Fraunhofer AISEC

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC

1. Cybersicherheitstag

Forschung trifft Industrie

9. November 2023

Agenda

13:00-14:00 Uhr	Demonstrator-Ausstellung
14:00-14:15 Uhr	Welcome

Parallele Programmpunkte

14:15-18:00 Uhr	Demonstrator-Ausstellung
14:15-16:15 Uhr	Expert Sessions
14:15-16:15 Uhr	Cybersecurity Labs
17:00-18:00 Uhr	Get-together

Demonstrator-Ausstellung

BlackBoxCam: Die datenschutzkonforme Dashcam

Der Einsatz von Dashcams im Straßenverkehr ist in Deutschland umstritten, denn das permanente Aufzeichnen von Personen ist nicht datenschutzkonform. Die »BlackBoxCam« nimmt Videodaten in unbeschränkter Länge und datenschutzkonform auf. Die Aufzeichnung wird verschlüsselt gespeichert. Dabei kann mithilfe eines Regelwerks bestimmt werden, für wen und unter welchen Umständen Videomaterial einsehbar ist. Ein integriertes Machine-Learning-Modell »verwischt« die Gesichter der abgebildeten Personen.

Exponat Nr. 01

Kontakt: mykolai.protsenko@aisec.fraunhofer.de

Webseite »BlackBoxCam«

Bug Hunting with Memory Safety: Weniger Fehler im Programmcode

Um spätere Schwachstellen zu vermeiden, müssen Programmierfehler bereits im Entwicklungsprozess von Software entdeckt werden. Durch eine individuelle, am Product-Live-Cycle orientierte Planung reduzieren unsere IT-Security-Spezialisten die Komplexität von Fuzzing-Prozessen, setzen anforderungsorientierte Schwerpunkte für die Code-Analyse und etablieren nachhaltige Abläufe, die auch in späteren Produktlebensphasen zu Kosteneinsparungen führen. Der Demonstrator zeigt, wie der Ansatz die Entwicklung von sicherer und fehlerfreier Software unterstützt, bevor es zu einem Sicherheitsvorfall kommt.

Exponat Nr. 02

Kontakt: konrad.hohentanner@aisec.fraunhofer.de

Webseite der Forschungsabteilung Secure Operating Systems

»Clouditor« auf GitHub

Clouditor: Überwachung von Cloud-Systemen

Zertifizierungsaudits sind ressourcenintensive Verfahren. Das Open-Source-Tool »Clouditor« ermöglicht eine automatisierte und kontinuierliche Überwachung von Cloud-Systemen. Ein Nachweis über Sicherheits- oder Compliance-Anforderungen bestehender Cloud-Dienste und eine Sicherheitszertifizierung sind jederzeit möglich. Automatisierte Scans und Berichte minimieren die Fehlerquote und redundante Auditvorbereitungen. Das spart Zeit und Kosten.

Exponat Nr. 03

Kontakt: nico.haas@aisec.fraunhofer.de

Webseite des Fraunhofer CCIT

Edge-Cloud-Continuum

Die Forschung und Entwicklung von Technologielösungen im Bereich Edge-Cloud-Continuum ist das Forschungsthema des Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT. Ziel ist, die Vorteile von Edge- und Cloud-Computing zu vereinen und die IoT-Ebene mitzuintegrieren. So wird ein kontinuierlicher Datenraum geschaffen, in dem die Verlagerung von Rechenleistung bedarfsorientiert und dynamisch erfolgt. Anwendungsbeispiele sind der intelligente Nutenstein, die intelligente Schraubverbindung und die Smart-Intersection.

Exponat Nr. 04

Kontakt: michael.fritz@aisec.fraunhofer.de

Plattform »Deepfake Total«

Deepfakes: Audio-Dateien auf ihre Authentizität prüfen

Für den Zugang zu sensiblen Daten setzen Unternehmen immer häufiger auf die Überprüfung der Identität anhand biometrischer Daten durch eine künstliche Intelligenz (KI). Dafür muss die KI Manipulationen von Audio-Dateien – sogenannte »Deepfakes« – erkennen. Die Plattform »Deepfake Total« prüft Audio-Dateien auf ihre Authentizität und liefert eine automatisierte Verifikation von Medieninhalten. Das anpassbare Machine-Learning-Modell schafft Vertrauen gegenüber authentischen Informationen.

Exponat Nr. 05

Kontakt: nicolas.mueller@aisec.fraunhofer.de

IIoT: Vertrauen schaffen in industriellen Umgebungen

Sensorknoten und Gateways in industriellen Umgebungen sind lohnende Ziele für Cyberangriffe. Eine vom Fraunhofer AISEC entwickelte Firmware kann einen Nachweis der Hardware- und Firmware-Integrität erbringen. Die eingesetzte Physical Unclonable Function (PUF) stellt dabei den Authentizitätsnachweis sicher. Die Verschlüsselung erfolgt mittels Attribute-Based Encryption (ABE). Eine große Reichweite der Datenübertragung wird durch die LoRa-Technologie erreicht.

Exponat Nr. 06

Kontakt: armando.miguel.garcia@aisec.fraunhofer.de

Webseite der Forschungsabteilung Hardware Security

IT-Sicherheit für Fahrzeuge

Durch physischen Fahrzeugzugriff können Angreifende Kontrolle über Steuergeräte erlangen und Fehlfunktionen auslösen. Das Diagnose-Tool »gallia« überprüft mithilfe von Unified Diagnostic Services (UDS) Steuergeräte und Dienste und kann den Ist-Zustand mit dem erwartbaren Zustand der Fahrzeugkomponenten abgleichen. Pentests durch Automotive-Security-Experten des Fraunhofer AISEC ermöglichen eine IT-Sicherheitseinschätzung. Sie konzipieren individuelle Lösungsansätze für Fahrzeuge, (Industrie- und Bau-)Maschinen, Eisenbahn und Schiffe.

Exponat Nr. 07

Kontakt: dieter.schuster@aisec.fraunhofer.de

»gallia« auf GitHub

Mobile ad hoc Networks für Katastrophenfälle

Im Katastrophenfall müssen Rettungskräfte miteinander kommunizieren. Dies gelingt mit mobilen ad-hoc-Netzwerken, die auch für die zivile Kommunikation nutzbar sind. Die Trennung von hoheitlicher und ziviler Kommunikation erfolgt durch die Plattform »GyroidOS«. Die Open-Source-Lösung isoliert Bereiche von Betriebssystemen und schafft privilegierte Instanzen. Auch Daten mit einer Geheimhaltungsstufe können verarbeitet werden. Das System unterstützt Zertifizierungsprozesse gemäß Industriestandard IDS / IEC 62443.

Exponat Nr. 08

Kontakt: michael.weiss@aisec.fraunhofer.de

»GyroidOS« auf GitHub

Webseite der Forschungsabteilung Secure Operating Systems

Pay per Scan: Durch vertrauenswürdige Logistikketten neue Geschäftsmodelle erschließen

Eine vertrauenswürdige Logistikkette ist entscheidend für einen reibungslosen Ablauf von Warenlieferungen. Unternehmen mit einer vertrauenswürdigen Erfassung von Transaktionen können Kosten reduzieren und neue Geschäftsfelder erschließen. Unverzichtbar ist dabei die Integrität, Authentizität und Manipulationsfreiheit der Sensordaten. Das in Kooperation mit der SICK AG erarbeitete Konzept »Pay per Scan« zeigt, wie eine sichere automatisierte Warenerfassung auf Basis der am Fraunhofer AISEC entwickelten Open-Source-Virtualisierungslösung »GyroidOS« gelingt.

Exponat Nr. 09
Kontakt: mykolai.protsenko@aisec.fraunhofer.de

Paper »Universal Remote Attestation for Cloud and Edge Platforms«

Remote Attestation: Plattformintegrität evaluieren

Beim Datenaustausch von vernetzten Geräten kann es durch bösartige oder veraltete Software auf Geräten des Kommunikationspartners zu einer missbräuchlichen Verarbeitung der übertragenen Daten kommen. Das am Fraunhofer AISEC entwickelte Remote Attestation Framework setzt an dieser Stelle an, indem es bereits vor dem Datenaustausch nicht nur die Identität des Kommunikationspartners, sondern auch die Integrität des verwendeten Software-Stacks sicherstellt. Dies funktioniert über kryptographische »Fingerabdrücke« der laufenden Software, welche von Hardware-Vertrauensankern gesammelt und übertragen werden. Nur bei erfolgreicher Prüfung findet ein Datenaustausch statt.

Exponat Nr. 10
Kontakt: monika.kamhuber@aisec.fraunhofer.de

Resilienz für eingebettete Systeme

Da IoT-Geräte über das Internet kommunizieren, bestehen oft Sicherheitsrisiken. Bei einem erfolgreichen Angriff ist die manuelle Wiederherstellung zeit- und kostenintensiv. Die Plattform »Resiliency for Embedded Devices« stellt die Funktionsfähigkeit von kompromittierten Geräten automatisiert wieder her. Die Open-Source-Software enthält ein abgeschottetes Softwaremodul, das vom IoT-Hub signierte Tickets empfängt. Ist diese Kommunikation durch einen Angriff gestört, wird das Gerät zurückgesetzt und ein Firmware-Update reinstalliert.

Exponat Nr. 11
Kontakt: simon.ott@aisec.fraunhofer.de

Webseite der Forschungsabteilung Secure Operating Systems

Robustheitsbewertung von neuronalen Netzen

Künstliche Intelligenz (KI) eröffnet neue Geschäftsfelder. KI-Systeme sind jedoch über Adversarial Examples angreifbar. Angreifende nehmen Veränderungen am Input vor, die zu einer Falschaussage des KI-Models führen. Die am Fraunhofer AISEC bereitgestellte Dienstleistung umfasst eine quantitative Robustheitsbewertung des Models, eine Risikoabschätzung des Gesamtsystems und Empfehlungen für Best-Practices sowie Gegenmaßnahmen. Unternehmen können so vertrauenswürdige KI-Anwendungen nutzen.

Exponat Nr. 12
Kontakt: konstantin.boettinger@aisec.fraunhofer.de

Webseite der Forschungsabteilung Cognitive Security Technologies

Schwachstellenanalyse gegenüber Fehlerangriffen

Beim Hochfahren eines IT-Systems wird die Software auf ihre Authentizität und Integrität geprüft. Im Fall eines Fehlerangriffs bringt ein Angreifer diese Verifizierung zum »Stolpern« und schleust Schadsoftware ein. Das automatisierte Open-Source-Tool »ARCHIE« des Fraunhofer AISEC analysiert den Programmcode auf Schwachstellen gegenüber Fehlerangriffen. Unsere Cybersicherheitsexperten unterstützen Unternehmen durch Konfiguration des Testing-Tools, Risikobewertungen und Konzeption von nachhaltigen Gegenmaßnahmen.

Exponat Nr. 13
Kontakt: alexander.wagner@aisec.fraunhofer.de

»ARCHIE« auf GitHub

Secure Data Ecosystems auf GitHub

Sichere Datenräume

Bei Smart Factories und Predictable Maintenance erzeugen Sensoren Daten, die über Cloud-Infrastrukturen mit Partnern geteilt werden. Der am Fraunhofer AISEC entwickelte Software-Stack zu »Secure Data Ecosystems« ermöglicht Kontrolle und Schutz dieser Daten in der Cloud und auf den Systemen auf Basis breit verfügbarer Hardware. Der Fokus liegt auf dem Trusted Execution Environment, das Daten nur an verhaltenskonforme Partner weiterreicht. Mithilfe dieser integrierten Datennutzungskontrolle schafft das Secure Data Ecosystem sichere und vertrauliche Datenverarbeitungsketten über Vertrauens- und Unternehmensgrenzen hinweg.

Exponat Nr. 14
Kontakt: mathias.morbitzer@aisec.fraunhofer.de

Webseite der Forschungsabteilung Secure Systems Engineering

Usable Security and Privacy: Nutzerfreundlichkeit mit IT-Sicherheit vereinen

Entscheidend für die Akzeptanz einer sicherheitsrelevanten Anwendung sind die Sicherheit des IT-Systems und das Vertrauen des Nutzenden gegenüber der Anwendung. Der Forschungsbereich »Usable Security & Privacy« setzt den Fokus auf benutzbare Sicherheit und vereint Nutzerfreundlichkeit mit IT-Sicherheit. Unsere IT-Sicherheitsexperten begleiten Implementierungsprozesse, erstellen Nutzerstudien und Anwendungen zur Veranschaulichung ihrer Nutzerfreundlichkeit und Sicherheit. Sie steigern die positive User Experience und schaffen Vertrauen und Aktzeptanz gegenüber dem Softwareprodukt.

Exponat Nr. 15
Kontakt: sandra.kostic@aisec.fraunhofer.de

Woodpecker: Effiziente und präzise Code-Analyse

Mit steigender Komplexität von Software steigt die Anzahl der Schwachstellen. Das Fraunhofer AISEC unterstützt in der Implementierungsphase mit Tool-basierter Analyse und manueller Detailanalyse des Quellcodes. Für eine umfassende Securityanalyse wird der modulare Werkzeugkasten »Woodpecker« verwendet. Cybersicherheitsfachleute definieren in Interviews mit den Entwicklern kritische Code-Module und prüfen diese manuell. So entsteht ein umfassender Detailbericht über gefundene Schwachstellen und Vorschläge zu Gegenmaßnahmen.

Exponat Nr. 16
Kontakt: hannah.schmid@aisec.fraunhofer.de

Webseite der Forschungsabteilung Product Protection and Industrial Security

Zero Trust für die Telematikinfrastruktur

Über die Telematikinfrastruktur (TI) sollen Akteure des Gesundheitswesens Patientendaten sicher, schnell und ortsunabhängig kommunizieren. Das Fraunhofer AISEC legt die konzeptionelle Grundlage für eine neue Sicherheitsarchitektur der TI 2.0. Neben einem auf Zero-Trust-Prinzipien basierenden Architekturkonzept und einem Migrationsplan wurde ein Demonstrator für die Sicherheitsarchitektur entwickelt. Zero-Trust-Architekturen stärken die Teilhabe an digitalen Gesundheitsdiensten sowie die Informationssicherheit der Dienste selbst. Die Machbarkeit der Architektur wurde außerdem mithilfe eines »Proof of Concept« nachgewiesen.

Exponat Nr. 17
Kontakt: martin.seiffert@aisec.fraunhofer.de

Pressemitteilung »Zukunftsfähige Sicherheitsarchitektur für die Kommunikation im Gesundheitswesen«

Expert Sessions

Migration zu quantenresistenter Kryptografie

14:15 - 14:45 Uhr | Box
Tudor Soroceanu

Die rasante Entwicklung von Quantencomputern verspricht enorme Fortschritte in Bezug auf Rechenleistung, doch sie wirft auch einen bedrohlichen Schatten auf die herkömmliche Kryptografie. Klassische Verschlüsselungsalgorithmen, die heute die Grundlage für Datensicherheit in Unternehmen bilden, könnten in Zukunft von Quantencomputern geknackt werden. Unternehmen müssen sicherstellen, dass ihre verschlüsselten Daten auch in Zukunft geschützt sind. Dies macht Post-Quanten-Kryptografie (PQC) zu einer unverzichtbaren Technologie. Wie können Unternehmen einen nahtlosen Übergang zur PQC vollziehen und eine erfolgreiche Migration meistern? Der Vortrag geht darauf ein, welche Lösungen für Unternehmen bestehen, ihre sensiblen Daten und Kommunikation in einer Welt mit Quantencomputern zu schützen.

IT-Sicherheit in der Ära der Künstlichen Intelligenz

15:00 - 15:30 Uhr | Box
Dr. Nicolas Müller

Die fortschreitende Entwicklung von Künstlicher Intelligenz (KI) hat zahlreiche Anwendungsgebiete revolutioniert, und die IT-Sicherheit bildet hier keine Ausnahme. Der Vortrag zeigt auf, wie KI in der Sicherheitsbranche immer präsenter wird. Mit KI können Netzwerkangriffe und Finanzbetrug durch Anomalieerkennung effizienter erkannt werden. Zudem ermöglicht KI-gestütztes Fuzzing die Identifikation von Systemschwachstellen. Doch KI-Systeme sind anfällig für Adversarial Attacks, welche die Künstliche Intelligenz fehlleiten. Wie können wir unsere KI-Modelle widerstandsfähig und verlässlich gestalten? Ein weiterer Brennpunkt sind Deepfakes – erzeugt durch KI-Techniken wie Text-to-Speech. Wie gehen wir vor, um diese täuschend echten Fälschungen zuverlässig zu identifizieren? Dieser Vortrag liefert einen Einblick in Chancen und Herausforderungen von KI in der IT-Sicherheit.

Vertrauenswürdige Elektronik – Grundlage für ein sicheres IoT

15:45 - 16:15 Uhr | Box
Andreas Seelos-Zankl

Neue eingebettete Systeme ermöglichen den Einsatz in immer neuen Anwendungen z. B. im Bereich des Internet der Dinge (IoT), Edge Computing oder eingebetteter KI. Durch die erhöhte Vernetzung und Verbreitung vergrößert sich die Angriffsfläche und das Sicherheitsrisiko für das Gerät, die verarbeiteten Daten und die Anwendung. Security Features wie kryptografische Implementierungen, sichere Schlüsselspeicher, secure Boot, Separierung auf Architekturebene oder Gegenmaßnahmen gegen physische Angriffe ermöglichen es im Zusammenspiel, Systeme aus der Hardware heraus zu schützen. Der Vortrag zeigt auf, wie diese Maßnahmen korrekt implementiert werden und geht auf Herausforderungen wie den Übergang zur Post-Quanten-Kryptografie, den Transfer von RISC-V-Prozessoren und den Einsatz von Open Source Hardware ein.

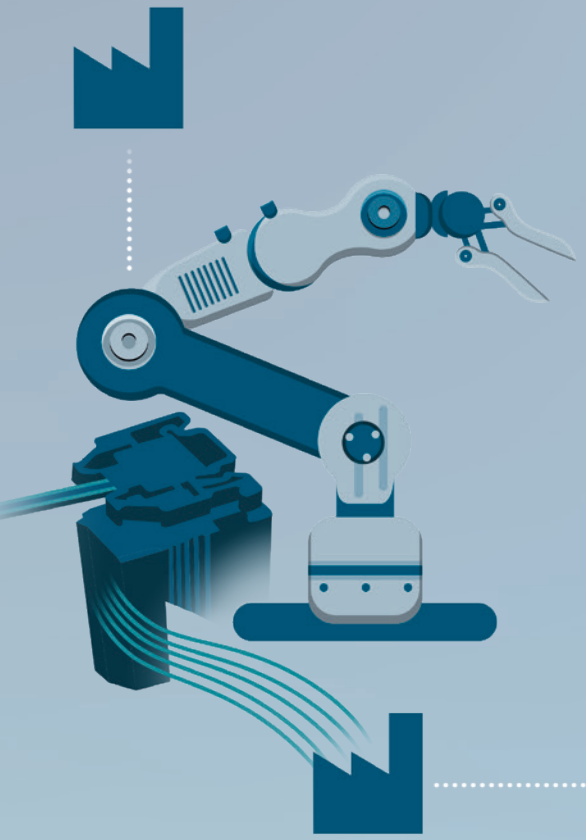
Tudor Soroceanu
Secure Systems Engineering
Tel. +49 89 32299 86-241
tudor.soroceanu@aisec.fraunhofer.de

Dr. Nicolas Müller
Cognitive Security Technologies
Tel. +49 89 3229986-197
nicolas.mueller@aisec.fraunhofer.de

Andreas Seelos-Zankl
Hardware Security
Tel. +49 89 3229986-186
andreas.zankl@aisec.fraunhofer.de

Cybersecurity Labs

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



INDUSTRIAL SECURITY LAB

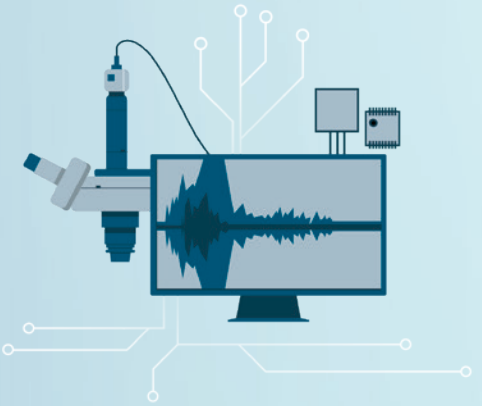
Das Angebotsspektrum des Industrial-Security-Labors reicht von Analysen für Industrie 4.0, Internet der Dinge und vernetzter Produktion bis hin zur Untersuchung der Sicherheit von Gebäudeautomation.

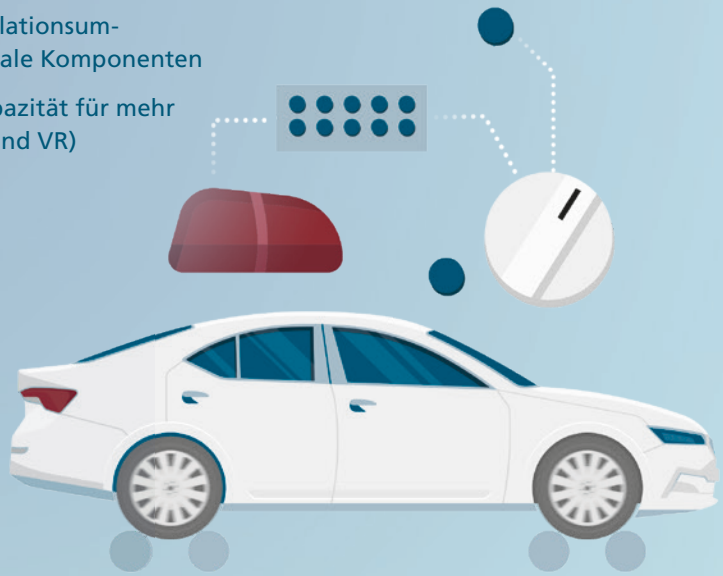
- Risikoanalysen und Penetrationstests
- Realitätsnahe Simulationsumgebungen durch reale Komponenten
- Erhöhte Rechenkapazität für mehr Simulationen (AR und VR)

HARDWARE SECURITY LAB

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

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



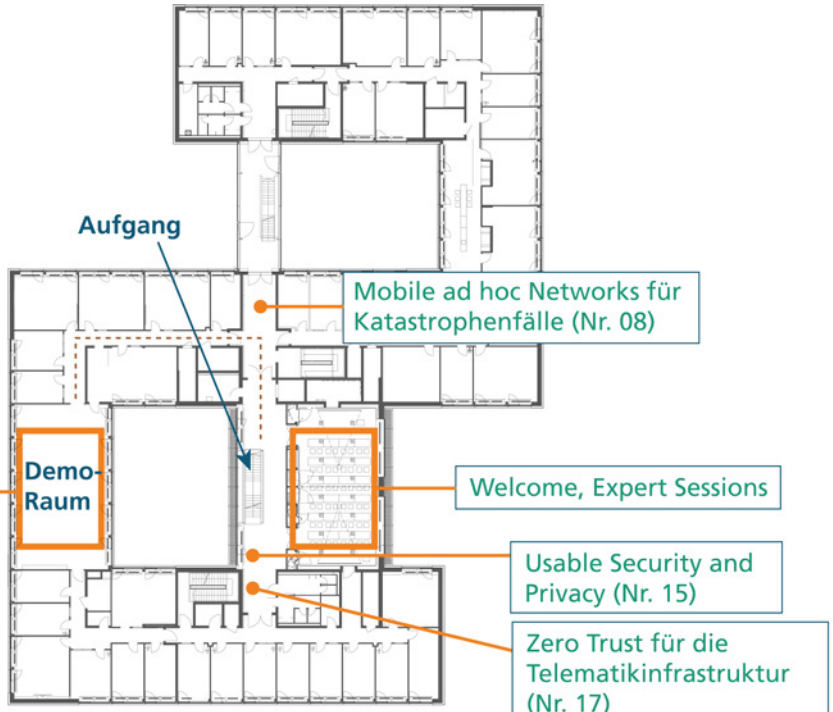


AUTOMOTIVE SECURITY LAB

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

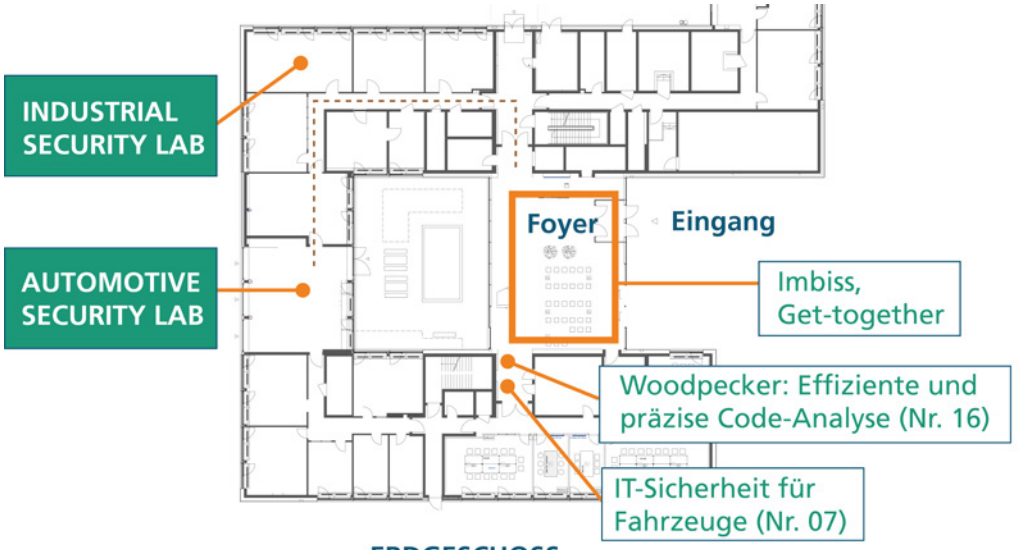
- Risikoanalysen und Penetrationstests
- Security Engineering und Methoden für die Fahrzeugentwicklung
- Entwicklung und Tests von Security-Maßnahmen
- Zertifizierte Umgebung nach TISAX Assessment Level 3

Übersichtsplan



1. OBERGESCHOSS

- Edge Cloud Continuum (CCIT) (Nr. 04)
- Clouditor: Überwachung von Cloud-Systemen (Nr. 03)
- Remote Attestation: Plattformintegrität evaluieren (Nr. 10)
- BlackBoxCam (Nr. 01)
- Resilienz für eingebettete Systeme (Nr. 11)
- Pay per Scan: Durch vertrauenswürdige Logistikketten neue Geschäftsmodelle erschließen (Nr. 09)
- Bug Hunting with Memory Safety: Weniger Fehler im Programmcode (Nr. 02)
- Deepfakes: Audio-Dateien auf ihre Authentizität prüfen (Nr. 05)
- Sichere Datenräume (Nr. 14)
- Robustheitsbewertung von neuronalen Netzen (Nr. 12)



ERDGESCHOSS

2. OBERGESCHOSS

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