Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

2. Cybersicherheitstag

CRA, NIS-2 & Co: Neue Regularien für Innovationsschub nutzen

Agenda

16:00-17:00 Uhr Treffpunkt Foyer, EG	AISEC Lab Tour (optional)
16:30-17:00 Uhr Foyer, EG	Registrierung & Pre-Networking
17:00-17:10 Uhr Raum 1.A.Box	Begrüßung
17:15-17:30 Uhr Raum 1.A.Box	Impuls »Cybersicherheits-Roadmap für NIS-2, CRA & Co.« (Prof. Dr. Claudia Eckert)
17:30-18:15 Uhr Raum 1.A.Box	Use Case Praxisnahe Einblicke in unsere Fallstudie mit der SICK AG
18:15-19:45 Uhr Demo-Raum	Demonstrator-Schau
18:15-19:15 Uhr Treffpunkt Foyer, EG	AISEC Lab Tour (optional)
19:45-20:00 Uhr Raum 1.A.Box	Wrap-up & Take-Home-Messages
19:45 Uhr	Networking

Impuls

Cybersicherheits-Roadmap für NIS-2, CRA & Co.

Prof. Dr. Claudia Eckert

Prof. Dr. Claudia Eckert

Die Institutsleiterin des Fraunhofer AISEC beleuchtet kurz die aktuellen EU-Regularien NIS-2 und Cyber Resilience Act (CRA) zur Erhöhung der Cybersicherheit und identifiziert Gemeinsamkeiten, die zumeist Standard-Techniken und Maßnahmen zur Umsetzung erfordern. Sie skizziert einige der am Fraunhofer AISEC in Entwicklung befindlichen Tools, die Administratoren und Sicherheitsverantwortliche darin unterstützen, die Anforderungen aus den Regularien zu erfüllen, das Sicherheitslevel im Unternehmen substanziell zu erhöhen und die Geschäftskontinuität zu sichern.
Kontakt: claudia.eckert@aisec.fraunhofer.de

Use Case

Praxisnahe Einblicke in unsere Fallstudie mit der SICK AG

Ingo Münch, Ian Murawski

Die SICK AG gibt in einer Fallstudie Einblicke, wie die neuen Regularien erfüllt und für den nächsten Innovationsschub genutzt werden können. Sie lernen eine in der Praxis erprobte Methode kennen, die Sie gemeinsam mit der SICK AG zum Standard weiterentwickeln können. Partner werden gesucht.
Kontakt:
ingo.muench@sick.de | ian.murawski@sick.de

Demonstrator-Schau

Expertise der Forschungsabteilung Hardware Security

Hardware-basierte Sicherheit und Vertrauenswürdigkeit für IoT

IoT-Geräte durchdringen viele Wirtschafts- und Alltagsbereiche. Da sie oft sensible Daten verarbeiten, ist ihre Sicherheit und Vertrauenswürdigkeit essenziell. Das Fraunhofer AISEC forscht in verschiedenen Projekten an der Absicherung von IoT-Geräten auf Hardware-Ebene. Dazu werden Analysemethoden und passende Gegenmaßnahmen entwickelt, um die Hardware und auch die auf dem System ausgeführte Software zu schützen. Ein wichtiger Aspekt ist die Analyse von Laser- und Fehlerangriffen oder die Manipulation von Versorgungsspannung und Takt.

Kontakt: matthias.hiller@aisec.fraunhofer.de

»Connector Measurement Component CMC« auf GitHub

Confidential Computing für Software Supply Chains

Die Sicherheit und Integrität von Software im gesamten Entwicklungs-Lebenszyklus ist eine Anfoderung des CRA. Die Ausführung von Software in der Cloud auf bereitgestellter Fremd-Infrastruktur ist jedoch risikobehaftet. Das am Fraunhofer AISEC entwickelte »Connector Measurement Component CMC« erfasst automatisiert die Vertrauenswürdigkeit von Software-Komponenten mithilfe von Hardware-basierten, kryptografischen Vertrauensankern. Das Open Source Tool schafft Transparenz und Nachprüfbarkeit gegenüber den verwendeten Software-Paketen. Es ermöglicht, das Vertrauen in die Software zu evaluieren und nicht vertrauenswürdige Änderungen an der Software zu erkennen.

Kontakt: albert.stark@aisec.fraunhofer.de

Schnelle Security-Risikoanalyse mit »QuBA«

In der Regel sind qualitative Security-Risikoanalysen aufwändig und ressourcenintensiv. Eine einfache Handhabung der Analyse bietet die vom Fraunhofer AISEC in Zusammenarbeit mit der SICK AG entwickelte Analysemethode »QuBA« (Questionnaire-Based Assessment). Der Risikostatus von einfachen Produkten mit einheitlichem Schutzbedarf lässt sich so in nur wenigen Stunden ermitteln. Die Risikoeinschätzung basiert auf einem Fragebogen, der Angriffe, Schäden und Schutzmaßnahmen abbildet und auf eigens zusammengestellte Kataloge zurückgreift.

Kontakt: hannah.schmid@aisec.fraunhofer.de

»QuBA« auf der Webseite des Fraunhofer AISEC

Automatisierte Konformitätsprüfung für den CRA

Mit »Confirmate« entwickelt das Fraunhofer AISEC ein Tool zur automatisierten Konformitätsprüfung von Software-Komponenten. Es unterstützt Hersteller, die Übereinstimmung ihres Software-Stacks mit dem CRA zu überprüfen und ihren individuellen Handlungsbedarf zu ermitteln. Die Lösung umfasst die Quellcode-Analyse der im Produkt enthaltenen Software-Komponenten und der bereitgestellten Schnittstellen, aber auch die Konfiguration der Deployment-Infrastruktur.

Kontakt: immanuel.kunz@aisec.fraunhofer.de

Pressemitteilung zu »Confirmate«

Sichere Ausführungsumgebungen mit »GyroidOS«

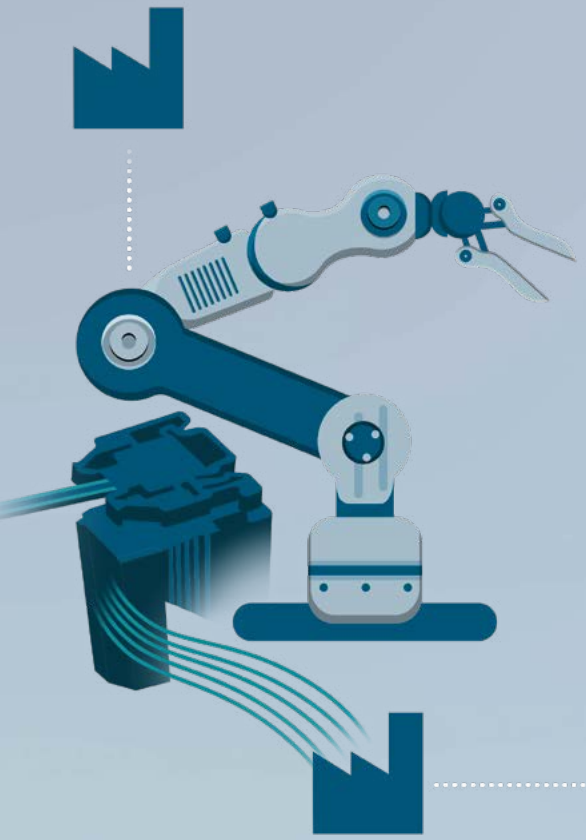
Die vom Fraunhofer AISEC entwickelte Plattformlösung »GyroidOS« unterstützt Zertifizierungsprozesse nach den Industriestandards DIN SPEC 27070 und IEC 62443-4-2 sowie gemäß Common Criteria. »GyroidOS« isoliert besonders schützenswerte Anwendungen und Daten und verhindert unkontrollierten Informationsaustausch zwischen Ausführungscontainern. Durch zahlreiche weitere Sicherheitsfunktionen trägt es entscheidend zur Erfüllung der Sicherheitsanforderungen des CRA bei.

Kontakt: michael.weiss@aisec.fraunhofer.de

»GyroidOS« auf GitHub

Cybersecurity Labs

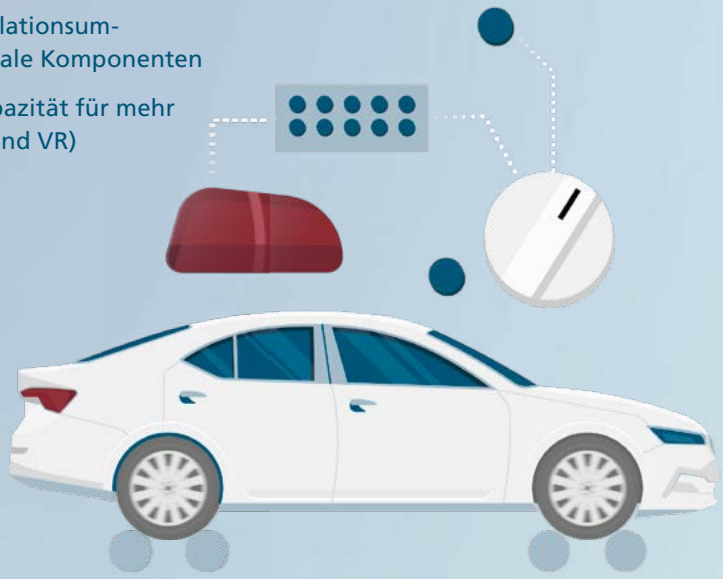
Erfahren Sie bei Laborführungen, wie Sie unsere Ausstattung nutzen können.



INDUSTRIAL SECURITY LAB

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

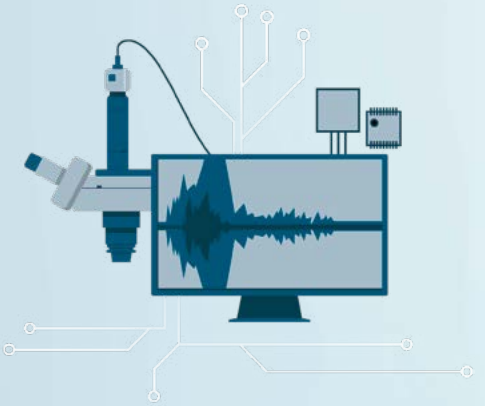
- Risikoanalysen und Penetrationstests
- Realitätsnahe Simulationsumgebungen durch reale Komponenten
- Erhöhte Rechenkapazität für mehr Simulationen (AR und VR)



HARDWARE SECURITY LAB

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

- Hochpräzise 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 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 Tests von Security-Maßnahmen
- Zertifizierte Umgebung nach TISAX Assessment Level 3

Kontakt

Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit AISEC
Lichtenbergstraße 11
85748 Garching bei München
marketing@aisec.fraunhofer.de
www.aisec.fraunhofer.de

Webseite

Cybersecurity Blog

Anmeldung zum Newsletter

@FraunhoferAISEC