Fraunhofer Institute for Applied and Integrated Security AISEC | Annual Report 2023

Fraunhofer
AISEC

Annual Report 2023

Innovating with security

#innovatingwithsecurity

Annual Report 2023

Fraunhofer Institute for Applied and Integrated Security AISEC

*Prof. Dr. Claudia Eckert,
Executive Director of the institute*

*Prof. Dr. Georg Sigl,
Institute Director*

Welcome to Fraunhofer AISEC!

Dear reader,

Threats in cyberspace reached new peaks in 2023, with vulnerabilities in software and hardware products being more widely exploited than ever before, attack methods becoming more sophisticated and the threat posed by ransomware continuing to be a cause for concern. Despite this, we have made significant progress in defense and protection. Fraunhofer AISEC's mission is and remains translating excellence in IT security research into applied solutions for greater dependability, trustworthiness and tamper protection in IT-based systems and products. With this in mind, in 2023 Fraunhofer AISEC developed new solutions for a secure digital transformation — covering everything from the secure use of key technologies such as artificial intelligence, secure autonomous driving, platform security, trustworthy data processing and cloud monitoring to secure, future-proof networks and cryptographic protocols for quantum-secure digital identity verification.

Our work has been primarily centered around pre-competitive research in the areas of trusted hardware, generative AI, the cloud, digital identity and embedded security. We have been focusing on expanding established solutions and skills — by creating security concepts and risk analyses, for example, and performing offensive tests. We have shared our current research findings with practitioners and numerous professional groups through research projects with companies, public authorities and institutions, as well as through the training we offer at the Cybersecurity Training Lab. In order to address the challenges found in cybersecurity, it is, after all, essential to engage as many stakeholders as possible to establish a strong culture of security.

In this Annual Report, we hope to give you an insight into our activities in 2023 and illustrate how we can participate securely in pioneering technologies.

We hope you enjoy reading it!

Best regards,

Prof. Dr. Claudia Eckert Prof. Dr. Georg Sigl

Claudia Eckert Georg Sigl

Contents

Autonomous Truck Takes to the Highway

Driverless trucks transporting goods autonomously from one logistics yard to another is a scenario that has great potential, but comes with cybersecurity risks in the form of unauthorized parties commandeering the autonomous vehicle and forcing it to make life-threatening decisions. Fraunhofer AISEC is harnessing its cybersecurity expertise and testing capabilities in the development of future mobility solutions to ensure that the logistics sector adopts secure automation concepts.

Named ATLAS-L4 (Automatisierter Transport zwischen Logistikzentren auf Schnellstrassen im Level 4, meaning Automated Transport Between Logistics Centers on Highways, Level 4), the research and development project is drawing on expertise from science, industry and infrastructure operators to form the basis for innovative transport concepts. The aim is to introduce autonomous trucks onto the highway for the first time by the middle of this decade.

In a joint research project funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK), Fraunhofer AISEC is working with MAN Truck & Bus, Knorr-Bremse, Leoni, Bosch, Fernride, BTC Embedded Systems, the Technical Universities of Munich and Braunschweig, TÜV SÜD, Autobahn GmbH and WIVW GmbH to develop an industry-ready concept for putting Level 4 automated trucks on the highway. Level 4 is the stage preceding fully autonomous driving, in which the vehicle’s system is able to take over most of the control. The project partners have been designing and testing the subsystems, sensors, vehicle electrical system, steering and braking system since January 2022. The control center in charge of technical supervision is also up and running. In 2023, the prototype vehicle successfully traveled its first few kilometers, starting on the test track and then moving to the highway.

End-to-end protection against cyber attacks

With ATLAS-L4, Fraunhofer AISEC is ensuring that comprehensive, traceable security requirements can be met. The security experts from the Product Protection and Industrial Security department carried out the risk analysis for the autonomous driving system in collaboration with MAN. For this purpose, they broadened their methods for security risk analyses to encompass automated trucks. The next stage involved defining security measures such as authentic and encrypted communication, plus functional security measures such as redundancy and degradation concepts, for the autonomous driving system. These measures are crucial for responding to cyber attacks with resilience, maintaining system integrity and ensuring road safety.

Safe operation on highways

Also in the process of being created are comprehensive security management concepts that take into account other aspects of the vehicle’s life cycle besides its development — for example, production and operation. These will be refined as the project progresses and implemented in t he form of a toolbox. Researchers will be able to use them as a means of identifying and addressing cybersecurity risks and requirements throughout the entire life cycle of the vehicle. Fraunhofer AISEC is also creating the risk analysis and protection concept for the control center as part of ATLAS-L4. This will cover all aspects of cybersecurity for Level 4 automated trucks and establish an industry-ready standard for operating them safely on highways.

Automotive Security at Fraunhofer AISEC

Fraunhofer AISEC is using its extensive expertise and analysis capabilities to assess and protect the security of vehicles and their communication systems. Dealing with everything from developing secure control units, vehicle electrical system architectures and Car-to-X (C2X) systems through to security measures for vehicle electronics and procedures for secure remote software updates, the Product Protection and Industrial Security department is advancing the state of the art in automotive security through its research. It is also supporting the development, implementation and integration of secure vehicle functions, applications and value-added services.

Contact

Bartol Filipovic
Head of the Product Protection
and Industrial Security department
Phone +49 89 3229986-128
bartol.filipovic@aisec.fraunhofer.de

Further information

ATLAS-L4 project

Product Protection and Industrial Security department

Cloud Security With Approval for the Future

Clouds are scalable, cost-effective and flexible — but are they secure? Cloud providers have been prioritizing security at least since the EU Cybersecurity Act came into force. The law sets out the EU Cybersecurity Certification Scheme for Cloud Services (EUCS) in the form of a European security criteria catalog.

Achieving cloud certification with MEDINA

Fraunhofer AISEC has been contributing its expertise to the EU-funded MEDINA project to make it easier for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) cloud providers to obtain EUCS certification in the future. The project's international consortium, drawn from science and industry, has developed a modular kit to make compliance with future EUCS requirements — and, consequently, the security of clouds — continuously and automatically quantifiable. "The tools and processes developed in the MEDINA project enable cloud providers to check whether they meet all compliance requirements — and, if necessary, to make improvements — without having to perform lengthy and cost-intensive manual searches to find evidence," explains Christian Banse, Head of the Service and Application Security department at Fraunhofer AISEC.

Collecting and evaluating evidence with Clouditor

The assurance tool Clouditor from Fraunhofer AISEC is an open-source tool that automatically and continuously checks that cloud-based services and applications are securely configured, specifically with regard to security aspects such as encryption, identity and access management, and logging. The research team at Fraunhofer AISEC has expanded the evaluation to include EUCS-relevant data sources, such as internal company compliance requirements, policies and software applications, to ensure that evidence of compliance with EUCS requirements is collected and evaluated automatically. The researchers translated the EUCS regulations into technical rules that Clouditor can use to automatically evaluate evidence and assign a certification status. This allows cloud providers to identify whether they meet all requirements or whether they need to take further action to obtain EUCS certification.

EUCS-compliant software with Codyze

Fraunhofer AISEC uses the AISEC analysis tool Codyze in the MEDINA project to assess software compliance. Codyze automatically identifies violations of EUCS requirements in software source code. It uses static code analysis in C, C++ and Java to ensure that the software in the cloud system correctly implements cryptographic protocols such as TLS and data encryption. As well as this, it ensures that APIs comply with the defined standards and that only trustworthy code is used. This means that compliance violations and vulnerabilities can be identified and rectified early on. "It is our goal to provide companies and institutions with the right tools for checking and strengthening their security efficiently, based on what works for their specific scenarios," explains Angelika Schneider, research scientist in the Service and Application Security department. "The technologies developed as part of the MEDINA project are helping industry and the public sector make their cloud services more secure and prepare for future challenges." Fraunhofer AISEC is using the results from the MEDINA project in the EU-funded follow-up projects EMERALD and COBALT. EMERALD is focusing on Certification-as-a-Service (CaaS) solutions in cloud environments, while COBALT is establishing a cross-domain certification model.

Automated Evaluation of Security and Privacy

Data sovereignty is a fundamental attribute in an industrial sector that is focused on the future. Fraunhofer AISEC's open-source tools enable companies and public institutions to establish secure data exchange and resilient, distributed systems based on automated security analyses and evaluations.

MEDINA project

Clouditor website

Codyze website

Service and Application Security department

Contact

Christian Banse
Head of Department
Service and Application Security
Phone +49 89 3229986-119
christian.banse@aisec.fraunhofer.de

Reliably Exposing Audio Deepfakes

The Deepfake Total platform developed by Fraunhofer AISEC uses artificial intelligence to identify audio deepfakes. The platform also provides information and materials to raise awareness of deepfakes alongside data sets for training and evaluating AI-based audio deepfake identification models.

Deepfake Total platform

Cybersecurity in the Generative AI Era

In the AIgenCY project, leading experts from science and industry are researching the implications that generative artificial intelligence (AI) has for cybersecurity. The feasibility of generative AI technologies is tested in real-world scenarios in the Fraunhofer AISEC experimental lab.

AIgenCY project

Cognitive Security Technologies department

Contact

Dr. Philip Sperl
Head of Department
Cognitive Security Technologies
Phone +49 89 3229986-141
philip.sperl@aisec.fraunhofer.de

Dr. Konstantin Böttinger
Head of Department
Cognitive Security Technologies
Phone +49 89 3229986-163
konstantin.boettinger@aisec.fraunhofer.de

Artificial Intelligence and IT Security

Artificial intelligence is becoming increasingly powerful, something that presents cybersecurity with opportunities and risks. Researchers at Fraunhofer AISEC are closely scrutinizing the technology involved in artificial intelligence, investigating how AI can be used in cybersecurity and how to protect AI systems from attacks. One particular focus is on new developments in the field of generative AI.

In 2023, the astounding capabilities of generative AI dominated discussions on digital technology. Large language models (LLMs) such as generative pre-trained transformers (GPTs) stood out in particular. These language models identify statistical correlations from text documents in a computationally intensive training process and then generate new texts independently. The AIgenCY project, launched in 2023, is exploring the opportunities and risks that generative AI presents for cybersecurity by devising forecasts relating to the use of generative AI over the next three years. AI and cybersecurity experts from Fraunhofer AISEC, CISPA, TU Berlin, FU Berlin and the Heidelberg-based AI start-up Aleph Alpha came together to work on this project in 2023. It is being funded by the German Federal Ministry of Education and Research (BMBF).

Defending against AI attacks on vehicles

There has been a rise in the popularity of AI among cybersecurity experts, and not just since the advances in generative AI. It is bringing about a number of major changes in IT security. While AI can be used to improve IT security — through anomaly detection using automated analysis of large data sets, for example — it is also vulnerable to attack. Algorithms can be tricked by entering incorrect data, known as adversarial examples. Vehicles, which are increasingly being equipped with AI, are a prime real-world example of this, as attackers can deliberately try to deceive systems in order to gain control of the vehicles. This can lead to risks that have serious safety ramifications. The Cognitive Security Technologies department has developed a tool that can be used to assess the risk of new attacks and prioritize defense strategies, with the aim of establishing a quick and reliable overview of new attack vectors and methods.

Detecting deepfakes with AI

The ambivalence surrounding AI in cybersecurity is mirrored in the topic of deepfakes — deceptively realistic video and audio simulations that are generated using deep neural networks. “The risks and challenges posed by deepfakes are considerable, not just for the media, but also for companies and individuals,” says Konstantin Böttinger, Co-Head of the Cognitive Security Technologies department. Luckily, AI also offers a way to reliably expose deepfakes. In 2023, Fraunhofer AISEC launched the Deepfake Total platform, which uses AI to recognize audio deepfakes.

The performance of AI is always heavily reliant on the quality of the training data. In response to this challenge, the Cognitive Security Technologies department conducted research into the integrity and reliability of AI data sets for the companies Bundesdruckerei and Logsight throughout 2023 as part of the Datenatlas project. The team developed concepts for maintaining, analyzing and cleansing data to ensure that AI training data is high-quality and meets ethical and safety requirements.

Vulnerable Hardware: The Achilles Heel of the Internet of Things

Microelectronics are at the very core of smart devices — from industrial and consumer products to critical infrastructures. Manufacturers of IoT products often resort to standard hardware due to costs and a lack of risk awareness, with little thought given to security during product development. This makes them easy targets for attackers.

Putting the security of microcontrollers under the microscope

Hardware security researchers at Fraunhofer AISEC have demonstrated the vulnerability of IoT devices in the study "Hardware Attacks against Microcontrollers," commissioned by the German Federal Office for Information Security (BSI). Almost all of the microcontrollers examined in the study were susceptible to hardware-based attacks, such as:

- Fault attacks on internal processes caused by voltage and clock glitching (i.e., interruptions in the execution of machine commands) or electromagnetic fault injection
- Side-channel attacks based on energy consumption or electromagnetic emissions
- Bypass attacks on read-out protection via weak points in communication interfaces

The researchers at Fraunhofer AISEC have not only provided proof of the vulnerability of chips to attacks — in their study, they have also recommended targeted protective measures to prevent these attacks.
One possible approach is to use simulations as a way of identifying the vulnerability of the code to fault attacks and automatically inserting countermeasures at the vulnerable points. The protective measures can be implemented using software, without the need for any changes to the hardware.

Turning a vulnerability into a security solution

The research results highlight the need to focus more on hardware security. This is why Dr. Matthias Hiller, Head of the Hardware Security research department, is focusing his attention on security analyses in the laboratory, the protection and integration of microcontrollers and secure elements, and the secure use of system-on-chips and hardware interfaces such as field-programmable gate arrays (FPGAs). The expertise and experience of his team, plus specially developed analysis and test tools, are supplemented by Fraunhofer AISEC's Common Criteria EAL7-certified Hardware Security Lab, which meets the requirements for developing trustworthy hardware. There, Fraunhofer AISEC researchers extensively examine complex system-on-chip systems for vulnerabilities, design individual security solutions and test the effectiveness of these directly on the chip. Hiller explains: "As research and application are tightly interwoven, our findings are fed directly into practice. This enables us to work with our partners to systematically evaluate, design and maintain the security of hardware throughout the entire product life cycle — something that is absolutely essential, especially within the context of the EU Cyber Resilience Act."

Certified Hardware Security Lab

In the Hardware Security Lab, security researchers at Fraunhofer AISEC expose security flaws in hardware and develop appropriate protective measures.

The Hardware Security Lab has achieved Common Criteria site certification at the highest security level, EAL (Evaluation Assurance Level) 7. This certification confirms that the test laboratory and the infrastructure fulfill all the requirements of various standards: ISO/IEC 15408-1:2009, -2:2008, -3:2008 and the Common Criteria for Information Technology Security Evaluation (CC).

Hardware Security Lab flyer

Contact

Dr. Matthias Hiller
Head of Department
Hardware Security
Phone +49 89 3229986-162
matthias.hiller@aisec.fraunhofer.de

Further information

"Hardware Attacks against Microcontrollers" study

Hardware Security department

Cryptographic Protocol for Quantum-Secure Passports

The security chips found on personal identity cards and passports are under threat from quantum computing. In 2023, as part of its PoQuID research project, Fraunhofer AISEC's Competence Center for Post-Quantum Cryptography developed cryptographic protocols that are tough enough to withstand attacks waged by quantum computers. The companies Infineon and Bundesdruckerei were partners in the project.

Electronic chips have been providing security for Germany's EU passports since 2005 and for the country's personal identity cards since 2010. German citizens can use the latter to authenticate themselves online (using what is known as the online ID function). A chip stores personal data and biometric features including a person's passport photo and two of their fingerprints, and also features proof of its own authenticity. However, the cryptography that chips currently include will not be able to stand up to the attacks from the powerful quantum computers that are expected over the next ten to fifteen years — it is believed that these computers will have the ability to solve the mathematical problems underpinning this cryptography much quicker than today's computers can. In this scenario, chips would no longer serve as an effective security feature.

A two-second security check

With this in mind, the Fraunhofer AISEC Competence Center for Post-Quantum Cryptography set out to develop a quantum-secure chip in its PoQuID research project. The companies Infineon and Bundesdruckerei were partners in the project, which was funded by the German Federal Ministry for Economic Affairs and Climate Action (BMWK). "We adapted and refined Extended Access Control (EAC), the standard cryptographic protocol used in passports, in a way that ensured it would be quantum-resistant and still able to perform well with the limited resources available from a security chip," explains Prof. Dr. Marian Margraf, co-head of the Competence Center for Post-Quantum Cryptography.

"Our research work showed that the new protocol delivers the same security functions as its predecessor. It takes just two seconds of calculation time to check the security feature, making it suitable for both electronic passports at border controls and the online ID function."

"The research project has laid the foundations for ensuring that the security of electronic ID documents is fit for the quantum computer age. Now, the race is on to get the technology to market," says Margraf. The researcher believes that the international standardization process will take at least five years. "Additionally, authorities responsible for ID documents and security chip manufacturers have to bear in mind that ID documents can be valid for as much as ten years, but the first powerful quantum computers are expected to come onto the scene by the mid-2030s."

Contact

Prof. Dr. Marian Margraf
Head of Department
Secure Systems Engineering
Phone +49 89 3229986-152
marian.margraf@aisec.fraunhofer.de

Competence Center for Post-Quantum Cryptography

The Competence Center for Post-Quantum Cryptography offers bespoke consultation services and assistance with migration to quantum-resistant architecture designs, security analyses of PQC implementations and an information portal on post-quantum cryptography.

Competence Center for Post-Quantum Cryptography

"Post-Quantum Security" Seminar

At the in-person "Post-Quantum Security" seminar at the Cybersecurity Training Lab, participants will acquire in-depth knowledge of how a quantum computer works and an overview of the challenges facing IT security.

"Post-Quantum Security" Seminar

Contact

Prof. Daniel Loebenberger
Head of Department
Secure Infrastructure
Phone +49 89 3229986-139
daniel.loebenberger@aisec.fraunhofer.de

Further information

PoQuID project

Security for Operating Systems and Hardware-Facing Software

The Secure Operating Systems department analyzes and develops secure software architectures and methods for protecting system integrity, ensuring resilience and isolating critical components and data.

Its research focuses on the evaluation and development of secure embedded systems. This includes confidential computing, software security and hardening, fuzz testing and code analysis, plus developing security measures and core technologies as open-source software for the mobile, embedded systems, edge computing, server and cloud domains.

Contact

Sascha Wessel
Head of Department
Secure Operating Systems
Phone +49 89 3229986-155
sascha.wessel@aisec.fraunhofer.de

Further information

GyroidOS website

Secure Operating Systems department

GyroidOS: A Secure Virtualization Solution for Data Storage, Processing and Communication

Whether it involves edge computing, artificial intelligence or the IoT, storing, sharing and processing data are essential parts of the digital value chain. Companies are facing the challenge of protecting the integrity, confidentiality and availability of data. This is where GyroidOS comes in.

Developed by Fraunhofer AISEC, GyroidOS is a virtualization solution at operating system level that has a special emphasis on IT security. The underlying Linux operating system kernel gives GyroidOS independence with regard to processor architectures. The solution is based on hardware functions that enable secure container isolation and the creation of lightweight, flexible execution environments that are also suitable for processing classified data.

Protecting data by isolating user contexts

Data is also protected by the special system architecture of GyroidOS. Especially sensitive applications and data are deployed in execution environments that are isolated from the core container and are therefore privileged. In addition to critical components such as remote maintenance and update functionalities, the core container houses the administrator system, which is exposed to attacks (including hacker attacks). Separating unprivileged application containers from the core container achieves a very high level of security. At this point, the core container is also unprivileged, but it has a defined interface for controlling the privileged virtualization layer.

Secure and confidential data collection, processing and communication

Complete hard disk encryption, secure booting with remote attestation, signing of components such as guest operating systems, kernels and modules, secure element support for two-factor authentication, and other security functions all help to protect data storage, processing and communication.

The open-source software can be used on numerous x86 and ARM platforms. GyroidOS also supports certification processes in accordance with the DIN SPEC 27070 and IEC 62443-4-2 industry standards. GyroidOS has been awarded the IDS-ready label as part of the Trusted Connector in the context of International Data Spaces. For Common Criteria certification, GyroidOS can be used as part of the product to be certified or as a Target of Evaluation (TOE). The security features of the software are suitable for implementing TOE Security Functions.

GyroidOS is a secure, highly configurable and flexible solution for executing isolated applications and services. Fraunhofer AISEC can provide support for implementing the open-source software and with customer-specific extensions to GyroidOS.

Security for Future-Proof Infrastructures

The Secure Infrastructure department at Fraunhofer AISEC in Weiden supports customers in applied cryptography, in migrating to quantum-secure architecture designs and in investigating and designing secure network protocols.

Secure Infrastructure department

Secure and User-Friendly Digital Systems

The research conducted by the Secure Systems Engineering department at the Fraunhofer AISEC site in Berlin focuses on the development of digital systems with security, data protection and user-friendliness in mind. The security architectures it develops support companies with certification in accordance with eIDAS, BSI-TR, ISO 27000 or Common Criteria.

Secure Systems Engineering department

Telematics infrastructure press release

Contact

Prof. Daniel Loebenberger
Head of Department
Secure Infrastructure
Phone +49 89 3229986-139
daniel.loebenberger@aisec.fraunhofer.de

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

Greater Data Security With Zero-Trust Access Control

Successful cyber attacks or the accidental disclosure of confidential data by internal users can have serious consequences for companies. The zero-trust concept is a data-centric approach that scrutinizes every data access request.

"Zero trust" denotes a security concept that does not have an internal trustworthy area or any default assumptions of trust where users, devices and networks are concerned. Every attempt to access resources is verified. Resource authentications and authorizations are based on a dynamic set of rules that are enforced before data is accessed. This allows users to establish communication without being restricted by their location or company network. By closely scrutinizing and monitoring all data access requests, companies can adhere to compliance requirements more easily and improve their own security levels.

Implementing zero trust requires consideration of the company's existing IT infrastructure as well as careful planning and execution. By developing application-led security solutions based on the zero-trust concept, Fraunhofer AISEC is encouraging its adoption in practice. Designing a zero-trust-based secure communication system in the healthcare sector and evaluating zero-trust strategies in the Bavarian government network are examples of this research being applied in the real world.

Telematics infrastructure 2.0: secure communication in the healthcare sector

The telematics infrastructure (TI) is the central method of communication in healthcare contexts. Working together with Bundesdruckerei, CompuGroup Medical, genua GmbH and D-Trust GmbH in a project commissioned by gematik, Fraunhofer AISEC has developed the conceptual basis for TI 2.0 in order to make the TI secure and future-proof. A demonstrator has been developed for the new security architecture, alongside an architecture concept based on zero-trust principles and a migration plan. The feasibility of the architecture has been verified with a proof of concept. Uniform access mechanisms for all user groups ensure equal integration of all stakeholders and extend the user group to include insured persons and service providers without a fixed location. The key criterion for authorizing individual data access requests is that the end devices meet the necessary security requirements.

Evaluation of zero trust in a government network

Commissioned by the Bavarian State Office for Information Security (LSI), Fraunhofer AISEC has been investigating the extent to which zero trust has been implemented in the Bavarian government network and how the concept can help improve the security infrastructure. Tools have been developed to derive requirements and recommendations for zero-trust security. The evaluation of three use cases demonstrated that a zero-trust security concept provides resilient solutions for improving network security in government networks. The challenge is to ensure that the new zero-trust approach does not weaken highly segmented networks. For this reason, the project has identified the challenges involved in migration and integration into the existing network. The recommendations show how the zero-trust concept can be implemented in the network infrastructure in stages so that the advantages of zero trust can be fully leveraged in the future.

Transferring Knowledge From Research to Practice

As digitalization becomes more commonplace, the potential threat of cyber attacks is steadily on the rise. The Cybersecurity Training Lab is part of the Fraunhofer Academy training facility and helps companies and public authorities develop specific skills in IT security.

The Cybersecurity Training Lab at Fraunhofer AISEC specializes in the areas of embedded systems, the internet of things and mobile security. The training courses present current research outcomes and IT security methods in a concise and practical manner, and can be adapted to specific interests and needs.

Contact

Vivija Čeprkalo-Simić
Project Manager
Cybersecurity Training Lab
Phone +49 89 3229986-138
vivija.ceprkalo@aisec.fraunhofer.de

Further information

Fraunhofer AISEC Cybersecurity Training Lab

Fraunhofer ACADEMY

Security Comes From Expertise

As soon as one gap in security is closed, another one immediately appears. With the protection of IT systems constantly evolving in different ways, and the protection of data, knowledge and products along with it, companies and public authorities have no choice but to keep pace with developments in cybersecurity. But how do you stay one step ahead when specialists are in short supply?

Direct access to applied research findings

Researchers from Fraunhofer AISEC share current scientific findings and practical experiences in the Cybersecurity Training Lab, which is part of the Fraunhofer Academy. "Initial contact with the training facility is often established through research and development projects between Fraunhofer AISEC and partners from industry and the public sector," says Vivija Čeprkalo-Simić, Project Manager at the Fraunhofer AISEC Cybersecurity Training Lab. It also receives inquiries from new contacts about risk analysis, post-quantum cryptography (PQC), blockchain technologies, hardware security and machine learning (ML). "When it comes to topics such as advanced ML or PQC, we are asked to provide training that simply no one else can offer at such a technical level," explains Čeprkalo-Simić.

She establishes the learning objectives during the initial consultation — in other words, who needs to know what, whether certain subjects need to be addressed, whether practical security knowledge or a strategic understanding of a technology is required, and whether there is a need for a customized training concept. When developing the learning content, researchers and trainers work closely with teachers and experts in digital learning content. This ensures that applied research findings are presented in a way that is understandable and memorable.

IT security for specific challenges

The trainers teach what they are researching in the Cybersecurity Training Lab: for example, risk analyses for automotive manufacturers and mechanical engineers, quantum-secure cryptography for financial service providers, secure FPGA-based systems for the transport sector and machine learning for telecommunications. The latest research findings are presented in virtual seminars, web-based training courses, in-house training sessions or the security labs at Fraunhofer AISEC, then put directly into practice in practical simulations, training hardware or hacking sessions in which participants assume the role of the attacker.

The concept works, and many customers are interested in long-term collaborations. Every day is a school day, as they say, and that is certainly the case at the Training Lab.

Moving into the future with cyber resilience

In view of recent technological advances in AI and quantum computing, for example, experts need to be trained not only to make IT systems more resistant to attacks, but also to make them more resilient in the event that an attack is actually successful. Fraunhofer AISEC is involved in developing assessments and further training on cyber resilience in the cross-Fraunhofer project CyRille. Researchers are helping companies to further develop their products with the aim of recognizing and overcoming attacks. Companies need to learn how to remain operational even during an attack, how to maintain control of processes and products, and how to recover quickly from an attack. As Čeprkalo-Simić says, the Cybersecurity Training Lab is making it possible to transfer cyber resilience knowledge, tools and practices to companies and public administration.

Inaugural Cybersecurity Day — Research Meets Industry

A Cybersecurity Day was held at Fraunhofer AISEC for the first time in November. Our cybersecurity experts used demonstrators to present results and solutions derived from research and industry projects. Customers had the opportunity to visit our cybersecurity labs and learn about key IT security issues in short expert sessions.

To the event website

TU Munich Awards Heinz Maier-Leibnitz Medal to Prof. Dr. Eckert

At TUM's Dies Academicus ceremony, Prof. Dr. Claudia Eckert, Head of Fraunhofer AISEC, received the Heinz Maier-Leibnitz medal — TUM's most prestigious award — in recognition of her outstanding work on system and application security and on embedded systems. In her Chair of IT Security position at TUM, she specializes in the protection of IT systems. As a member of various national and international industrial advisory boards and scientific committees, she advises companies, trade associations and the public sector on issues relating to IT security.

Read the press release

"Türen auf mit der Maus" Open Day 2023

At the "Türen auf mit der Maus" open day at Fraunhofer AISEC, children between the ages of eight and fourteen were introduced to the world of cybersecurity for the first time. Across three stations, around a hundred guests in total had the opportunity to identify images and sounds created by artificial intelligence, crack a safe and learn the basics of quantum computers in a computer game called Charlie and the Quantum Factory.

To the event website

YOUR DOG'S NAME IS NOT A STRONG PASSWORD.
Strong passwords are long and use lower & upper case letters, numbers and special characters. They don't have any reference to keyboard patterns or personal details.
Fraunhofer AISEC
OFF TO AN ADVENTURE? ...LOCK YOUR SCREEN FIRST.
Fraunhofer AISEC
SMELLS PHISHY?
Fraunhofer AISEC
CYBERSECURITY STARTS WITH US
AN UPDATE A DAY KEEPS THE MALWARE AWAY.
Updates fix security flaws and protect you and our data. Check for updates regularly and run them.
CYBERSECURITY STARTS WITH US
Fraunhofer
TWO AR ETTER THAN ON
Two-factor authentication (2FA) adds an extra layer of protection to your account making it much harder to hack. Enable 2FA today.
CYBERSECURITY STARTS WITH US

COSADE 2023 at Fraunhofer AISEC

The International Workshop on Constructive Side-Channel Analysis and Secure Design (COSADE) has been providing science and industry with a platform for presenting current research findings since 2010. In 2023, TUM and Fraunhofer AISEC organized the 14th edition of this workshop series. Topics ranged from implementation attacks to efficient and secure HW/SW implementations, even touching on hardware-intrinsic security and automated tools.

To the event website

Fraunhofer AISEC Welcomes Singapore's Deputy Prime Minister

The issue of cybersecurity extends beyond national borders. Fraunhofer AISEC works closely with research institutions in Singapore to promote the exchange of information and open up new markets in Asia. The visit from high-ranking representatives of the Singaporean government and research community to the Garching site in June highlighted the importance of international cooperation and provided fresh impetus for joint research projects. The guests of honor from the spheres of government and research included the Singaporean Deputy Prime Minister and Coordinating Minister for Economic Policies, Heng Swee Keat, and CEO of the National Research Foundation Singapore, Beh Kian Teik.

Read the press release

Awareness of IT Security

The human element is a key factor in IT security. Fraunhofer AISEC has designed a poster campaign outlining the basic rules of IT security, with the aim of raising awareness of how to use IT systems responsibly. The information posters will help increase people's understanding of cybersecurity and are available to download free of charge.

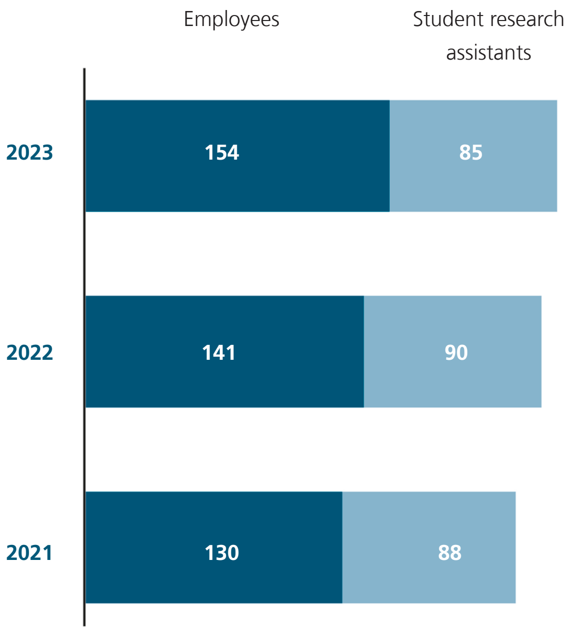
To the download

Our Mission: To Evaluate, Design and Safeguard Cybersecurity

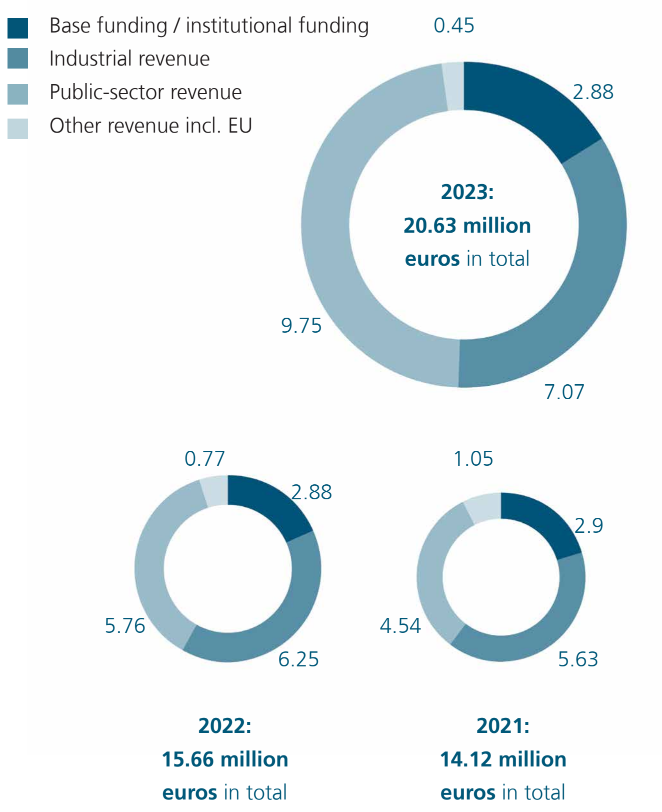
Fraunhofer AISEC translates excellence in IT security research into applied solutions for greater dependability, trustworthiness and tamper protection in IT-based systems and products.

Facts and Figures

Number of employees

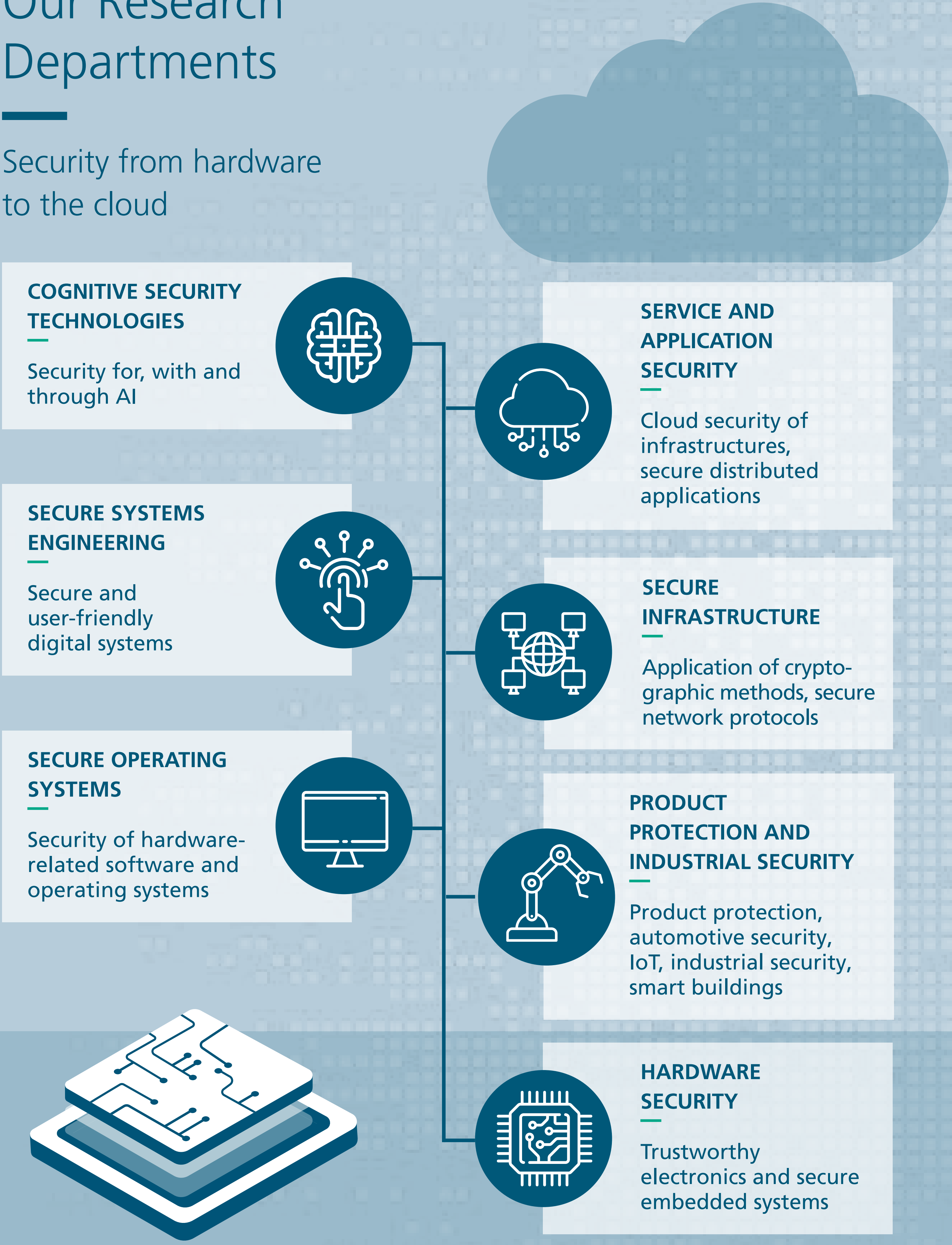


Research revenues (in millions of euros)



Our Research Departments

Security from hardware to the cloud



COGNITIVE SECURITY TECHNOLOGIES

Security for, with and through AI

SECURE SYSTEMS ENGINEERING

Secure and user-friendly digital systems

SECURE OPERATING SYSTEMS

Security of hardware-related software and operating systems

SERVICE AND APPLICATION SECURITY

Cloud security of infrastructures, secure distributed applications

SECURE INFRASTRUCTURE

Application of crypto-graphic methods, secure network protocols

PRODUCT PROTECTION AND INDUSTRIAL SECURITY

Product protection, automotive security, IoT, industrial security, smart buildings

HARDWARE SECURITY

Trustworthy electronics and secure embedded systems

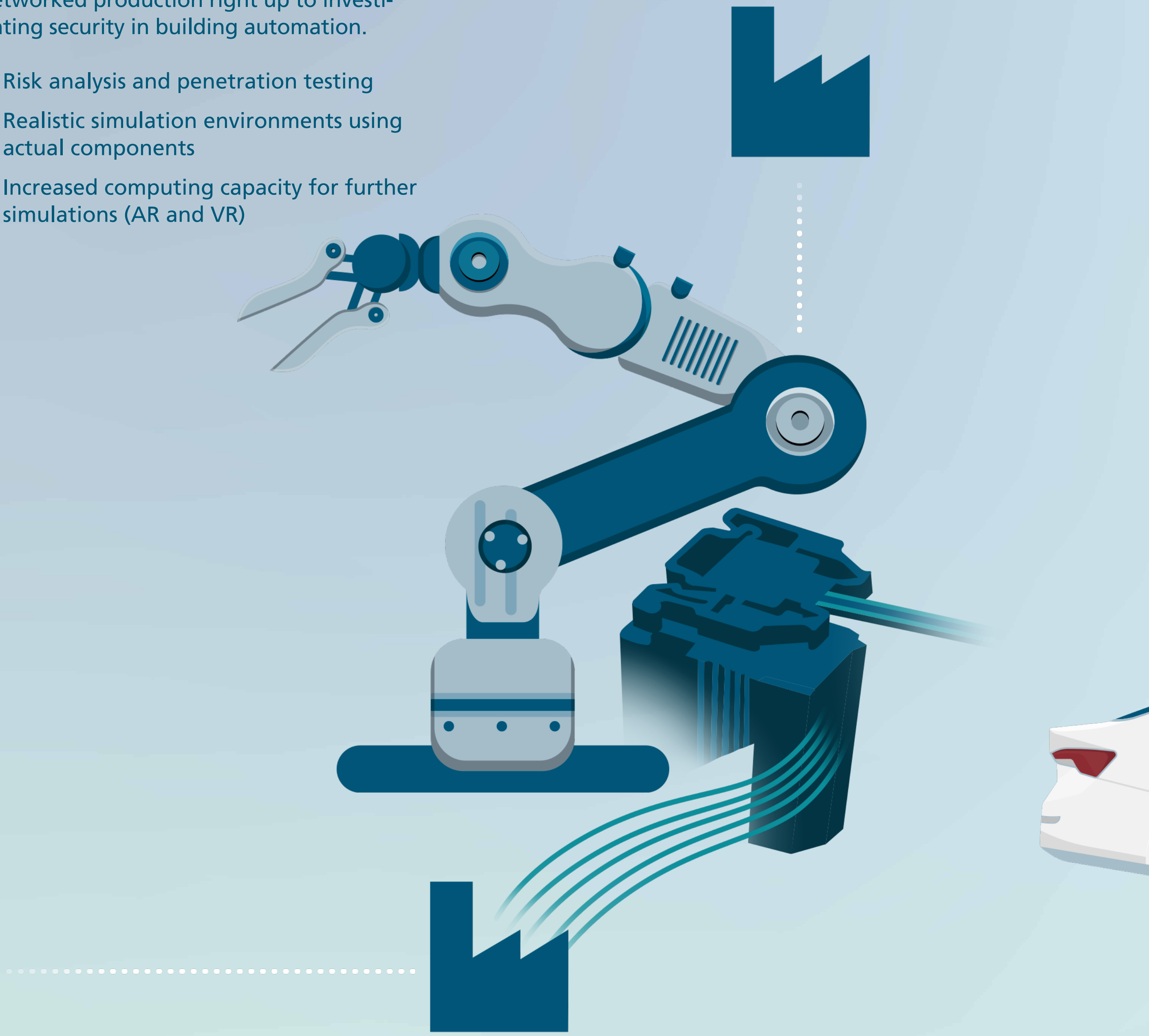
The World of Labs at Fraunhofer AISEC

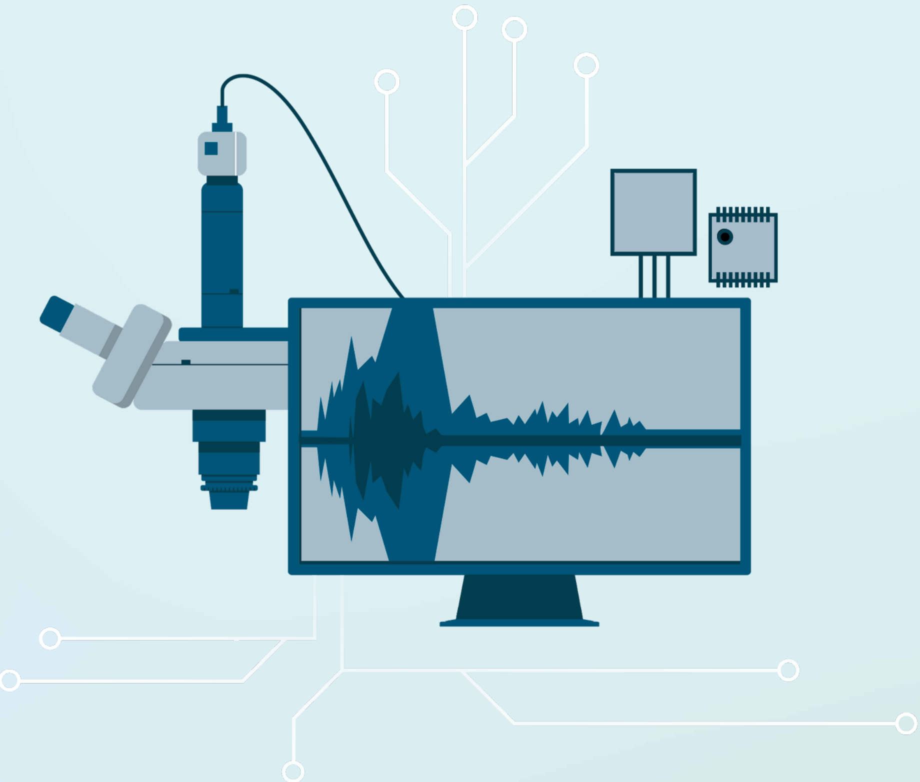
Tailor-made solutions based on research excellence

INDUSTRIAL SECURITY LABS

The spectrum of services offered by the Industrial Security Labs ranges from analyses for industry 4.0, the internet of things and networked production right up to investigating security in building automation.

- Risk analysis and penetration testing
- Realistic simulation environments using actual components
- Increased computing capacity for further simulations (AR and VR)

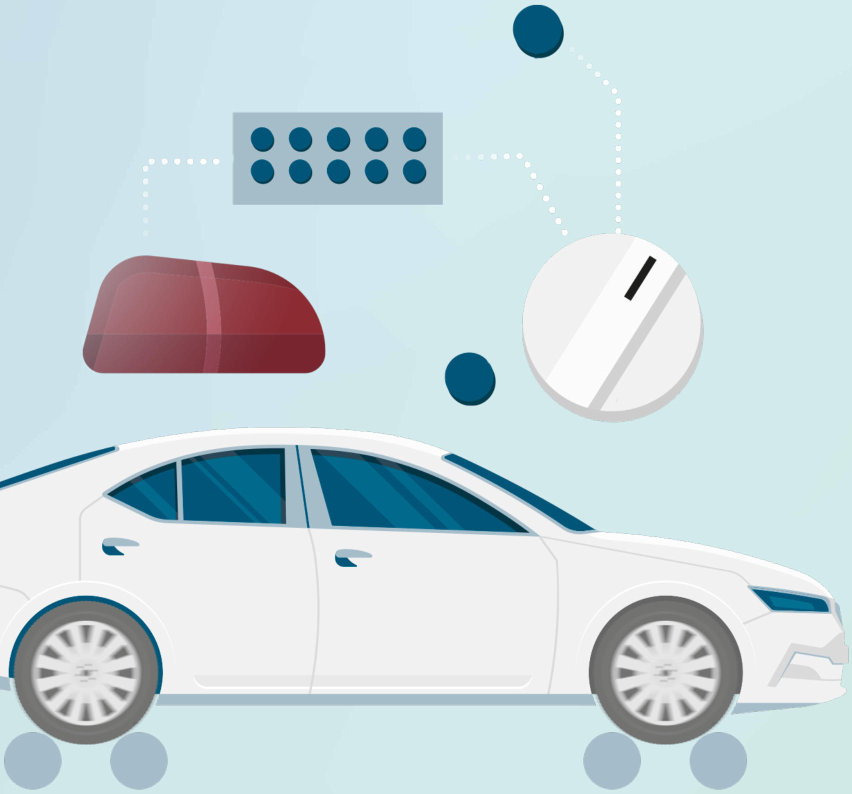




HARDWARE SECURITY LAB

The Hardware Security Lab offers a spectrum of hardware security analyses, ranging from penetration testing and side-channel analyses to attacks on security implementations.

- High-precision EM measurements for side-channel analysis
- Evaluating the security of embedded systems against hardware-based attack vectors
- Multiple laser stations for front- and backside fault injection
- Common Criteria site certification for EAL (Evaluation Assurance Level) 7



AUTOMOTIVE SECURITY LAB

The Automotive Security Lab enables security testing of complete vehicles and multiple, interacting components in a secure, trusted environment.

- Risk analysis and penetration testing
- Security engineering and vehicle development methods
- Development and testing of security measures
- Environment certified according to TISAX AL 3

Our Journey Toward Climate Neutrality

Fraunhofer AISEC is aiming to be climate-neutral by 2045. With this ambitious goal in mind, Iris Karabelas is pushing ahead with sustainability management in her role as Climate Neutrality and Sustainability Officer.

How close is Fraunhofer AISEC to becoming climate-neutral?

Iris Karabelas: We are on the right track. Our climate protection strategy requires us to record our greenhouse gas emissions annually. In 2022, we generated 911 tonnes of CO_2 equivalents. That's 4.03 tonnes of CO_2 per capita — which is low compared to companies of the same size and in the same industry. We are pleased with this figure, but the balance sheet also shows that our heat and electricity consumption and our hardware are responsible for the majority of our emissions.

In other words, it's clear where improvements could be made. What do you plan to do with these results?

Iris Karabelas: We have identified measures to reduce our carbon footprint and are now gradually putting them into practice. For example, we are now using 100% green electricity like the other Fraunhofer institutes. However, in the future, we also want to reduce our dependence on suppliers and produce our own green electricity via a photovoltaic system, as well as integrate district heating into our energy mix.

Apart from electricity and heating, what else is being done to offset emissions?

Iris Karabelas: Since emissions are generated even during our commutes to work, Fraunhofer AISEC encourages remote working, subsidizes public transport and supports the use of electric cars by providing its own charging stations. Sustainability standards are now an integral part of Fraunhofer's supplier contracts in order to reduce carbon emissions from outsourced services.

We are also committed to incorporating sustainability into our day-to-day operations. Since 2023, our dedicated employees in the AISEC Zero CO_2 Club have been launching climate-friendly initiatives such as switching to recycled paper and securely sharing the use of hardware. They are also raising awareness among their colleagues with campaign days on sustainable nutrition and mobility, for example, and taking other measures to promote the conservation of resources.

How does this commitment to climate neutrality affect customers?

Iris Karabelas: We are increasingly finding that sustainability is a key factor that our customers and partners consider in project applications and award processes. Our sustainability management system provides evidence that we can meet our customers' environmental requirements — for example, within the framework of the German Supply Chain Act (LkSG) or the globally recognized sustainability standard of the automotive industry (Sustainability Assessment Questionnaire, SAQ 5.0). This allows us to remain an attractive research partner and employer.

Contact

Dr. Iris Karabelas
Climate Neutrality and Sustainability Officer
Phone +49 89 3229986-1047
iris.karabelas@aisec.fraunhofer.de

Continuous Quality Management Ensures Adaptability

Scientific excellence, systematic improvement of processes and appropriate responses to changes and requests from our customers and partners are crucial factors in our success. They form the basis for continuous and effective quality management at Fraunhofer AISEC.

TISAX® (Trusted Information Security Assessment Exchange)

The automotive industry has defined standards for the confidentiality, availability and integrity of information. With TISAX®, the ENX Association is working on behalf of the German Association of the Automotive Industry (VDA) to provide support for the common acceptance of Information Security Assessments in the automotive industry. Working with the VDA's Information Security Assessment catalog, Fraunhofer AISEC has taken extensive measures in accordance with TISAX Assessment Level 3 to safeguard information with strict protection requirements, prototype components, parts and vehicles that require protection, and images of objects that require protection. It has received the TISAX Assessment Level 3 certificate.

TISAX®
RESULT AVAILABLE

Common Criteria site certification

The Common Criteria site certification is an international IT security standard for trustworthy software and hardware. Since 2024, Fraunhofer AISEC's Garching site has been one of a select number of laboratory infrastructures officially certified to perform assessments of hardware and software based on the Common Criteria standard. Fraunhofer AISEC has achieved Common Criteria site certification at the highest security level, EAL (Evaluation Assurance Level) 7. This certification confirms that the test laboratory and the infrastructure fulfill all the requirements of various standards: ISO/IEC 15408-1:2009, -2:2008, -3:2008 and the Common Criteria for Information Technology Security Evaluation (CC).

Common Criteria

ISO 9001:2015

Fraunhofer AISEC has been certified in accordance with the international quality management standard ISO 9001:2015 since December 2018. This demonstrates our performance abilities, efficiency and focus on service to our partners and customers in Germany and elsewhere. The high standard established in our approach to quality management is reflected in the excellent results achieved in past certifications awarded by TÜV SÜD Management Service GmbH.

TÜV SÜD ISO 9001
ISO 9001
Zertifiziertes Qualitätsmanagementsystem
www.tuev-sued.de/ms-zert

Our Advisory Board

Prof. Dr.-Ing. Georg Carle
Chair of Network Architectures and
Services, School of Computation,
Information and Technology,
Technical University of Munich

Dr. Astrid Elbe
Vice President Product Development,
Aviat Networks

Dr.-Ing. Stefan Hofschen
Spokesperson for the
advisory board and CEO,
Bundesdruckerei GmbH

Dr. Bettina Horster
Executive board
VIVAI Software AG

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

Andreas Könen
Former Director-General of Cyber
and Information Security,
German Federal Ministry of the
Interior and Community (BMI)

Prof. Dr. Dr. h.c. Mira Mezini
Head of Software Technology Group,
Department of Computer Science,
Technical University of Darmstadt

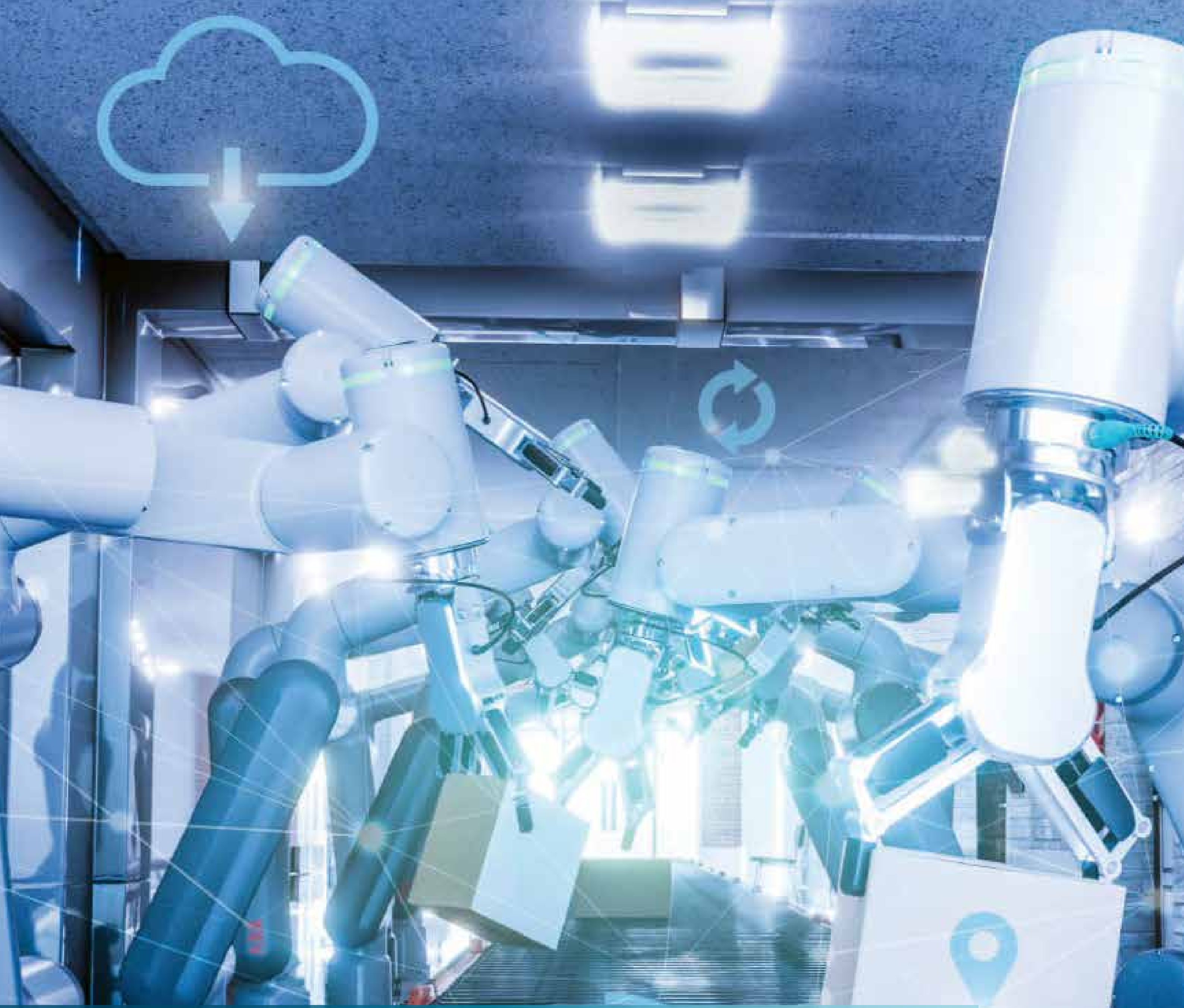
Dr. Manfred Paeschke
Chief Visionary Officer,
Bundesdruckerei GmbH

Dr.-Ing. Heike Prasse
Head of the Security and Networking
of Digital Systems department,
German Federal Ministry of Education
and Research (BMBF)

Thomas Rosteck
Division President Connected Secure
Systems, Infineon Technologies AG

Vera Schneevoigt
Managing Partner,
Guiding for Future GmbH

Dr. Stefan Wimbauer
Deputy Head of the Applied Research
and Cluster Policy department,
Bavarian Ministry of Economic Affairs,
Regional Development and Energy



Use case: state-of-the-art condition monitoring

Fraunhofer CCIT is demonstrating the added value that the edge-cloud continuum can bring to system monitoring through its AIQ-Bo (AI enhanced Intelligent Bolt) research project. A smart sensor detects vibrations on mechanical components in wind turbines or overhead cranes and reports anomalies to prevent damage and failures.

AI evaluates vibration data directly on the sensor at a local level, autonomously detects deviations from normal operation and reports these to the cloud. Computationally intensive tasks such as training the AI algorithm or adapting the model are carried out in the cloud, and the AI at the edge is updated from there. Pre-processing data directly in the edge device drastically reduces data transfer and makes the system extremely energy-efficient. The cloud has a proven track record of scalability and cost efficiency.

AIQ-Bo project

From Sensor to Cloud and Back Again: Technologies for the Digital Transformation

The internet of things (IoT) is fundamentally changing the demands being placed on technology. Relying exclusively on either decentralized data processing or network computing in remote data centers is not enough. New technologies that merge edge and cloud computing into one continuous data space are needed in order to leverage the full potential of the digital transformation. This will ensure that computing capacity can be used dynamically wherever it is most efficient.

Seamless data flow in the edge-cloud continuum

When processes need to be performed within a fraction of a second, computing power and storage space at the edge are used (i.e., in local sensors, machines or end devices). Data is analyzed, filtered or compressed in real time where it is generated. This minimizes delays, reduces the load on the network and ensures functionality even without an internet connection. On the other hand, tasks that are not dependent on time or are computationally intensive — such as simulations or AI algorithm training — are performed in the cloud, where storage space and computing power can be scaled and costs are manageable. This dynamic use of the edge and cloud takes place automatically, working on the basis of data volumes and requirements. Data space connectors, such as the Eclipse Dataspace Connector (EDC), are key to maintaining a dynamic flow of data within the edge-cloud continuum. They make it possible for data to be processed, retrieved and distributed sustainably in order to generate new knowledge.

Cutting-edge applied research from a single source

With Fraunhofer AISEC as the lead institute, the Fraunhofer Cluster of Excellence Cognitive Internet Technologies CCIT brings together cutting-edge applied research from multiple Fraunhofer institutes with the aim of advancing technologies focused on the edge-cloud continuum. These range from trustworthy IoT technologies for sensors and communication modules to intelligent and secure data spaces, and even innovative machine learning methods. “Fraunhofer CCIT’s customized solutions help companies make their processes and products ready for the future and fully exploit their innovation potential,” explains Michael Fritz, Head of Fraunhofer CCIT. In addition to technology development, the researchers at Fraunhofer CCIT provide comprehensive support for integrating individual components, ensuring smooth interaction between the edge and the cloud.

Contact

Michael Fritz
Head of central office,
Fraunhofer Cluster of Excellence
Cognitive Internet Technologies CCIT
Phone +49 89 3229986-1026
michael.fritz@aisec.fraunhofer.de

Further information

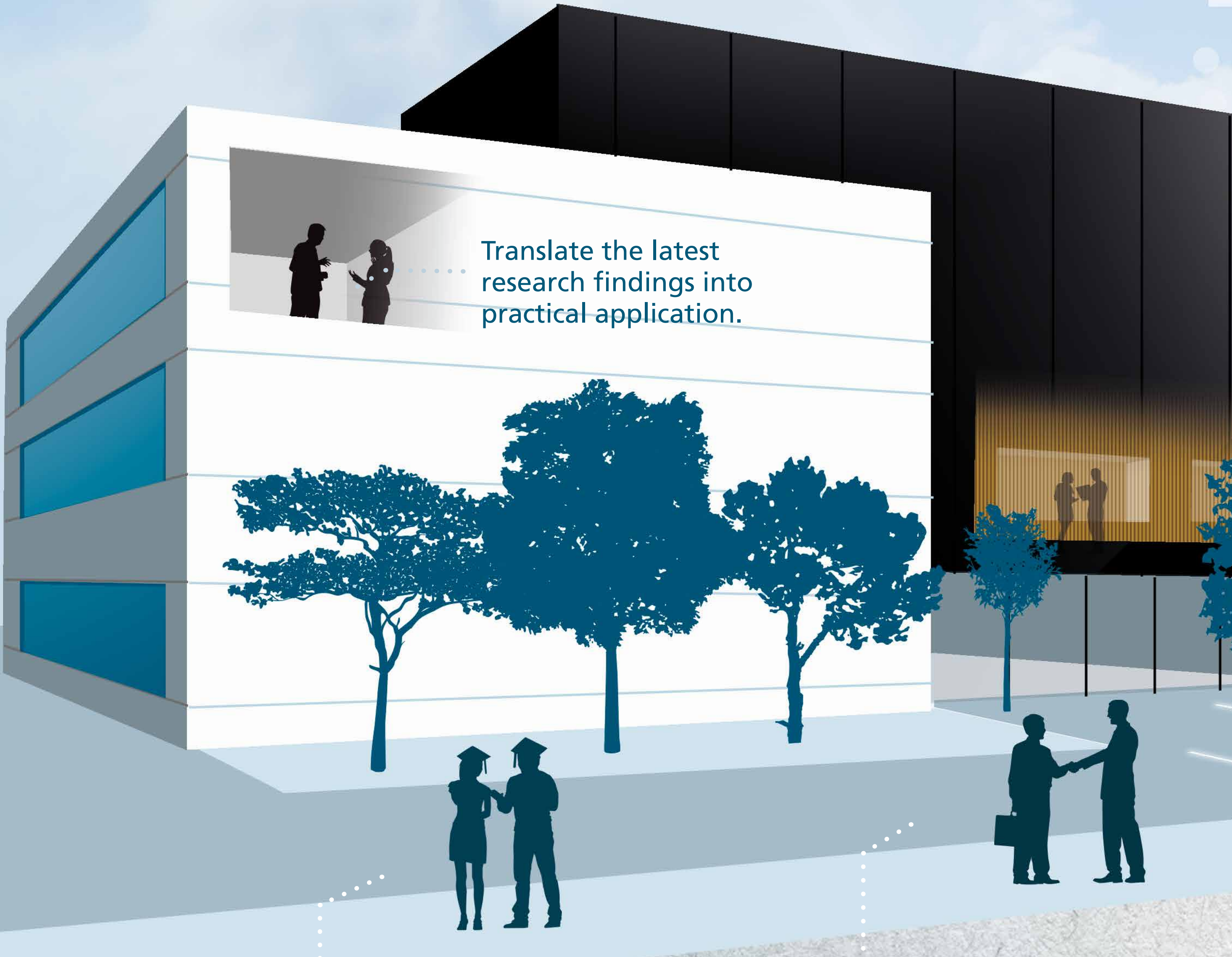
Fraunhofer CCIT website of Fraunhofer AISEC

Fraunhofer AISEC — A Great Place to Work

Ten reasons to work at Fraunhofer AISEC

Experience the diversity of cybersecurity research across various fields of application.

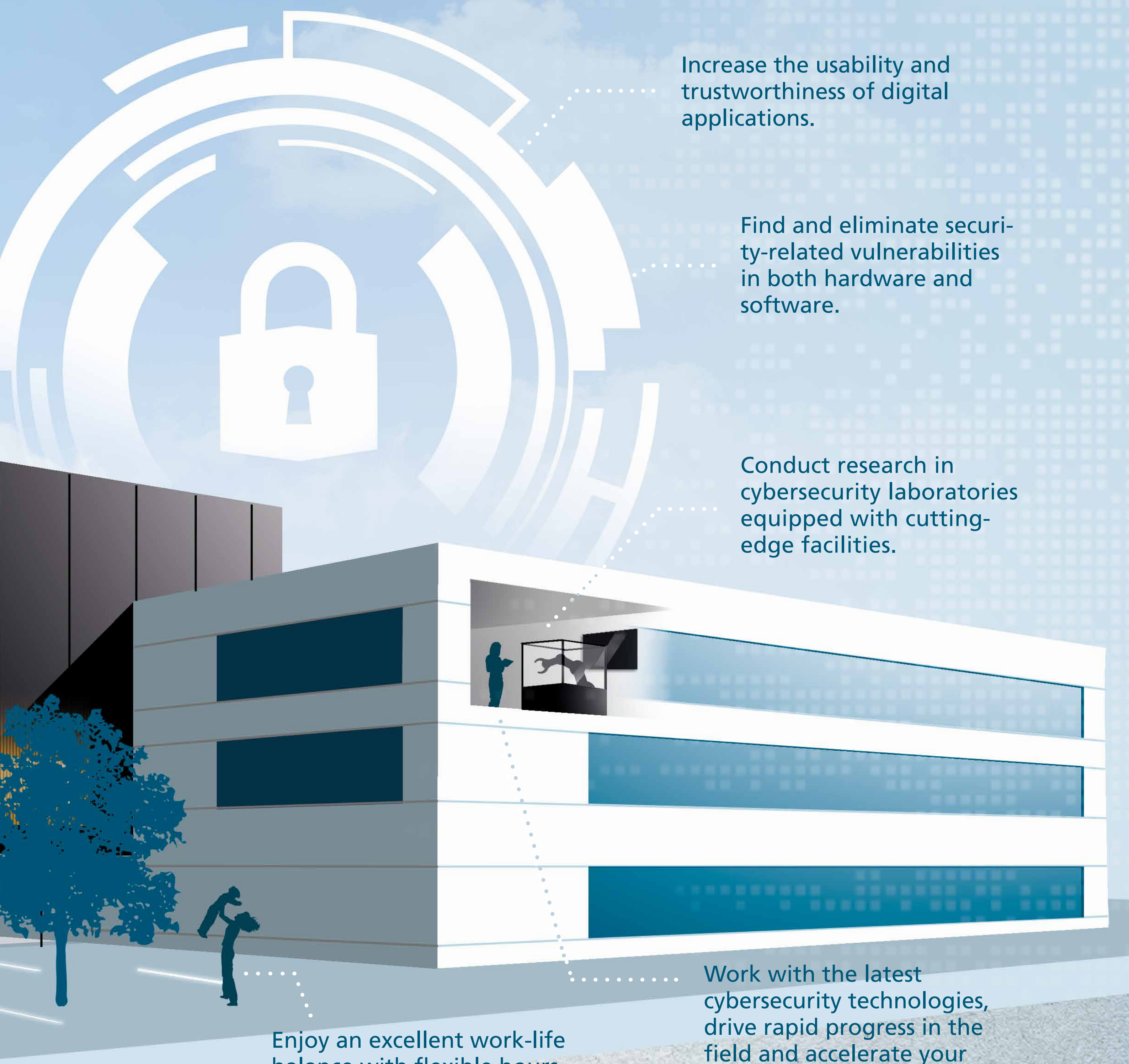
Work in a research field that's only growing in importance: cybersecurity.



Translate the latest research findings into practical application.

Gain practical experience while completing a doctorate in your chosen field.

Bring research and industry together and connect both worlds.



Increase the usability and trustworthiness of digital applications.

Find and eliminate security-related vulnerabilities in both hardware and software.

Conduct research in cybersecurity laboratories equipped with cutting-edge facilities.

Work with the latest cybersecurity technologies, drive rapid progress in the field and accelerate your own personal development.

Enjoy an excellent work-life balance with flexible hours and remote working.

Awards for Fraunhofer-Gesellschaft as an employer

1. PLATZ
Attraktivste Arbeitgeber
2023
Für Absolventen
Forschung
trendence

YOUNG PROFESSIONAL
Most Attractive
EMPLOYERS
GERMANY
universum
2023

STUDENT
Most Attractive
EMPLOYERS
GERMANY
universum
2023

glassdoor
BESTE
ARBEITGEBER
2022

Dr.-Ing. Nisha Jacob Kabakci

Head of the Physical Analysis and Countermeasures research group

> **"I am fascinated by cutting-edge hardware, especially FPGAs. Protecting them means looking beneath the surface, which is something I do: I scrutinize security properties, and I develop security strategies and make them safe to use in businesses and wider society."**

In Nisha Jacob Kabakci's hometown of Bengaluru, a major Indian city, many women can be found pursuing technical careers. On enrolling in the Bachelor's degree course in Electrical Engineering at Visvesvaraya Technological University, she received a great deal of support from her extensive family. After completing the course, her thirst for knowledge and global outlook brought her to Switzerland. She studied for a Master's degree in Embedded Systems at USI Università della Svizzera italiana in Lugano, where she became aware of cryptography in a lecture on IT security. As early as the second year of her Master's degree, she went on to complete a one-year internship at Nanyang Technological University (NTU) in Singapore, focusing on cryptographic methods and their implementation in microcontrollers. This also marked the first time she saw IT security in action.

"I saw the direct impact my work was having on protecting hardware systems — and the significant societal impact it had. That encouraged me to pursue a career in IT security," says Kabakci. She wrote academic papers, attended conferences and began actively seeking a job that would allow her to carry out her own research projects while gaining practical experience in IT security — and at Fraunhofer AISEC, she found exactly what she was looking for. She became a research assistant in the Embedded Systems Security department at Fraunhofer AISEC while working on her doctorate at TUM under Georg Sigl at the Chair for Security in Information Technology, which she successfully completed in 2020.

On a tour of discovery in the Hardware Security Lab

In her projects at Fraunhofer AISEC, she examines the security of embedded systems — especially integrated circuits such as field-programmable gate arrays (FPGAs) and FPGA systems on chips, uncovering vulnerabilities and developing measures to make them more secure and minimize risks. "My work is very varied, interesting and challenging all at the same time. I really value our open culture and the mutual support shown by colleagues," she says. As Head of the Physical Analysis and Countermeasures group, she advocates diversity, mutual listening and pursuing common goals.

At the Hardware Security Lab at Fraunhofer AISEC, she and her team investigate physical attacks, subjecting chips that are supposedly secure to side-channel analysis. This involves a probe reading electromagnetic pulses from the chip micrometer by micrometer and extracting its cryptographic key. In fault injection attacks, lasers are used to tamper with a chip so that it continues to make calculations based on false conditions. Glitching attacks that change the supply voltage or clock frequency by fractions of a second achieve the same results. Kabakci applies her knowledge of existing vulnerabilities to support customers and public institutions in the development of new security solutions. The Common Criteria certification of the Hardware Security Lab provides the right environment for innovative projects requiring a special level of protection. New workflows and tasks are emerging due to security measures relating to building technology and personnel. Kabakci is looking forward to new challenges and acquiring more insights to make hardware even more secure.

Ferdinand Jarisch

Doctoral student in the Product Protection and Industrial Security department

> **"Cybersecurity measures can only succeed if they are tailored to the system in question. This requires an understanding of the system and knowledge of its weak points, and that's exactly what my job at Fraunhofer AISEC involves."**

Ferdinand Jarisch studied physics at TUM. During his Master's degree, he specialized in quantum optics and seemed destined for a career in basic research. But then he discovered quantum cryptography during a lecture — and was immediately captivated. He was particularly interested in the role that quantum physics plays in the interception-proof exchange of keys as a means of securing communication. This was an area in which he was able to combine his passion for solving puzzles and doing system deep-dives with his interest in programming and coding. While he was still a student, he even scripted a program that reserved the best seats in the movie theater for preview screenings. As his studies progressed, he frequently participated in hacking contests such as capture-the-flag (CTF) events, and counted escape games and geocaching among his hobbies. Jarisch had found his calling: solving puzzles in the pursuit of cybersecurity. Next, he wanted to take this skill to a professional level — and that was when he discovered Fraunhofer AISEC.

Cybersecurity for the automotive and industrial sectors

Jarisch is directly involved in the latest developments and understands the challenges that customers in the automotive and industrial sectors are facing. He is currently researching the automated detection of vulnerabilities in embedded systems — big brains on a small scale that are playing an increasingly important role in the internet of things (IoT) and are at the heart of many intelligent devices, such as in those found in smart homes and smart factories. During penetration tests for the automotive sector, Jarisch and his colleagues immerse themselves in vehicle IT systems, trying to understand them and find weak spots such as the ability to tamper with the mileage display or bypass digital payment services. It is also important to consider that companies are constantly having to comply with new regulations, such as cybersecurity features being incorporated as early as the production phase. Jarisch keeps an eye on these requirements for his customers, tests vehicle prototypes before release and creates security concepts that ensure system designs are as secure as possible. This involves monitoring central digital vehicle technologies — including applications, communication with the manufacturer's backend or communication between vehicles and their environment.

Since 2018, he has been conducting a study on product piracy for the German Mechanical Engineering Industry Association (VDMA). This has delivered important insights into how companies can protect themselves against the theft of their intellectual property. Alongside his research, Jarisch represents Fraunhofer AISEC on the Fraunhofer Scientific and Technical Council (STC), an internal advisory body to the Fraunhofer executive board. He has also been lending his fast and confident problem-solving skills to the German Federal Agency for Technical Relief (THW) since 2008. As a highly trained member of the THW team, he has already been deployed to missions abroad in Moldova, Haiti and Guatemala.

Barbora Hrdá

Doctoral student in the Secure Operating Systems department

Looking back on her time at a high school that specialized in science, surrounded by predominantly male teachers and classmates, Barbora Hrdá describes herself as a reserved girl from a migrant background. While she was aware of her talent in mathematics, she wasn't sure whether it would be enough for her to study for a degree in a technical subject.

Born in Prague, she decided to return to her cultural roots and studied Slavic Studies and Theater Studies at Ludwig Maximilian University (LMU) of Munich. She completed her Bachelor's degree with top grades — but hadn't found her true calling yet. While walking the Camino de Santiago from León to Finisterre, she decided to free herself from other people's expectations. "It has to be right for me," she realized, and shortly after she enrolled in Computing in the Humanities, an interdisciplinary computer science course at the University of Bamberg. Her love of mathematics, logic, statistics, programming and developing software systems reassured her that she was on the right track, and her Master's degree gave her a new sense of pride and self-confidence. "I don't feel I have to hide. If there's something I don't know, I find out more about it," is her approach to challenges.

During her time as an IT trainee, she enjoyed trying out new things and developing her skills in different areas, but then found that her first corporate position lacked these opportunities. She applied to Fraunhofer in the hope of contributing her own ideas and creating work that would have a positive societal impact.

Appreciation and space for development

During her job interview at Fraunhofer AISEC, she was immediately made to feel valued; a sense of appreciation that has always stayed with her. Over her four years at Fraunhofer AISEC, she has experienced a steep learning curve and worked on exciting projects. Starting out in mobile security and virtualization technologies, she now specializes in IT security for quantum computing platforms. She is currently working on protective mechanisms for this emerging technology, using both classic and quantum mechanical approaches. "It requires a completely different way of thinking and a lot of creativity," she says. She analyzes data streams, develops ideas and designs security tools that expand the range of security measures available specifically in the field of quantum computing. As an example, she is currently investigating options for encryption between a classic client and a quantum server. Her endeavors are laying the foundations for the secure use of quantum computers in both business environments and wider society. Curiosity, the joy of learning, creative freedom and the societal relevance of her work are what she values most.

Barbora is currently completing her doctoral project on the integrity and confidentiality of data for Quantum Computing-as-a-Service. Her research is being applied directly in customer projects, adding real value to the world of business and society.

> "You should do what you love — and that's also true for your choice of career. The most rewarding aspects of my work are quenching my thirst for knowledge, contributing my own ideas and having a positive impact on the economy and society."

Martin Seiffert

Senior Scientist in the Secure Systems Engineering department

> "We construct the toolbox and help you choose the right tools for designing and operating digital systems securely."

Martin Seiffert stores a variety of electronic ID types on his smartphone and uses them to identify himself in online services. His digital ID card makes completing his tax return easier, for example, and the Berlin native is also experimenting with health insurance apps, curious to see what his work looks like in practice.

Since graduating with a degree in IT and working as a research assistant and doctoral student at the Freie Universität Berlin, Seiffert has been researching information security and secure digital identities in the Secure Systems Engineering department of Fraunhofer AISEC since 2018. Working with industry partners and public institutions — for example, in the Secure Digital Identities Showcase innovation competition held by the German Federal Ministry for Economic Affairs and Climate Action — the computer scientist helps to design secure eID solutions and digital ecosystems, and evaluates them on the basis of international standards, national guidelines and European regulations such as the eIDAS Regulation (governing electronic identification and trust services). His goal is to provide comprehensive information security that works in harmony with other requirements, such as privacy, usability, interoperability and scalability.

Digital identities in a trustworthy environment

In a secure ecosystem, there are other factors besides digital identities that determine whether access to sensitive data is granted. Seiffert and his team have developed a concept for the future security architecture of the telematics infrastructure with this in mind. In the healthcare sector information network, only selected stakeholders, such as practices, hospitals, pharmacies and health insurance companies, are currently able to access patient data or electronic prescriptions using proprietary hardware. Ever logic-focused, Seiffert is looking to zero trust as a means of future-proofing healthcare services: This means that every single access request is checked, authenticated and authorized using an eID on a smartphone in combination with other factors such as location and time of access. Despite this data-hungry approach, Seiffert is highly committed to protecting the privacy of users. This is important not only to the millions of people whose highly private data is affected by his work (see page 21 for more information on the telematics infrastructure), but also to himself.

Finding the best solution with logic and structure

Seiffert considers his strength to be his understanding of structure. As the analyst states, "If we want to see progress in major digitalization projects, we need to understand which tools can help us make groundbreaking decisions." His field of research is based on extensive experience and expertise. He is passionate about helping his customers overcome the challenging task of maintaining a clear view when dealing with highly complex systems. Together with his team, he develops solution options systematically and clearly, making them measurable and therefore comparable. His affinity for methodology enables him to make informed decisions in favor of good, feasible solutions — but not perfection, as there is no such thing as a perfect solution in this dynamic field.

Publications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Marc Fischlin, Jonas von der Heyden, Marian Margraf, Frank Morgner, Andreas Wallner, Holger Bock: »Post-Quantum Security for the Extended Access Control Protocol«. In: 8th Security Standardisation Research Conference, SSR 2023, Lyon, France. 2023.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Publishing Notes

Published by
Fraunhofer Institute for Applied and Integrated Security AISEC
Prof. Dr. Claudia Eckert
Prof. Dr. Georg Sigl

Lichtenbergstr. 11
85748 Garching bei München, Germany
Phone +49 89 3229986-0
www.aisec.fraunhofer.de/en.html

Editorial team
Maria Schwab-Kloe, Wiebke Ramm, Pia Kinzler,
Tobias Steinhäusser (lead editor)

Layout
Maria Schwab-Kloe

Graphics
Daniela Miedaner

Printed by
Zimmermann GmbH Druck & Verlag

Contact
Fraunhofer Institute for Applied and Integrated Security AISEC
Lichtenbergstr. 11
85748 Garching bei München, Germany
Phone +49 89 3229986-170
marketing@aisec.fraunhofer.de

Cover
Targeted electromagnetic measurements on an exposed chip in the Fraunhofer AISEC Hardware Lab.

Photo acknowledgments
Cover: Oliver Bodmer
Page 4: Bernd Müller, Andreas Heddergott
Page 9: MAN, Andreas Heddergott
Page 10: Freepik, Fraunhofer AISEC
Page 13: Oliver Bodmer
Page 14: Freepik, Fraunhofer AISEC
Page 17: Andreas Heddergott, Creative Commons/TECNALIA
Page 18: Gene Glover, AllEyesOnYou.de, Freepik
Page 21: Adobe Stock, AllEyesOnYou.de, Oliver Bodmer
Page 22: Oliver Bodmer, Andreas Heddergott
Page 24: Oliver Bodmer
Page 26: HGEsch
Page 32: Andreas Heddergott/TUM, Oliver Rösler,
Adam Bacher, Bundesdruckerei GmbH, Rene Bertrand,
Bundesdruckerei GmbH
Page 33: Werner Bartsch; Bavarian Ministry of Economic
Affairs, Regional Development and Energy; Hessian.AI
Page 34: Fraunhofer CCIT
Page 35: Fraunhofer-Gesellschaft
Page 38: Oliver Bodmer
Page 41: Oliver Bodmer
Page 42: Oliver Bodmer
Page 45: Gene Glover
All other photos: © Fraunhofer AISEC

Follow us!

Fraunhofer AISEC cybersecurity blog

LinkedIn

XING

X