound+CETS Revisited: More Than a Decade Later«. In: The 17th European Workshop on Systems Security (EuroSec '24). Athens, Greece: ACM, April 2024. ISBN: 979-8-4007-0542-7. DOI: 10.1145/3642974.3652285.

Ott, S.; Orthen, B.; Weidinger, A.; Horsch, J.; Nayani, V.; Ekberg, J-E.: »MultiTEE: Distributing Trusted Execution Environments«. In: Proceedings of the 19th ACM Asia Conference on Computer and Communications Security. ASIA CCS '24. Singapore, Singapore: Association for Computing Machinery, 2024, pp. 1617–1629. ISBN: 9798400704826. DOI: 10.1145/3634737.3637675.

Peters, S. N.; Puch, N.; Heinl, M. P.; Zieris, P.; Protsenko, M.; Larsen-Vefring, T.; Gomes, M. E.; Maftun, A.; Zeschg, T.: »Gateway to the Danger Zone: Secure and Authentic Remote Reset in Machine Safety«. In: ARES 2024. Vienna, Austria: ACM, 2024. DOI: 10.1145/3664476.3670940.

Schanzenbach, M.; Nadler, S.; Henderson, I.; Jeyakumar, J.: »GRAIN: Truly Privacy-friendly and Self-sovereign Trust Establishment with GNS and TRAIN«. In: Open Identity Summit 2024. Bonn: Gesellschaft für Informatik e.V., 2024, pp. 85–92. ISBN: 978-3-88579-744-9. DOI: 10.18420/OID2024_07.

Schink, M.; Wagner, A.; Oberhansl, F.; Köckeis, S.; Strieder, E.; Freud, S.; Klein, D.: »Unlock the Door to my Secrets, but don't Forget to Glitch: A Comprehensive Analysis of Flash Erase Suppression Attacks«. In: IACR Transactions on Cryptographic Hardware and Embedded Systems, vol. 2024.2 (2024), pp. 88–129. DOI: 10.46586/tches.v2024.i2.88-129.

Schöberl, S.; Banse, C.; Geist, V.; Kunz, I.; Pinzger, M.: »CertGraph: Towards a Comprehensive Knowledge Graph for Cloud Security Certifications«. In: 27th International Conference on Model Driven Engineering Languages and Systems, 2024.

Tatschner, S.; Heinl, M. P.; Pappler, N.; Specht, T.; Newe, T.: »Tracking Down Software Cluster Bombs: A Health State Analysis of the Free Open-Source Software (FOSS) Ecosystem«. In: SSRN, 2024. DOI: 10.2139/ssrn.4847570.

Tatschner, S.; Peters, S.; Heinl, M. P.; Specht, T.; Newe, T.: »ParsEval: Evaluation of Parsing Behavior using Real-world Out-in-the-wild X.509 Certificates«. In: ARES 2024. Vienna, Austria: ACM, 2024. DOI: 10.1145/3664476.3669935.

Wang, K.; Kasatkin, D.; Ahlrichs, V.; Auer, L.; Hohentanner, K.; Horsch, J.; Ekberg, J-E.: »Cherifying Linux: A Practical View on Using CHERI«. In: The 17th European Workshop on Systems Security (EuroSec '24). Athens, Greece: ACM, April 2024. ISBN: 979-8-4007-0542-7. DOI: 10.1145/3642974.3652282.

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, František Strnadel,
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
Server des Fraunhofer AISEC

Bildquellen
Cover: Andreas Heddergott
Seite 4: Bernd Müller, Andreas Heddergott
Seite 8: Freepik, Fraunhofer AISEC
Seite 10: Bernd Müller
Seite 13: Freepik, Fraunhofer AISEC
Seite 15: Freepik, Fraunhofer AISEC
Seite 15: Freepik, Fraunhofer AISEC, FU Berlin
Seite 19: Oliver Bodmer
Seite 21: Adobe Stock, AllEyesOnYou.de
Seite 22: Gene Glover, Freepik, Fraunhofer AISEC
Seite 24: Oliver Bodmer
Seite 27: Andreas Heddergott
Seite 28: 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 36: Governikus GmbH & Co. KG
Seite 37: SICK AG
Seite 40: Andreas Heddergott
Seite 44: Andreas Heddergott
Seite 47: Andreas Heddergott
Alle übrigen Abbildungen: © Fraunhofer AISEC

Alle Rechte vorbehalten.
Vervielfältigung und Verbreitung nur mit Genehmigung der Redaktion.

© Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC
Garching bei München, Mai 2025

Folgen Sie uns!

Cybersecurity-Blog des Fraunhofer AISEC

LinkedIn