KASTEL Security Research Labs

Insight

2024|2025

KASTEL

Part I: Research & Researchers

Editorial Notes

Published by

KASTEL – Institute of Information Security and Dependability,
Engineering Secure Systems
Spokesperson: Prof. Dr. Jörn Müller-Quade

Editorial Team

Dr. Klaus Lehmann,
Dr. Martin Schmidt,
Dr. Mario Strefler,
Annette Wettach

Copy-Editing

mentorium GmbH, Berlin

Layout & Print

modus: medien + kommunikation gmbh
76829 Landau in der Pfalz
www.modus-media.de

Contact

KASTEL – Institute of Information Security and Dependability
Topic “Engineering Secure Systems”
Am Fasanengarten 5, 76131 Karlsruhe, Germany
E-mail: geschaeftsstelle@kastel.kit.edu
www.kastel-labs.de

Graphics

Dorfjungs., Karlsruhe
modus: medien + kommunikation gmbh, Landau

Photos & Figures

Adobe Stock: p. 5; Patricia Arias Cabarcos: p. 36, 46; Alessandro Erba: p. 46; Fraunhofer IOSB: p. 27; Emilia Grass: pp. 37, 46; Robert Heinrich: p. 46; Karlsruhe Institute of Technology (KIT): pp. 7, 9, 11, 22–26, 28, 31, 33–43, 45, 47, 49, 53, 56, 59, 62, 69–70; Peter Mayer: pp. 38, 47; André Platzer: p. 39; Ralf Reussner: p. 40; Andy Rupp: p. 40; Gunther Schiefer: p. 41; Indra Spiecker gen. Döhmann: p. 41; Ali Sunyaev: p. 42; Marcus Wiens: p. 43; Christian Wressnegger: pp. 43, 47, 66; J. Marius Zöllner: p. 44; Frederike Zufall: p. 44

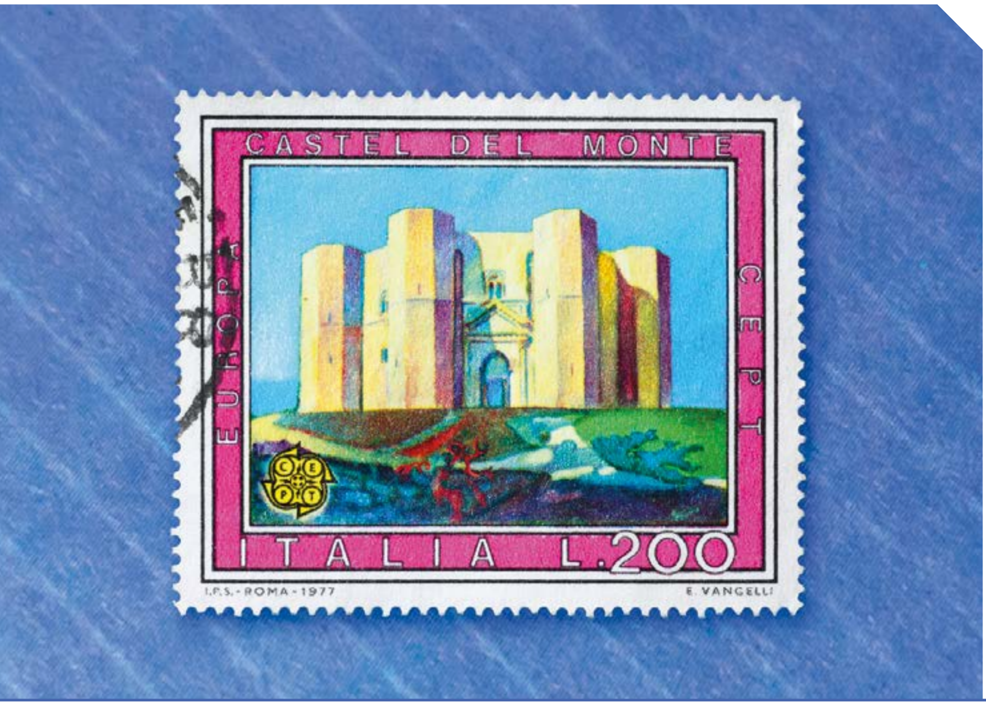
August
2025

CONTENTS

Part I: Research & Researchers

Part II: Facts & Numbers

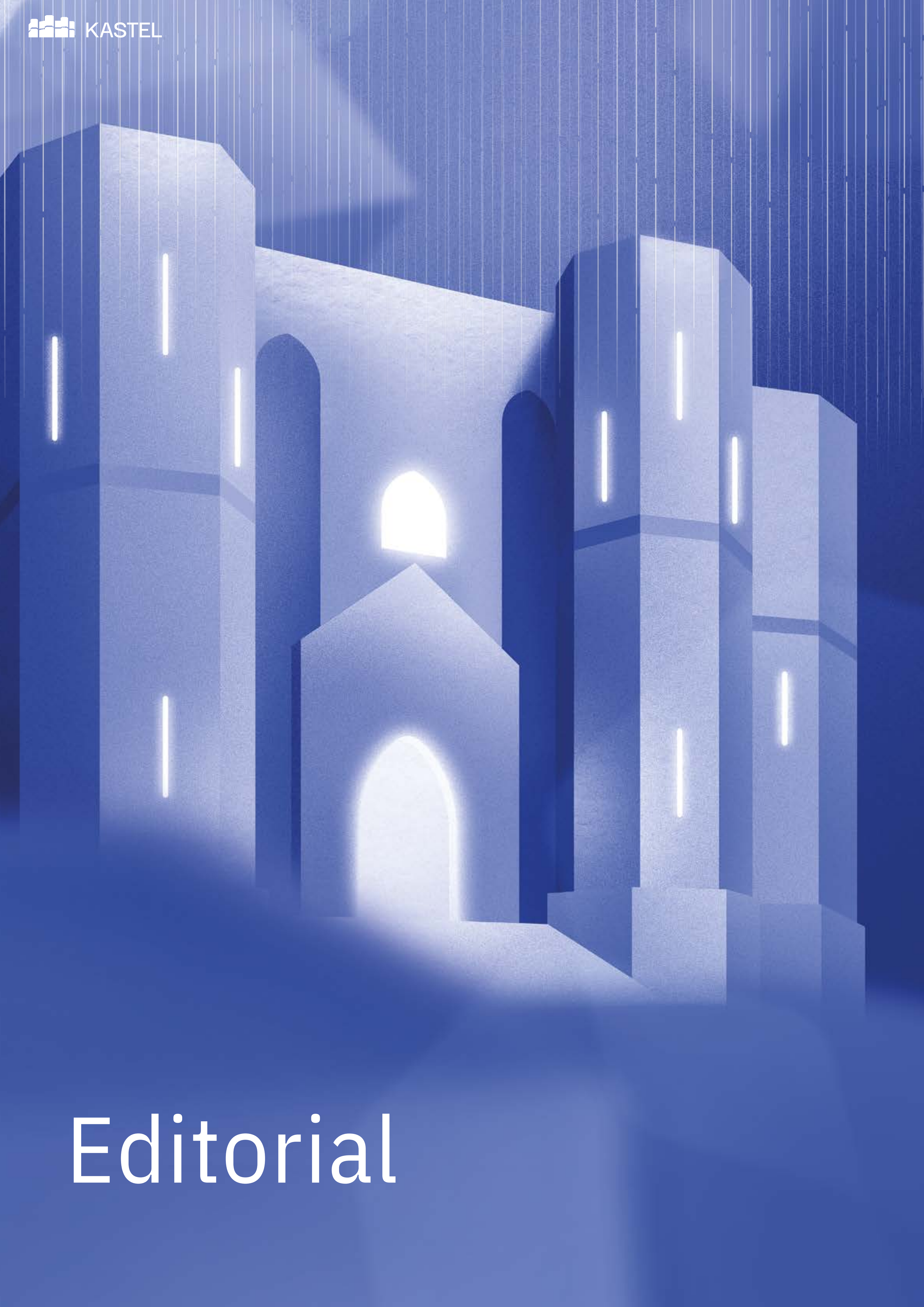
Castel del Monte



In 1959, the postal administrations of nineteen European countries came together to form the umbrella organisation the “European Conference of Postal and Telecommunications Administrations” (CEPT), which is located in Copenhagen, Denmark. In the postal sector, they retained the concept of jointly issued “Europa postage stamps”, which had already been initiated in 1956 by the states of the European Coal and Steel Community. These stamps are intended to symbolize the common interests and goals of the European states. Initially, the Europa stamps appeared with a corporate design, and from 1973 a common theme was agreed upon, which was implemented individually by the member states.

In the “Landscapes” series from 1977, the Italian 200-lire stamp shows the eastern side of Castel del Monte, built in the 13th century by the Hohenstaufen Emperor Frederick II in Apulia, Italy (artwork: Egidio Vangeli, realized in photogravure, approx. 48 mm x 40 mm).

Castel del Monte with its sophisticated architecture was chosen as the symbol for KASTEL Security Research Labs. It represents resilience against attacks from both internal and external sources.



Editorial

What Level of Security Do We Need to Ensure IT Security?

Dear readers,

It was almost eight years ago when KASTEL first participated in the Scientific Evaluation of the Helmholtz Association, resulting in the continuation of KASTEL as the Topic "Engineering Secure Systems". In May 2025, our scientific excellence was evaluated a second time – an event that took the better part of a year to prepare.

When KASTEL proposed to become part of the Helmholtz Association, one of its key commitments was to advance the field of cyber risk quantification. Quantifying the risk in an accurate and scientifically way is a huge challenge. At the same time, it helps to answer important questions, for example whether deploying a system is appropriate or, given a fixed budget, how to maximize the return on security investment.

Quantification also serves as an interface between disciplines, which is of particular importance in an interdisciplinary environment like KASTEL Security Research Labs: On the one hand, scientific results that can be expressed as meaningful numbers are easy to understand even for non-specialists. On the other hand, quantifying security raises similar methodological challenges across disciplines, namely how to quantify the validity of assumptions or prerequisites security builds on.

Our key quantification results include three new quantitative indicators from different disciplines, more than 65 peer-reviewed publications and four dissertations. During the Lab Visit at the evaluation, we presented several quantification-related demonstrators, including the production assistance system "4Crypt" (see p. 22), for which we conducted a quantitative game-theoretic analysis to assess its impact on workers as well as a quantitative security analysis for which we developed a novel methodology.

We also transferred our results to industry: In the project "VINKRYPTOR" with Mercedes-Benz, we developed a novel approach to pseudonymizing so-called vehicle identification numbers (VINs) – the resulting algorithm is used by several teams of Mercedes-Benz and was deemed GDPR-compliant by its legal department.

With "IIP 2.0", KASTEL Security Research Labs and SAFE e.V. defeated a patent troll by proposing a novel cryptographic scheme that was certified by the 'Physikalisch-Technische Bundesanstalt'. In the project "EVerest" with Pionix, we applied a novel methodology for quantitative formal verification on real software.

Beyond these highlights, quantification played a key role in every Research Group and Lab at KASTEL Security Research Labs, ranging from user studies quantifying the impact of security awareness measures to security type systems for secure software development. I invite you to learn more about our achievements on the following pages.

It is my pleasure to share that our hard work across KASTEL Security Research Labs was appreciated by the reviewers, the Topic received the grade 'excellent' in every aspect, with an emphasis on our progress related to cyber risk quantification.

I would like the opportunity to thank everyone involved – without your outstanding contributions, this result would not have been possible!

Prof. Dr. Jörn Müller-Quade

**Spokesperson of
KASTEL Security Research Labs**

Impressions I

Science & Art – "Code Beautiful Like a Clock"

EINLADUNG ZUR FEIERLICHEN ERÖFFNUNG DER VERANSTALTUNGSREIHE
KUNST | SOMMER | TECHNIK
Freitag, 11. Juli 2025
Zentrum für Kunst und Medien Karlsruhe (ZKM), Lorenzstraße 19, 76135 Karlsruhe
Einlass ab 18:00 Uhr | Programmstart um 18:30 Uhr
HERZLICH WILLKOMMEN
WELCOME !

"Code Beautiful Like a Clock" was on display at ZKM – Center for Art and Media Karlsruhe as part of the opening event "Art, Summer, Technology" on July 11, 2025.

Programs as mechanical works of art.

The installation revealed the hidden beauty of code. Created by Jörn Müller-Quade and Jeremias Mechler, the interactive piece visualized program execution like clockwork.

Who We Are …

KASTEL – from Competence Center to Security Research Labs

The "**Competence Center for Applied Security Technology KASTEL**" was founded in 2011 as one of three national competence centers for IT security funded by the German Federal Ministry of Education and Research (BMBF, now BMFTR). Funding was scheduled for a period of four years.

The unique situation in Karlsruhe as a research location was a great advantage: the extensive expertise of the institutional partners (1) Karlsruhe Institute of Technology (KIT), (2) Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, and (3) FZI Research Center for Information Technology in various areas of theoretical and applied cybersecurity were part of an unprecedented line-up. From the beginning, KASTEL has explicitly focused on interdisciplinary research that combines the most diverse aspects of cybersecurity. The successes achieved since then show that retaining this concept has proven its worth. This also contributed to the funding being extended and significantly increased by the BMBF following a successful evaluation in 2014.

The Competence Center KASTEL has developed into an important pillar of Karlsruhe's cybersecurity ecosystem and has an established position in the German cybersecurity landscape. In 2017/2018, KASTEL also participated in the Helmholtz Association's evaluations for the fourth period of program-oriented funding (PoF IV: 2021–2027). The evaluators emphasized the scientific excellence and recommended KASTEL for permanent Helmholtz funding.

At the beginning of the 2021 funding period, key research fields of KASTEL were transferred to the Topic Engineering Secure Systems (ESS), as an integral part of the Program "Engineering Digital Futures" (EDF) in the Research Field Helmholtz Information. This created the basis for pursuing long-term research goals that are of direct importance to the well-being of society. In addition, the umbrella brand "**KASTEL Security Research Labs**" was formed, providing a joint platform for IT security research in Karlsruhe with the aim of promoting a broad spectrum of research at an interdisciplinary level.

Milestones

2011
Establishment of "Competence Center for Applied Security Technology" KASTEL, funded by the BMBF (now BMFTR), as one of three national competetence centers for IT security.

2014
Successful evaluation by BMBF.

2017, 2018
Successful evaluations by the Helmholtz Association for the PoF IV.

2021
Perpetuation of KASTEL as Topic ESS in the Program "Engineering Digital Futures" (EDF) of Helmholtz Information and as KASTEL Security Research Labs as the overarching brand.

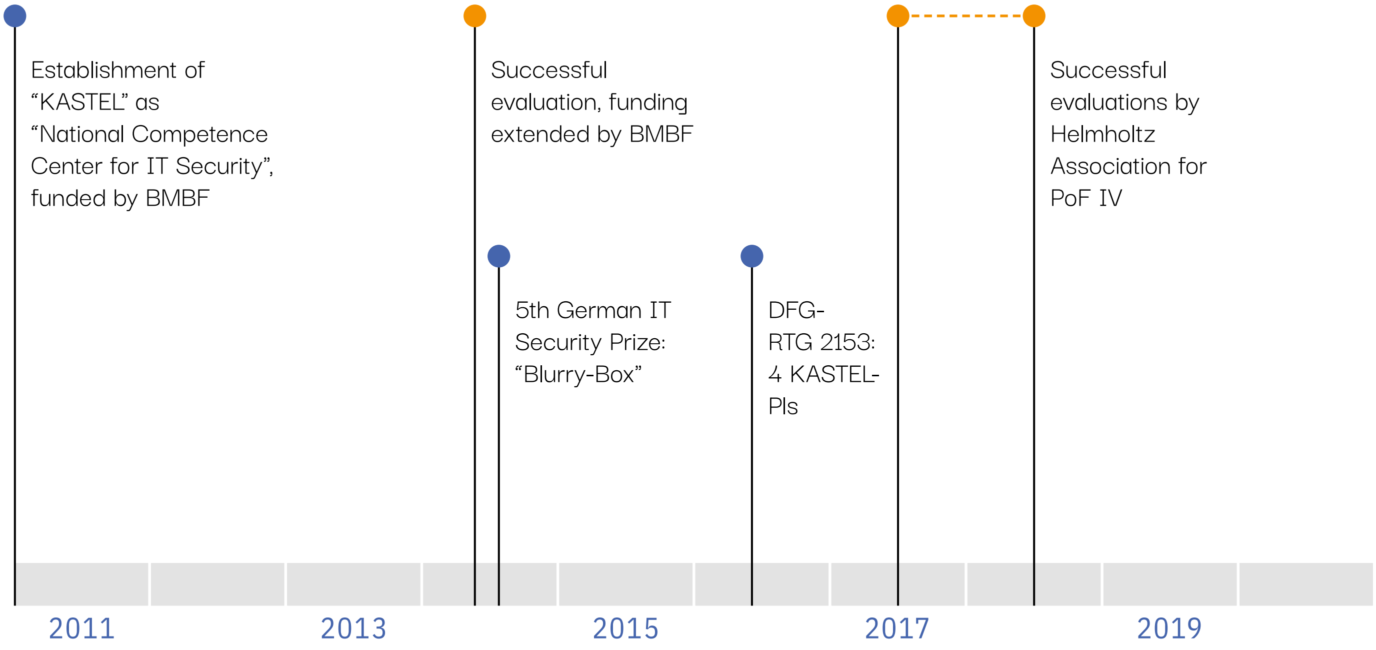
2025
Scientific Evaluation of Topic ESS by the Helmholtz Association.

2026
Outlook: Strategic Evaluation of Topic ESS by the Helmholtz Association regarding the PoF V.

KASTEL

Competence Center for Applied Security Technology

Bundesministerium für Bildung und Forschung


Establishment of "KASTEL" as "National Competence Center for IT Security", funded by BMBF
Successful evaluation, funding extended by BMBF
5th German IT Security Prize: "Blurry-Box"
DFG-RTG 2153: 4 KASTEL-PIs
Successful evaluations by Helmholtz Association for PoF IV
2011
2013
2015
2017
2019

Highlights

2014
"Blurry Box®" – First prize, 5th German IT Security Award of the Horst Görtz Foundation: FZI, KIT, and WIBU-SYSTEMS AG.

2016
DFG Research Training Group 2153 "Energy Status Data – Informatics Methods for its Collection, Analysis and Exploitation": KIT, participation of four KASTEL-PIs.

2023
Alexander von Humboldt Professorship for Artificial Intelligence: André Platzer.

2023
Start of Helmholtz Investigator Group "Building Network Resilience in Healthcare against Cyber-Attacks": Emilia Grass.

2023
Funding of the Collaborative Research Center 1608 "Convide".

2024
KASTEL SRL Fellows are Spokespersons of Research Division "Cybersecurity and Law" at FZI Research Center for Information Technology.

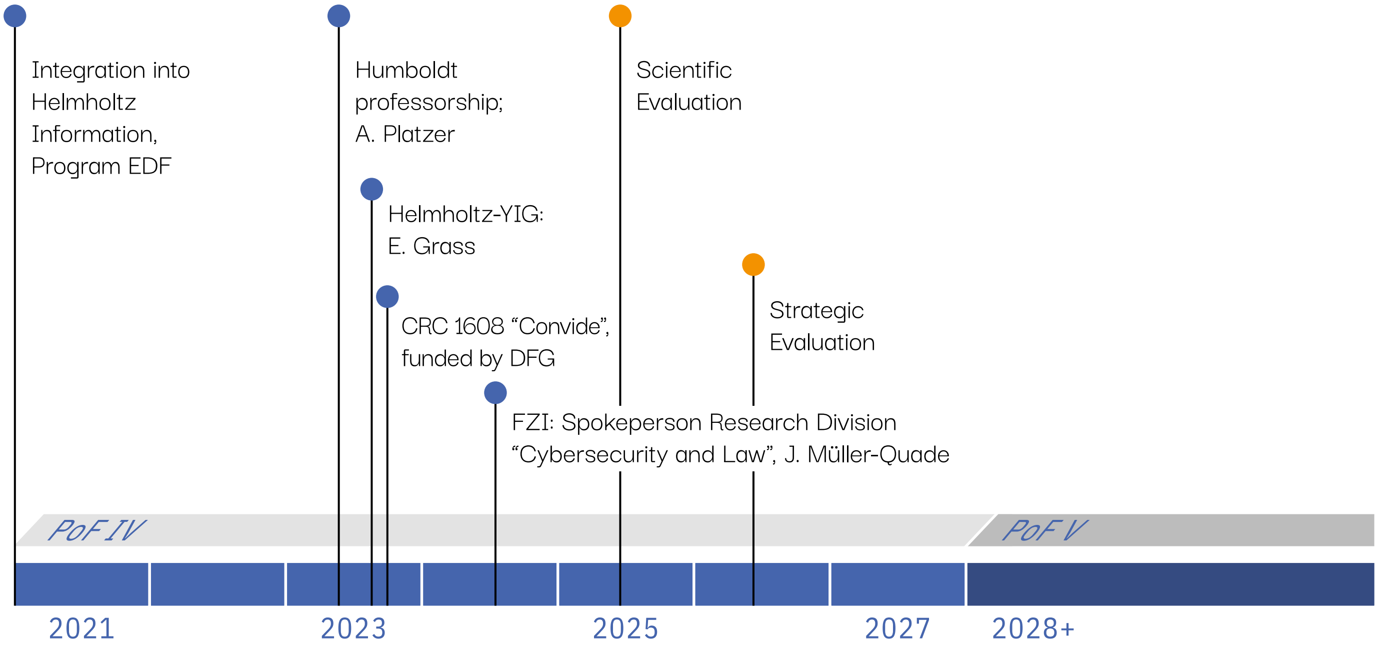
KASTEL

KASTEL Security Research Labs

Topic Engineering Secure Systems

HELMHOLTZ

Topic Trustworthy Security Technologies for Digital Societies



Integration into Helmholtz Information, Program EDF

Humboldt professorship; A. Platzer

Helmholtz-YIG: E. Grass

CRC 1608 "Convide", funded by DFG

FZI: Spokeperson Research Division "Cybersecurity and Law", J. Müller-Quade

Scientific Evaluation

Strategic Evaluation

PoF IV

PoF V

2021

2023

2025

2027

2028+

KASTEL – IT Security Research in Karlsruhe

KASTEL Security Research Labs (SRL)

After the end of the funding period of the "Competence Center for Applied Security Technology" in 2021, the name KASTEL lives on in "**KASTEL Security Research Labs**" and referring to an alliance for joint research in the field of IT security in Karlsruhe. **KASTEL Security Research Labs** serves as an umbrella brand supported by its institutional partners

- Karlsruhe Institute of Technology (KIT)
- Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB
- FZI Research Center for Information Technology

KASTEL Security Research Labs encompasses the activities of the Topic ESS, but also extends beyond that by covering a broader spectrum of research in the field of IT security involving additional Fellows and working groups.

IT Security Region Karlsruhe

Karlsruhe is an outstanding research location in the field of cybersecurity due to its broad spectrum of research and application. In addition to the contributions of KASTEL Security Research Labs, the Karlsruhe IT security region is also supported by

- Karlsruher IT Sicherheitsinitiative (KA-IT-Si)
  (Karlsruhe IT Security Initiative, initiated and coordinated by Secorvo GmbH),

- Kompetenzzentrum IT-Sicherheit
  (IT Security Competence Center), further developed into the research area "Cybersecurity and Law" at FZI in 2024.

These efforts are embedded in an extensive network of developers, practitioners, and users from business and industry.

The Topic Engineering Secure Systems

As part of **KASTEL Security Research Labs**, the Helmholtz Topic Engineering Secure Systems (ESS) is dedicated to researching theoretically sound, targeted and effective IT security measures to protect critical infrastructures. This is achieved by addressing not only the technical but also the social and human aspects of cyber-physical systems. In this context, security encompasses the aspects of safety, dependability, and privacy.

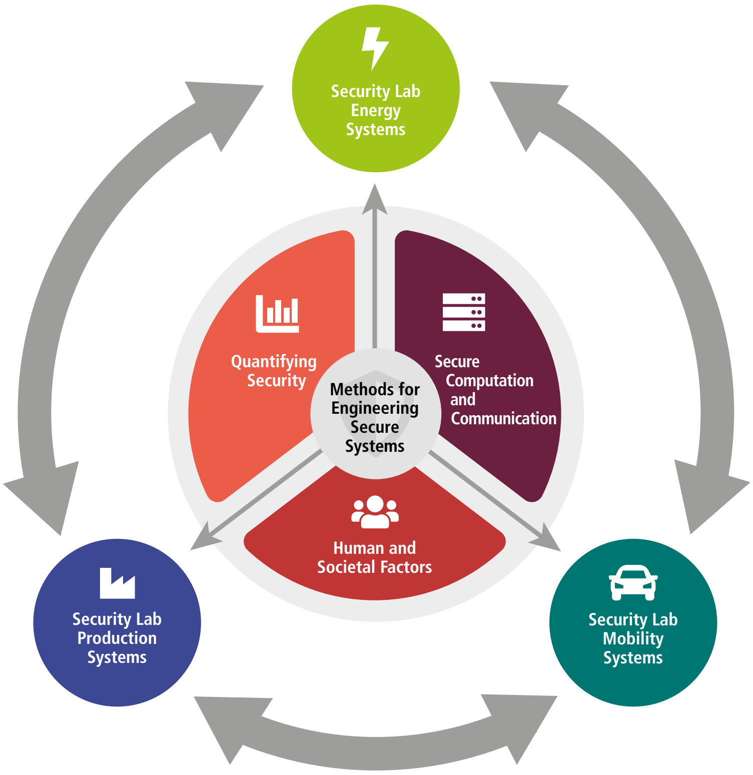
To this end, Topic ESS is organized into three Research Groups focusing on cross-sectional methodology on Quantifying Security (Q), Engineering Secure Computation and Communication (C&C), and Human and Societal Factors (HSF) and three domain-specific Security Labs focusing on engineering security in the application domains of energy, mobility, and production.

- Subtopic 1:
  Methods for Engineering Secure Systems
  - Research Group Quantifying Security
  - Research Group Secure Computation and Communication
  - Research Group Human and Societal Factors

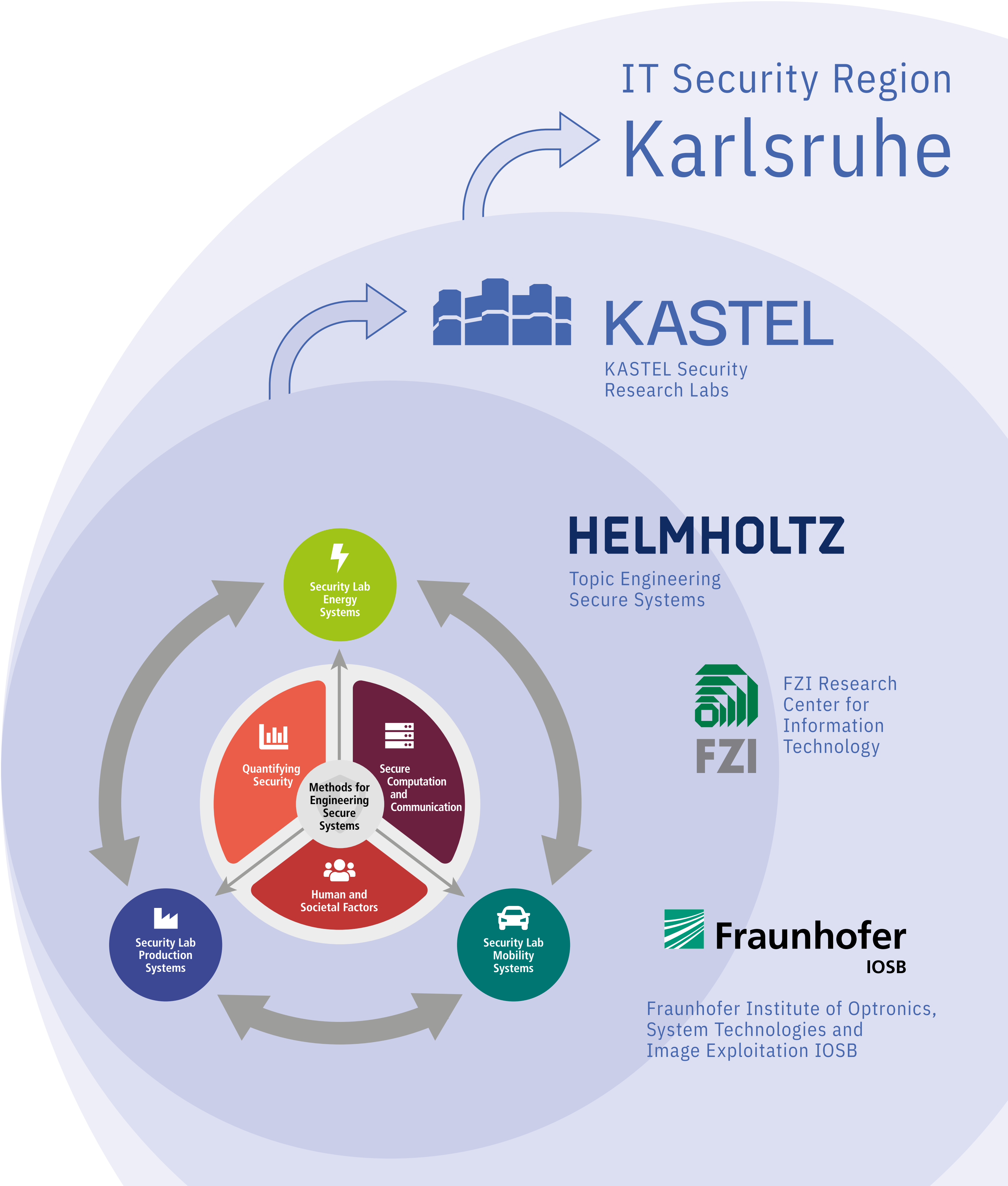
- Subtopic 2:
  Engineering Security for Energy Systems

- Subtopic 3:
  Engineering Security for Mobility Systems

- Subtopic 4:
  Engineering Security for Production Systems


Security Lab Energy Systems
Quantifying Security
Secure Computation and Communication
Methods for Engineering Secure Systems
Human and Societal Factors
Security Lab Production Systems
Security Lab Mobility Systems

KASTEL – IT Security Research in Karlsruhe



IT Security Region
Karlsruhe

KASTEL

KASTEL Security
Research Labs

HELMHOLTZ

Topic Engineering
Secure Systems

FZI

FZI Research
Center for
Information
Technology

Fraunhofer
IOSB

Fraunhofer Institute of Optronics,
System Technologies and
Image Exploitation IOSB

Security Lab Energy Systems
Quantifying Security
Secure Computation and Communication
Methods for Engineering Secure Systems
Human and Societal Factors
Security Lab Production Systems
Security Lab Mobility Systems

KIT
Karlsruher Institut für Technologie

In cooperation with:

- University of Cologne
- University of Luxembourg
- University of Paderborn
- TU Bergakademie Freiberg

Kompetenzzentrum
IT-Sicherheit

Competence Center for IT Security
(at FZI)

KA-IT-Si
Karlsruher IT-Sicherheitsinitiative

(Karlsruhe IT Security Initiative)

The different organizational layers

- Topic Engineering Secure Systems
- KASTEL Security Research Labs
- IT Security Region Karlsruhe

of IT security research in Karlsruhe and their constituting and supporting institutions become apparent in this structural presentation.

Research Foci

"[...] *when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind: it may be the beginning of knowledge, but you have scarcely, in your thoughts, advanced to the stage of science, whatever the matter may be.*"

Lord Kelvin (1824–1907)

W. Thomson [Lord Kelvin] (1889): *Electrical Units of Measurements.* – Popular Lectures and Addresses, Vol. I: 73-136, London, Macmillan and Co.

Research Group "Quantifying Security" – Cross-cutting Issue

Active Fellows in the Research Group "Quantifying Security"

Bernhard Beckert,
Jürgen Beyerer,
Emilia Grass,
Jörn Müller-Quade
(Spokesperson),
Ralf Reussner,
Thorsten Strufe,
Marcus Wiens

Given that cybersecurity, even when solely focusing on a technical perspective, has many facets, cyber risk quantification necessarily is an interdisciplinary endeavor. In KASTEL Security Research Labs – and in the Helmholtz Topic ESS –, there is a dedicated interdisciplinary Research Group Quantifying Security with principal investigators from the domains of cryptography, IT security, privacy, formal methods, software engineering, business economics, and operations research. Within this Research Group, theoretical foundations of security quantification are explored, with the goal of developing an integrated methodology.

However, quantitative security at KASTEL Security Research Labs has a much broader focus that extends beyond this single Research Group. As a cross-cutting issue across all Research Groups and Security Labs, quantification plays a role in many results and serves as a common language between different disciplines.

In the following, we present several examples, highlighting the benefits of our interdisciplinary approach to quantitative security applied across the Research Groups and Security Labs.

KASTEL SRL Publications

related to quantifying security issues:

- More than 65 (2021–2025),
- thereof: 22 CORE A*/A papers, see next pages.

CORE A*/A Publications related to Quantifying Security

2021

- P. Arias-Cabarcos, T. Habrich, K. Becker, C. Becker & T. Strufe (2021): *Inexpensive Brainwave Authentication: New Techniques and Insights on User Acceptance.* – Proceedings of the 30th USENIX Security Symposium: 55–72.
- F. Boenisch, R. Munz, M. Tiepelt, S. Hanisch, C. Kuhn & P. Francis (2021): *Side-Channel Attacks on Query-based Data Anonymization.* – CCS '21: Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security: 1254–1265.
- B. Broadnax, A. Koch, J. Mechler, T. Müller, J. Müller-Quade & M. Nagel (2021): *Fortified Multi-Party Computation: Taking Advantage of Simple Secure Hardware Modules.* – Proceedings on Privacy Enhancing Technologies, 2021 (4): 312–338.
- B. Broadnax, J. Mechler & J. Müller-Quade (2021): *Environmentally Friendly Composable Multi-Party Computation in the Plain Model from Standard (Timed) Assumptions.* – In: K. Nissim & B. Waters (eds.): Theory of Cryptography. TCC 2021. Lecture Notes in Computer Science, vol. 13042: 750–781.

2022

- M. Grundmann, H. Amberg, M. Baumstark & H. Hartenstein (2022): *Short Paper: What Peer Announcements Tell Us about the Size of the Bitcoin P2P Network.* – In: I. Eyal & J. Garay (eds.): Financial Cryptography and Data Security. FC 2022. Lecture Notes in Computer Science, vol. 13411: 694–704.
- F. Lanzinger & A. Weigl (2022): *Towards a Formal Approach for Data Minimization in Programs (Short Paper).* – In: J. Garcia-Alfaro, J.L. Muñoz-Tapia, G. Navarro-Arribas & M. Soriano (eds.): Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM CBT 2021. Lecture Notes in Computer Science, vol. 13140: 161–169.
- T. Runge, M. Servetto, A. Potanin & I. Schaefer (2022): *Immutability and Encapsulation for Sound OO Information Flow Control.* – ACM Transactions on Programming Languages and Systems, 45 (1): 3-1–3-35

2023

- P. Arias-Cabarcos, M. Fallahi, T. Habrich, K. Schulze, C. Becker & T. Strufe (2023): *Performance and Usability Evaluation of Brainwave Authentication Techniques with Consumer Devices.* – ACM Transactions on Privacy and Security, 26 (3): 26-1–26-36.
- R. Berger, B. Broadnax, M. Klooß, J. Mechler, J. Müller-Quade, A. Ottenhues & M. Raiber (2023): *Composable Long-term Security with Rewinding.* – In: G. Rothblum & H. Wee (eds.): Theory of Cryptography. TCC 2023. Lecture Notes in Computer Science, vol. 14372: 510–541.
- F. Dörre, J. Mechler & J. Müller-Quade (2023): *Practically Efficient Private Set Intersection From Trusted Hardware with Side-Channels.* – In: J. Guo & R. Steinfeld (eds.): Advances in Cryptology – ASIACRYPT 2023. Lecture Notes in Computer Science, vol. 14441: 268–301.

- M. Fallahi, T. Strufe & P. Arias-Cabarcos (2023): *BrainNet: Improving Brainwave-based Biometric Recognition with Siamese Networks.* – 2023 IEEE International Conference on Pervasive Computing and Communications (PerCom): 53–60.
- S. Hahner, R. Heinrich & R. Reussner (2023): *Architecture-based Uncertainty Impact Analysis to Ensure Confidentiality.* – 2023 IEEE/ACM 18th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS): 126–132.
- F.K. Kaiser, U. Dardik, A. Elitzur, P. Zilberman, N. Daniel, M. Wiens, F. Schultmann, Y. Elovici & R. Puzis (2023): *Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graph.* – IEEE Transactions on Dependable and Secure Computing, 20 (6): 4793–4809.
- M. Leinweber & H. Hartenstein (2023): *Brief Announcement: Let It TEE: Asynchronous Byzantine Atomic Broadcast with $n \geq 2f+1$.* – 37th International Symposium on Distributed Computing (DISC 2023). Leibniz International Proceedings in Informatics (LIPIcs), 281: 43:1–43:7.
- À. Miranda-Pascual, P. Guerra-Balboa, J. Parra-Arnau, J. Forné & T. Strufe (2023): *SoK: Differentially Private Publication of Trajectory Data.* – Proceedings on Privacy Enhancing Technologies, 2023 (2): 496–516.

2024

- B.M. Berens, F. Schaub, M. Mossano & M. Volkamer (2024): *Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool.* – CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, art. no. 826: 60 pp.
- N. Boltz, L. Schmid, B. Taghavi, C. Gerking & R. Heinrich (2024): *Modeling and Analyzing Zero Trust Architectures Regarding Performance and Security.* – In: M. Galster, P. Scandurra, T. Mikkonen, P. Oliveira Antonino, E.Y. Nakagawa & E. Navarro (eds.): Software Architecture. ECSA 2024. Lecture Notes in Computer Science, vol. 14889, 253–269.
- J. Camara, S. Hahner, D. Perez-Palacin, A. Vallecillo, M. Acosta, N. Bencomo, R. Calinescu & S. Gerasimou (2024): *Uncertainty Flow Diagrams: Towards a Systematic Representation of Uncertainty Propagation and Interaction in Adaptive Systems.* – 2024 IEEE/ACM 19th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS): 37–43.
- C. Coijanovic, C. Weis & T. Strufe (2024): *Panini – Anonymous Anycast and an Instantiation.* – In: G. Tsudik, M. Conti, K. Liang & G. Smaragdakis (eds.): Computer Security – ESORICS 2023. Lecture Notes in Computer Science, vol. 14345: 193–211.
- P. Guerra-Balboa, À. Miranda-Pascual, J. Parra-Arnau & T. Strufe (2024): *Composition in Differential Privacy for General Granularity Notions.* – 2024 IEEE 37th Computer Security Foundations Symposium (CSF): 680–696.
- D. Schadt, C. Coijanovic, C. Weis & T. Strufe (2024): *PolySphinx: Extending the Sphinx Mix Format With Better Multicast Support.* – 2024 IEEE Symposium on Security and Privacy (SP): 4386–4404.

2025

- M. Fallahi, P. Arias-Cabarcos & T. Strufe (2025): *On the Usability of Next-Generation Authentication: A Study on Eye Movement and Brainwave-based Mechanisms.* – CHI EA '25: Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, art. no. 420: 14 pp.

Quantitative Analyses of 4Crypt – Privacy-Preserving Documentation for Assembly Assistance Systems

A privacy-friendly and trustworthy interactive assembly table serves as a showcase for our methodological results with respect to quantification. Its video feed is recorded for later analysis of critical work steps. While this is useful for quality control, it also entails a major privacy concern, as workers may be subjected to unfounded video surveillance by their employer. We quantified the privacy-related technical mechanisms of 4Crypt with respect to their security as well as their effect on workers.

Research Group "Secure Computation and Communication"

Involved Fellows

Bernhard Beckert,
Jürgen Beyerer,
Veit Hagenmeyer,
Hannes Hartenstein,
Anne Koziolek (Spokesperson),
Jörn Müller-Quade,
Ralf Reussner,
Andy Rupp (Spokesperson),
Thorsten Strufe,
Ali Sunyaev,
Martina Zitterbart

There are several cases where quantification plays a crucial role in secure computation and communication:

Continuous Automated Risk Management: We develop automated risk quantification methods for OT systems that minimize the need for expert input, using the MITRE ATT&CK framework to assess systems, attack techniques, and countermeasures. These quantifications help prioritize risks and evaluate countermeasures based on vulnerability coverage under budget constraints.

Secure and Efficient Bookkeeping and Analytics: We design privacy-preserving, decentralized ticketing architectures for Mobility-as-a-Service. Architecture 1 (NxB-FT) achieves 400 kOps/s with approximately 0.5 s latency and Byzantine fault tolerance via TEE-based broadcast. Architecture 2 (POBA) ensures UC security and unlinkability against ORAM adversaries, processing 1 million transactions/day [1]. Architecture 3 uses formally verified payment-channel protocols.

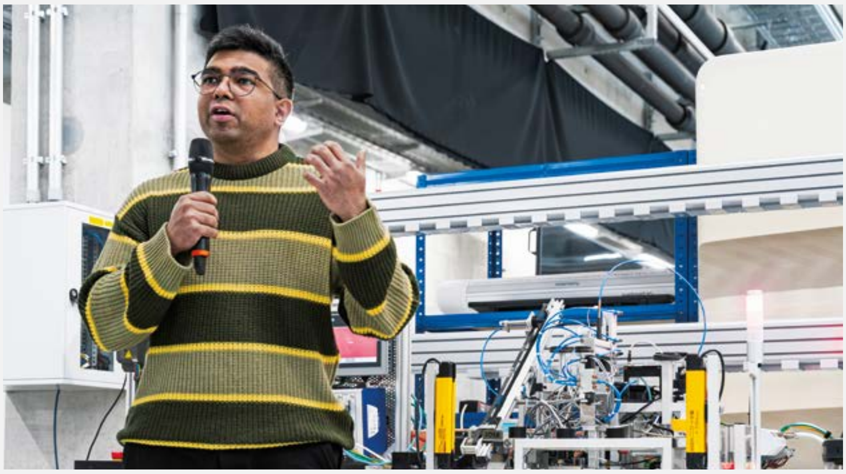
Smart Grid Testbed for Cybersecurity Research: Our testbed for energy systems integrates threat models and realistic scenarios to assess resilience [2]. It enables quantifiable security assessment through empirical validation of defense strategies, aligns with the NIST framework, and bridges theory with practice for critical infrastructure protection.

References

[1] D. Faut, V. Fetzer, J. Müller-Quade, M. Raiber & A. Rupp (2025): *POBA: Privacy-Preserving Operator-side Bookkeeping and Analytics.* – IACR Communication in Cryptology, 2 (2): 1-56.

[2] G. Elbez, G. Sánchez, S. Canbolat, S. Corallo, C. Fruböse, F. Lanzinger, N. Kellerer, G. Keppler, F. Neumeister, B. Beckert, A. Koziolek, M. Zitterbart & V. Hagenmeyer (2025): *Insights and Lessons Learned from a Realistic Smart Grid Testbed for Cybersecurity Research.* – e-Energy '25: Proceedings of the 16th ACM International Conference on Future and Sustainable Energy Systems: 805-812.

Continuous Automated Risk Management (CARM) System for Industrial Networks



CARM is a non-intrusive industrial network security monitoring framework designed to assist asset owners of operational industrial systems in managing risks and developing the IEC 62443-mandated security architecture. CARM automates system information collection, assesses security posture, and measures descriptive security metrics using machine learning and graph theory-based analyses. It also helps select the optimal set of technical countermeasures while considering constraints such as budget limitations.

Research Group "Human and Societal Factors"

Involved Fellows

Patricia Arias Cabarcos,
Jürgen Beyerer,
Emilia Grass,
Peter Mayer,
Indra Spiecker gen. Döhmann,
Thorsten Strufe,
Melanie Volkamer (Spokesperson),
Marcus Wiens,
Christian Wressnegger,
Frederike Zufall

In the Research Group Human and Societal Factors, we measure to what extent the risk is reduced through awareness measures and/or tool support [1]. To this end, we measure, for example, the detection rate of phishing and legitiamte e-mails [2] or the remediation of vulnerabilities in web services. We are particularly interested in how risk changes over time (months) after the awareness measure and when a new awareness measure is necessary in the form of a refresher [3]. There are multiple different awareness measures, e.g., we developed and evaluated four anti-phishing awareness measures: the NoPhish videos, a serious game, an online course, and the Security Teaching & Awareness Robot (STAR). A variety of the measures has been used by the scientific community, by organizations, and by end users.

References

[1] B.M. Berens, F. Schaub, M. Mossano & M. Volkamer (2024): *Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool.* – CHI '24: Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems, art. no. 826: 60 pp.

[2] J. Petelka, B. Berens, C. Sugatan, M. Volkamer & F. Schaub (2025): *Restricting the Link: Effects of Focused Attention and Time Delay on Phishing Warning Effectiveness.* – 2025 IEEE Symposium on Security and Privacy (SP), 2025: 55-73.

[3] B.M. Berens, M. Mossano & M. Volkamer (2024): *Taking 5 Minutes Protects You for 5 Months: Evaluating an Anti-Phishing Awareness Video.* – Computers & Security, 137, art. no. 103620: 1-19.

NoPhish Concept and Awareness Measures

To better understand the attack form 'fraudulent messages' and learn how to protect themselves, we have developed awareness, education and training measures. The concept covers four issues: (1) Introduction to the topic; (2) Detection of implausible, fraudulent messages; (3) Detection of dangerous links (including finding the URL behind the link, structure of the URL and tricks of the attackers); (4) Detection of messages with dangerous attachments (including finding the format of the file, list of particularly dangerous file formats and tricks of the attackers).

"KASTEL Security Lab Energy"

Involved Fellows

Bernhard Beckert,
Veit Hagenmeyer
(Spokesperson),
Anne Koziolek,
Jörn Müller-Quade,
Indra Spiecker gen.
Döhmann,
Christian Wressnegger,
Martina Zitterbart
(Co-Spokesperson)

Quantification plays a crucial role in enhancing the security and resilience of energy infrastructure against diverse cyber-physical threats. In the KASTEL Security Lab Energy, simulations of adversarial and multi-stage attacks on critical systems such as SCADA, IEDs, and RTUs enable precise assessment of their potential impacts, facilitating the identification and measurement of specific attack vectors. Threat modeling with Large Language Models (LLMs) allows for the generation of probabilistic threat scenarios based on substation configuration data, quantifying the likelihood and potential consequences of various attack pathways. Research on GPS/GNSS time synchronization attacks employs simulation to measure the risks associated with spoofing and jamming, evaluating their effects on substation operations and safety. Thus, providing a metric-driven understanding of vulnerability severity. Additionally, the development of Intrusion Detection Systems (IDS) emphasizes quantifying detection performance through false positive/negative rates and response times, critical for operational security. Similarly, SIEM systems are analyzed for their efficiency in correlating security events across infrastructure layers, enabling the quantification of mitigation effectiveness. Collectively, these quantification efforts support data-driven decision-making, optimize defense strategies, and strengthen the resilience of energy systems against evolving threats. (see also: "FENCE: Future ENergy Cybersecurity Evaluation").

References

S. Canbolat, C. Fruböse, G. Elbez & V. Hagenmeyer (2024): *Extended Abstract: Assessing GNSS Vulnerabilities in Smart Grids.* – In: F. Maggi, M. Egele, M. Payer & M. Carminati (eds.): Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2024. Lecture Notes in Computer Science, vol. 14828: 545-555.

FENCE: Future ENergy Cybersecurity Evaluation

FENCE is a cybersecurity research platform bridging theoretical methods and practical security implementations within the energy sector. FENCE facilitates a thorough analysis of vulnerabilities, supports research in intrusion detection, and enables effective mitigation strategies and systematic risk assessment. It specifically targets critical cybersecurity challenges within energy systems and presents our research findings through an intuitive web interface for enhanced accessibility and usability.

"KASTEL Security Lab Mobility"

Involved Fellows

Ingmar Baumgart,
Hannes Hartenstein,
Anne Koziolek,
Raffaela Mirandola,
Jörn Müller-Quade,
Oliver Raabe,
Ralf Reussner
(Spokesperson),
Andy Rupp,
Ina Schaefer
(Co-Spokesperson),
Ali Sunyaev,
Christian Wressnegger,
Martina Zitterbart,
J. Marius Zöllner

The importance of secure software for the automotive industry was recently demonstrated by a prominent security incident at a German car manufacturer. Movement data from 800,000 e-cars and the owners' contact information were published on the Internet. Researchers from the KASTEL Mobility Lab are counteracting such data leaks by providing development methods and tools for automotive software, in which the level of security to be achieved can be quantitatively specified and enforced. A specific approach makes it possible to distinguish program data between multiple types of security levels, which can be specified directly inside the program code of an object-oriented language [1].

On this basis, a dedicated tool enforces security by only accepting programs with secure data types, while the corresponding typing rules ensure that not too many secure programs are rejected during coding. In a follow-up work, the typing rules were translated into rules for the construction of programs [2]. When refining the code of a secure program, these rules ensure that security can be retained directly by construction.

References

[1] T. Runge, M. Servetto, A. Potanin & I. Schaefer (2023): *Immutability and Encapsulation for Sound OO Information Flow Control. – ACM Transactions on Programming Languages and Systems,* 45 (1): 3-1-3-35.

[2] T. Runge, A. Kittelmann, M. Servetto, A. Potanin & I. Schaefer (2022): *Information Flow Control-by-Construction for an Object-oriented Language.* – In: B.H. Schlingloff & M. Chai (eds.): Software Engineering and Formal Methods. SEFM 2022. Lecture Notes in Computer Science, vol. 13550: 209-226.

Design & Development Methods for Secure Automotive Software Systems

In the automotive industry, design and development methods for secure software gain in importance due to larger attack surfaces and legal obligations. In our lab, we provide design and development methods covering the whole development lifecycle, including its early phases. Our methods address domain-specific characteristics such as variability of product lines, complex supply chains between companies, or collaborative development spanning multiple engineering disciplines.

“KASTEL Security Lab Production”

Involved Fellows

Patricia Arias Cabarcos,
Jürgen Beyerer
(Spokesperson),
Marcus Wiens,
Christian Wressnegger
(Co-Spokesperson)

The KASTEL Security Lab Production considers the quantification of security in the research topics industrial security testing, automation of risk management for asset owners in production, and finally in interdisciplinary quantification of security for manufacturing assistance systems in the Research Group Quantifying Security.

We conducted two separate analyses of industrial components [1, 2] using automated testing tools, including our own Tool ISuTest, quantifying their vulnerability. These results serve also as a baseline for comparing future testing approaches and quantifying their performance with respect to identified vulnerabilities. We conducted automated tests as part of a test strategy specifically designed for industrial components, uncovering multiple types of vulnerabilities within them. Our experiments reveal findings for all considered OT components, which are quantified according to their severity including crashes, hangs, and information on outdated software.

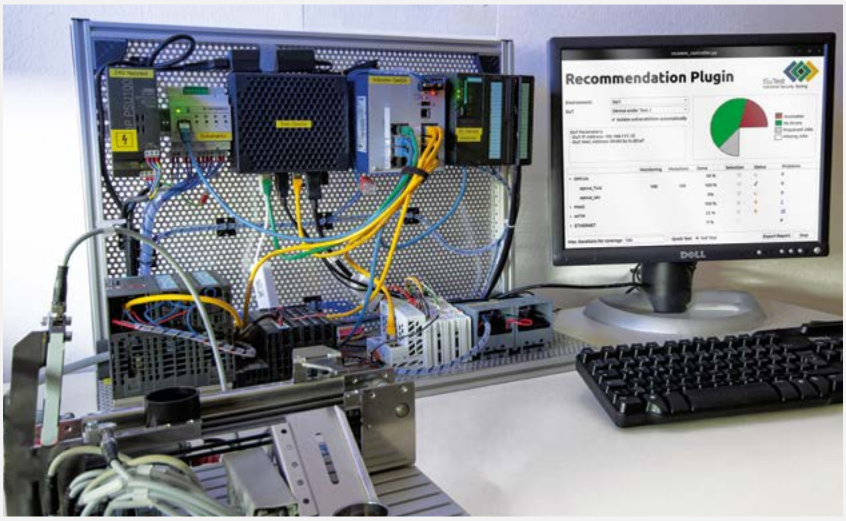
With the Continuous Automated Risk Management (CARM) framework to help industrial asset owners design and implement secure architectures. CARM passively captures network traffic to assess Security Posture using granular security metrics. It leverages the MITRE ICS framework to identify threats and includes a module that evaluates countermeasures – individually or combined – within budget limits, enabling optimized, iterative security planning.

References

[1] A. Borcherding, P. Takacs & J. Beyerer (2022): *Cluster Crash: Learning from Recent Vulnerabilities in Communication Stacks.* – Proceedings of the 8th International Conference on Information Systems Security and Privacy (ICISSP 2022), 334-344.

[2] A. Borcherding, M. Giraud & L. Tzigiannis (2025): Show Me What You Got: Vulnerabilities of Industrial Components Revealed by Automated Black Box Testing. – 20th International Conference on Availability, Reliability and Security (ARES 2025), submitted.

“ISuTest”



The “ISuTest” automated vulnerability assessment framework for industrial automation components as well as “SMILE4VIP” (Smart eMaIl Link domain Extractor to support Visual Impaired People), were finalists for the NEO Innovation price awarded by the Karlsruhe TechnologyRegion in 2022. Ideas from a proof of concept for the topic became part of a demonstrator for the Federal Office for Information Security (BSI).

Research Focus
Health: Secure AI for Medical Data

Secure hardware and their applications have been a common research issue in KASTEL, as hardware-based security can offer great performance. However, the hardware usually needs to be fully trusted, which might not be justified in real life.

At the Lindau Nobel Laureate Forum in 2023 and at ASIACRYPT 2023, we presented an approach for secure computations applicable to medical data that uses secure hardware, but greatly reduces the required trust by using a hybrid approach that includes light-weight cryptography. Inspired by this success, KASTEL SRL and DKFZ (German Cancer Research Center, Heidelberg) have joined forces for the project "SECAIMED", short for "Secure AI for Medical Data". In this project, researchers from the domains of medical informatics, law and cryptography join forces to develop secure and legally compliant solutions for high-performance and scalable computations on medical data. Our new approach will advance the state-of-the-art of privacy-preserving computations in the domain of health, which is of highest societal relevance.

Key technical tool is a so-called "cryptographic enclave" to perform the computations at near-native performance while, at the same time, achieving provable security guarantees. To this end, the security is based on cryptographic methods combined with comparatively simple building blocks, resulting in an architecture that is amenable to quantifying its security.

Preliminary results were presented at this year's Helmholtz AI conference in Karlsruhe.

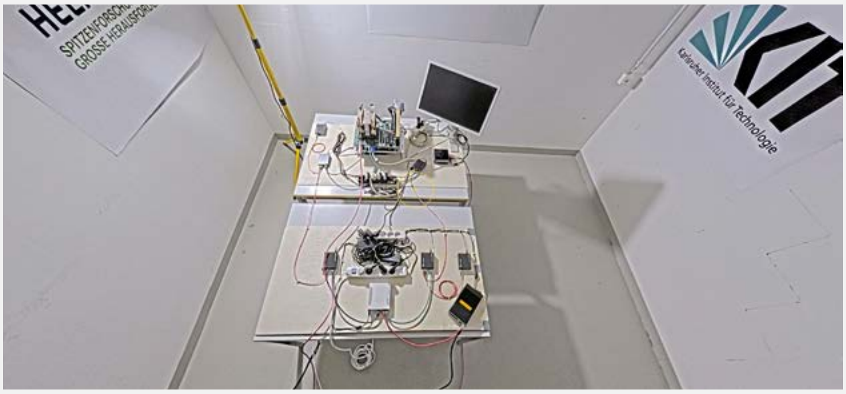
References

N. Bindel, X. Bonnetain, M. Tiepelt & F. Virdia (2024): *Quantum Lattice Enumeration in Limited Depth.* – In: L. Reyzin & D. Stebila (eds.): Advances in Cryptology – CRYPTO 2024. Lecture Notes in Computer Science, vol. 14925: 72-106.

F. Dörre, J. Mechler & J. Müller-Quade (2023): *Practically Efficient Private Set Intersection from Trusted Hardware with Side-Channels.* – In: J. Guo & R. Steinfeld (eds.): Advances in Cryptology – ASIACRYPT 2023. Lecture Notes in Computer Science, vol. 14441: 268–301.

B. Broadnax, A. Koch, J. Mechler, T. Müller, J. Müller-Quade & M. Nagel (2021): *Fortified Multi-Party Computation: Taking Advantage of Simple Secure Hardware Modules.* – Proceedings on Privacy Enhancing Technologies, 2021 (4): 312-338.

SECAIMED: Secure and Compliant AI for Medical Data



The cryptogaphic enclave is hosted in a high-security data center in Karlsruhe. Its security is based on simple trusted hardware such as a trusted platform module (TPM), data diodes and BSI-certified network encryptors. To protect against the consequences of physical attacks, the enclave is continuously under camera surveillance. Also, all data is erased as soon as the single door to the enclave's room is opened.
(Photo by a surveillance camera.)

Research Focus
Securing Democracies

Involved Fellows

Jürgen Beyerer,
Bernhard Beckert,
Jörn Müller-Quade,
Indra Spiecker gen. Döhmann,
Thorsten Strufe,
Melanie Volkamer,
Christian Wressnegger

The world changed dramatically since the start of KASTEL Security Research Labs:

(1) Due to the COVID-19 pandemic, remote electronic voting became very popular. As a consequence, we decided to research on understanding and mitigating threats associated with remote electronic voting in order to protect our democracies.

(2) In particular, in the beginning of the Russian invasion, fake information became an emerging topic. Therefore, it was decided to conduct research on the understanding and mitigation of threats in the context of fake information.

(3) Cambridge Analytics demonstrated the power of political microtargeting related to election campaigns on social media platforms. Therefore, it was decided to research political microtargeting.

Remote electronic voting

In the context of remote electronic voting, the main activities were:

- Two interdisciplinary projects ("Trust Through Explainability in Verifiable Online Voting Systems" [1] in collaboration with the Topic Knowledge for Action and "End-to-End Verifiable and Secret Online Elections at KIT" [2]).
- General Chair of the international conference of E-VOTE-ID [3] with the Topic ESS being the main sponsor.

EVOTeID INTERNATIONAL CONFERENCE

- One ongoing PhD project in the area of "Usable Secure End-to-End Verifiable Voting Systems" and one finished PhD project on "Formal Methods for Trustworthy Voting Systems: From Trusted Components to Reliable Software".
- Providing a verifier for the GI (German Informatics Society) elections since 2023 to enable voters to verify that their vote was cast as intended and stored as cast, as well as a verifier to enable everyone to check that all stored votes were properly tallied.
- Consultation for the study "E-Voting – Status Quo and Perspectives for Germany" [4] from the Office of Technology Assessment at the German Bundestag (TAB).
- Consultation for the study "A Study of Mechanisms for End-to-End Verifiable Online Voting" [5] from the German Federal Office for Information Security (BSI).
- Setting up a webpage summarizing the various competences in the area of electronic voting [6].

Fake information

In the context of fake information, the main activities were:

- A paper on "How to Protect the Public Opinion Against New Types of Bots?" [7] in which the authors developed and evaluated an algorithm to detect social bots more effective than existing approaches do.
- A joint project between the Topics ESS and Knowledge for Action called "Interdisciplinary Approaches to Deepfakes" [8].

Political microtargeting

In the context of political microtargeting is a systematic legal analysis of the EU regulation on the transparency and targeting of political advertising from 2024 [9] available. This will be followed by an analysis from the voters' perspective focusing on their awareness.

Future democracies

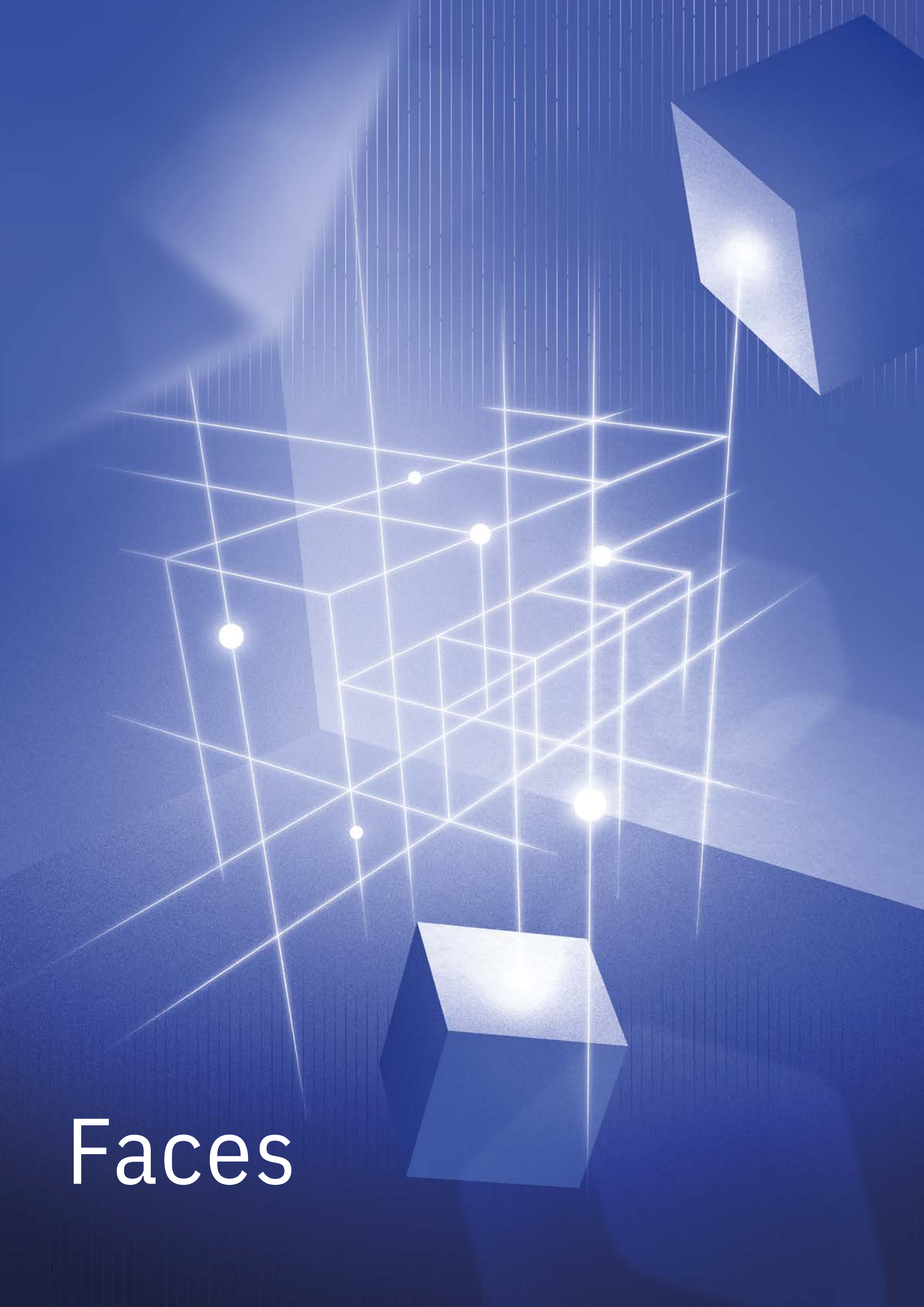
Furthermore, several KIT-wide workshops titled "Future Democracies" [10] were organized to discuss the results and, more importantly to identify interdisciplinary research questions, e.g., in the context of liquid democracy as well as on trust and transparency in technology.

[1] Project "Trust Through Explainability in Verifiable Online Voting Systems". < https://formal.kastel.kit.edu/projects/erklaerbareWahlsysteme/?lang=en >.
[2] Project "End-to-End Verifiable and Secret Online Elections at KIT". < https://formal.kastel.kit.edu/projects/e2eWahlenAmKIT/?lang=en >.
[3] Tenth International Joint Conference on Electronic Voting, October 1–3, Nancy, France. < https://www.e-vote-id.org/ >.
[4] Study "E-Voting – Status Quo and Perspectives for Germany", Office of Technology Assessment at the German Bundestag (TAB). < https://www.tab-beim-bundestag.de/english/news-2023-09-e-voting-status-quo-and-future-prospects-for-germany.php >.
[5] Project "A Study of Mechanisms for End-to-End Verifiable Online Voting". German Federal Office for Information Security (BSI). < https://www.bsi.bund.de/EN/Service-Navi/Publikationen/Studien/Verifiable_Online-Voting/Verifiable_Online-Voting.html >.
[6] Webpage "KIT E-Voting Kompetenzzentrum". < https://evoting.kastel.secuso.org/ >.
[7] J.L. Reubold, S.C. Escher, C. Wressnegger & T. Strufe (2022): *How to Protect the Public Opinion Against New Types of Bots*? – 2022 IEEE International Conference on Big Data (Big Data): 1671–1680.
[8] Project "Interdisciplinary Approaches to Deepfakes". < https://www.itas.kit.edu/english/projects_ jahn21_izdf.php >.
[9] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising. Official Journal of the European Union, L-Series. < https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202400900 >.
[10] Project "Future Democracies". < https://secuso.aifb.kit.edu/english/2189.php >.

HELMHOLTZ
KIT
Karlsruhe Institute of Technology
Regulatory approaches on technological advancement
Research Question
Impact
Research Activities and Results
Publications
KASTEL
www.kit.edu
General Data Protection Regulation
Datenschutzrecht
DS-GVO/BDSG
Nomos
Digitalisierung im Vertrieb

"Regulatory Approaches on Technological Advancement".

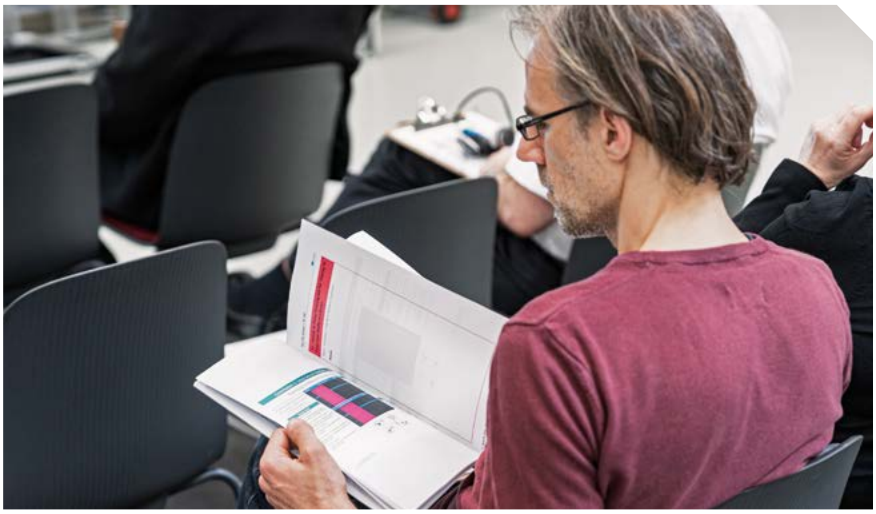
Faces



Impressions II

Presentation of Research Results

KASTEL SRL Fellows
discussing the presentations
of research results, April 2025.



Our Team

Interdisciplinarity

An unique selling point of **KASTEL Security Research Labs** is the interdisciplinary approach of our research groups: The issues of security and safety are analyzed and investigated from the perspective of different scientific disciplines. Only by looking beyond the boundaries of single disciplines it is possible to tackle societally relevant issues in such a way that applicable and user-friendly solutions can be developed and derived.

Our 25 Fellows and their teams have specialists from the various disciplines:

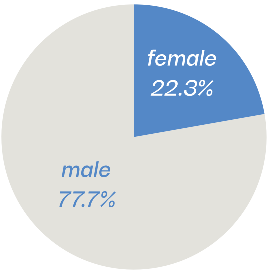
- Computer Science,
- Economics,
- Electrical Engineering,
- Law,
- Mathematics,
- Physics,
- Psychology.

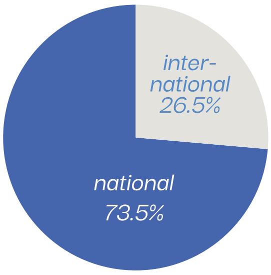
We organize the exchange between the disciplines:

- Joint discussion rounds and research group meetings,
- Joint seminars and meetings,
- Joint projects and initiatives,
- Joint publications and transfer measures.

Diversity

Currently, 211 scientists are involved in the KASTEL Security Research Labs. The proportion of female researchers is 22%, while international colleagues make up 27%. For more detailed information, please refer to Part II.





KASTEL SRL Fellows

On the following pages we present our KASTEL Security Research Labs Fellows with the keywords of their scientific activities and some selected publications.

The KASTEL SRL team at the Scientific Evaluation of the Helmholtz Topic ESS, May 2025.

Fellows

Selected Publications

Prof. Dr. Patricia Arias Cabarcos

- Research Group IT Security at University of Paderborn
- PhD in Telematic Engineering (U Carlos III Madrid, 2013).
- Chair for IT Security (U Paderborn, since 2021).

Intersection of security, privacy, and human-computer interaction, password security and usability, novel behavioral biometrics, behavioral data privacy, privacy awareness and transparency enhancing technologies.

A.K. Chaurasia, M. Fallahi, T. Strufe, P. Terhörst & P. Arias Cabarcos (2024): *NeuroIDBench: An Open-Source Benchmark Framework for the Standardization of Methodology in Brainwave-based Authentication Research.* – 2024. Journal of Information Security and Applications, 85, art. no. 103832: 1-18.

P. Arias-Cabarcos & P. Mayer (2025): *'The more accounts I use, the less I have to think': A Longitudinal Study on the Usability of Password Managers for Novice Users.* – 21st Symposium on Usable Privacy and Security (SOUPS 2025), Seattle, Washington, USA: accepted.

PD Dr.-Ing. Ingmar Baumgart

- Competence Center for IT Security at FZI Research Center for Information Technology
- PhD in Informatics (U Karlsruhe (TH), 2010).

Automotive cybersecurity, network security, IoT security, privacy enhancing technologies, design of distributed systems.

N. Goerke, A. Märtz & I. Baumgart (2024): *Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability.* – e-Energy '24: Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems, 2024: 46-54.

T. Lauser, M. Müller, I. Baumgart & C. Krauß (2025): *Data Distribution and Redistribution – A Formal and Practical Analysis of the DDS Security Standard.* – SAC '25: Proceedings of the 40th ACM/SIGAPP Symposium on Applied Computing: 1839-1848.

Prof. Dr. Bernhard Beckert

- Research Group Application-oriented Formal Verification at KIT
- PhD in Computer Science (U Karlsruhe (TH), 1998).
- Professor of Computer Science (KIT, since 2009).

Formal methods for the specification and verification of software, IT security, automated deduction, verification of relational properties and software evolution, verification of information-flow properties, formal methods for the development of CPS.

F. Lanzinger, C. Martin, F. Reiche, S. Teuber, R. Heinrich & A. Weigl (2024): *Quantifying Software Correctness by Combining Architecture Modeling and Formal Program Analysis.* – SAC '24: Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing, 2024: 1702-1711.

J. Schiffl & B. Beckert (2024): *A Practical Notion of Liveness in Smart Contract Applications.* – 5th International Workshop on Formal Methods for Blockchains (FMBC 2024). Open Access Series in Informatics (OASIcs), 118: 8:1-8:13.

Fellows

Selected Publications

Prof. Dr.-Ing. habil. Jürgen Beyerer

- Chair of the Vision and Fusion Lab at the Institute for Anthropomatics and Robotics (IAR) at KIT, Head of the Fraunhofer IOSB
- PhD in Engineering (U Karlsruhe (TH), 1994).
- Professor of Computer Science (KIT, since 2004).

Automated visual inspection and image processing, signal processing, AI, pattern recognition, systems theory, information fusion, metrology, man-machine interaction, security, robotics.

P.G. Wagner, P. Birnstill & J. Beyerer (2024): *DDS Security+: Enhancing the Data Distribution Service With TPM-based Remote Attestation.* – ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security, art. no. 159: 11 pp.

T. Zander, J. Wohnig & J. Beyerer (2024): *Understanding, Describing, and Mitigating the Flow of Personal Data in ROS 2 Systems to Comply with the GDPR and Beyond.* – 2024 IEEE International Conference on Advanced Robotics and Its Social Impacts (ARSO): 146-152.

Jun.-Prof. Dr. Emilia Grass

- Research Group Building Healthcare Resilience against Cyber-Attacks at KIT
- PhD in Operations Research (TU Hamburg, 2018).
- Jun. Professor (KIT, since 2024).

Resilience of critical infrastructures, cybersecurity, disaster management, decision support under uncertainty.

E. Grass, C. Pagel, S. Crowe & S. Ghafur (2024): *A Stochastic Optimisation Model to Support Cybersecurity within the UK National Health Service.* – Journal of the Operational Research Society, 76 (7): 1379-1390.

Y. Angler, S: Flessa, E. Grass & O. Goetz (2025): *Assessing the Impact of Technology Partners on the Level of Cyberattack Damage in Hospitals.* – Health Policy and Technology, 14 (1), 100955: 16 pp.

Prof. Dr. Veit Hagenmeyer

- Director of the Institute for Automation and Applied Informatics (IAI) at KIT
- PhD in Automation (U Paris XI, 2002).
- Professor of Energy Informatics, KIT (since 2014).

Energy informatics, automation of technical processes, control engineering, cybernetics, simulation.

G. Elbez, G., K. Nahrstedt & V. Hagenmeyer (2023): *Early Attack Detection for Securing GOOSE Network Traffic.* – IEEE Transactions on Smart Grid, 15 (1): 899-910.

G. Sánchez, G. Elbez & V. Hagenmeyer (2024): *Attacking Learning-based Models in Smart Grids: Current Challenges and New Frontiers.* – e-Energy '24: Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems, 2024: 589-595.

Fellows

Selected Publications

Prof. Dr. Hannes Hartenstein

- Research Group Decentralized Systems and Network Services (DSN) at KIT
- PhD Computer Science (U Freiburg, 1998).
- Professor of Computer Science (KIT, since 2003).

Decentralized systems, security engineering and management, discrete event modeling and simulation.

F. Jacob & H. Hartenstein (2025): *To the Best of Knowledge and Belief: On Eventually Consistent Access Control.* – CODASPY '25: Proceedings of the Fifteenth ACM Conference on Data and Application Security and Privacy: 107-118.

N. Marx, F. Jacob & H. Hartenstein (2025): *Proof-Carrying CRDTs allow Succinct Non-Interactive Byzantine Update Validation.* – PaPoC '25: Proceedings of the 12th Workshop on Principles and Practice of Consistency for Distributed Data: 15–21.

Prof. Dr.-Ing. Anne Koziolek

- Research Group Modelling for Continuous Software Engineering (MCSE) at KIT
- PhD in Informatics (KIT, 2011).
- Professor of Software Engineering (KIT, since 2013).

Security requirements, tracelink recovery and inconsistency detection with natural language processing.

J. Keim, S. Corallo, D. Fuchß, T. Hey, T. Telge & A. Koziolek (2024): *Recovering Trace Links Between Software Documentation and Code.* – Proceedings of the 2024 IEEE/ACM 46th International Conference on Software Engineering, 2024: 2655-2667.

J. Keim, S. Corallo, D. Fuchß & A. Koziolek (2023): *Detecting Inconsistencies in Software Architecture Documentation Using Traceability Link Recovery.* – 2023 IEEE 20th International Conference on Software Architecture (ICSA): 141-152.

Prof. Dr.-Ing. Peter Mayer

- Research Group Human and Societal Factors (HSF) at KIT and Section Artificial Intelligence, Cybersecurity and Programming Languages at University of Southern Denmark
- PhD in Usable Security (KIT, 2019).
- Assistant Professor of Cybersecurity and Privacy (U Southern Denmark, since 2023).

Cybersecurity, privacy, usable security, human factors, security awareness, authentication. password managers, security notifications, e-mail security, security by design, cyberwarfare, security of critical infrastructure.

Y. Zou, K. Le, P. Mayer, A. Acquisti, A.J. Aviv & F. Schaub (2024): *Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory.* – ACM Transactions on Computer-Human Interaction, 31 (5): 63-1-63:45.

L. Schöni, N. Roch, H. Sievers, M. Strohmeier, P. Mayer & V. Zimmermann (2025): *It's a Match – Enhancing the Fit between Users and Phishing Training through Personalisation.* – CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, art. no. 592: 3123-3137.

Fellows

Selected Publications

Prof. Dr. Raffaela Mirandola

- Research Group Self-Adaptive Software-Intensive Systems at KIT
- PhD in Computer Science (Tor Vergata U Rome, 1994).
- Professor of Computer Science (KIT, since 2023).

Software performance and reliability engineering, self-adapting systems, model-driven engineering.

M. Camilli & R. Mirandola (2025): *Parametric Falsification of Many Probabilistic Requirements under Flakiness.* – 2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE): 178–190.

M. Camilli, F. Luccioletti, R. Mirandola & P. Scandurra (2024): *Integrated QoS- and Vulnerability-Driven Self-adaptation for Microservices Applications.* – Service-Oriented Computing: 22nd International Conference, ICSOC 2024: 55–71.

Prof. Dr. Jörn Müller-Quade

- Research Group Cryptography and Security at KIT
- PhD in Computer Science (U Karlsruhe (TH), 1998).
- Professor of Cryptography and Security (KIT, since 2008).

Cryptography, secure multiparty computations, quantification of security.

D. Faut, V. Fetzer, J. Müller-Quade, M. Raiber & A. Rupp (2025): *POBA: Privacy-Preserving Operator-side Bookkeeping and Analytics.* – IACR Communication in Cryptology, 2 (2): 1-56.

S. Bayreuther, R. Berger, F. Dörre, J. Mechler & J. Müller-Quade (2024): *Hidden Δ-Fairness: A Novel Notion for Fair Secure Two-Party Computation.* – In: T. Zhu & Y. Li (eds.): Information Security and Privacy. ACISP 2024. Lecture Notes in Computer Science, vol. 14896: 330–349.

Prof. Dr. André Platzer

- Research Group Logic of Autonomous Dynamic Systems at KIT
- PhD in Computer Science (U Oldenburg, 2008).
- Alexander von Humboldt Professor for Logic of Autonomous Dynamic Systems at KIT (since 2022).

Logic of dynamical systems, logic in computer science, cyber-physical systems, programming languages, theorem proving, formal methods.

N. Abou El Wafa & A. Platzer (2024): *Complete Game Logic with Sabotage.* – In: U. Dal Lago & J. Esparza (eds.): LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science, 2024, art. no. 1: 1-15.

A. Kabra, J. Laurent, S. Mitsch & A. Platzer (2024): *CESAR: Control Envelope Synthesis via Angelic Refinements.* – In: B. Finkbeiner & L. Kovács (eds.): Tools and Algorithms for the Construction and Analysis of Systems, TACAS 2024. Lecture Notes in Computer Science, vol. 14570: 144–164.

Fellows

Selected Publications

Prof. Dr. iur. Oliver Raabe

- Research Group Legal Informatics and IT Security Law (ITR) at the Center for Applied Legal Studies (ZAR), KIT
- PhD in Law (U Kiel, 2003); Habilitation in Legal Informatics (KIT, 2015).
- Assoc. Professor (KIT, since 2015).

Privacy law, IT-security law, energy law, legal informatics.

Ch. Werner, N. Brinker & O. Raabe (2022): *Grundlagen für ein gesetzliches IT-Sicherheitsrisikomanagement: Ansätze zur Vereinheitlichung von Rollenmodell, Risikomanagement und Definitionen für das IT-Sicherheitsrecht.* – Computer und Recht, 38 (12): 817-824.

L. Sterz, Ch. Werner & O. Raabe (2023): *Intelligente Verkehrssysteme – IT-Sicherheit in offenen Infrastrukturen Teil 2.* – Recht der Datenverarbeitung, 39 (2): 97–105.

Prof. Dr. Ralf Reussner

- Research Group Dependability of Software-intensive Systems (DSiS) at KIT
- PhD in Computer Science (U Karlsruhe (TH), 2001).
- Professor of Software Engineering (KIT, since 2006).

Software architecture, dependable software, modelling and simulation.

M. Walter, R. Heinrich & R. Reussner (2023): *Architecture-based Attack Path Analysis for Identifying Potential Security Incidents.* – In: B. Tekinerdogan, C. Trubiani, C. Tibermacine, P. Scandurra & C.E. Cuesta (eds.): Software Architecture. ECSA 2023. Lecture Notes in Computer Science, vol. 14212: 37-53.

S. Hahner, R. Heinrich & R. Reussner (2023): *Architecture-based Uncertainty Impact Analysis to Ensure Confidentiality.* – 2023 IEEE/ACM 18th Symposium on Software Engineering for Adaptive and Self-Managing Systems (SEAMS): 126-132.

Dr. Andy Rupp

- Research Group Cryptographic Protocols at KIT and University of Luxemburg and KASTEL SRL
- PhD in Electrical Engineering and Information Sciences (U Bochum, 2008).
- Head of Research Group "Cryptographic Protocols" (U Luxembourg, since 2023).

Cryptographic protocols, privacy-enhancing technologies, provable security, security and privacy in important application domains, anonymous payments and communication.

D. Faut, J. Hesse, L. Kohl & A. Rupp (2025): *Scalable and Fine-Tuned Privacy Pass from Group Verifiable Random Functions.* – Proceedings of the 10th IEEE European Symposium on Security and Privacy: 28 pp., in press.

D. Faut, V. Fetzer, J. Müller-Quade, M. Raiber & A. Rupp (2025): *POBA: Privacy-Preserving Operator-side Bookkeeping and Analytics.* – IACR Communication in Cryptology, 2 (2): 1-56.

Fellows

Selected Publications

Prof. Dr.-Ing. Ina Schaefer

- Research Group Test, Validation and Analysis of Software-Intensive Systems (TVA) at KIT
- PhD in Computer Sciences (U Kaiserslautern, 2008).
- Professor of Software Engineering (KIT, since 2022).

Software quality, software variability and evolution, automotive cybersecurity, quantum software engineering, formal methods, correctness-by-construction engineering.

A. Peduri, I. Schaefer & M. Walter (2025): *QbC: Quantum Correctness by Construction.* – Proceedings of the ACM on Programming Languages, 9 (OOPSLA1): 534-562.

T. Runge, M. Servetto, A. Potanin & I. Schaefer (2022): *Immutability and Encapsulation for Sound OO Information Flow Control.* – ACM Transactions on Programming Languages and Systems (TOPLAS), 45 (1): 3-1-3-35.

Dr.-Ing. Gunther Schiefer

- Research Group Digital Privacy at KIT
- PhD in Applied Informatics (KIT, 2015).
- Academic Employee (KIT, since 2000).

Privacy, digital sovereignty, m-business, mobile technologies, e-assessment, security, jurisprudence.

F. Sharevski, M. Mossano, M. Veit, G. Schiefer & M. Volkamer (2024): *Exploring Phishing Threats through QR Codes in Naturalistic Settings.* – Network and Distributed System Security (NDSS) Symposium 2024: 1-17.

F. Rybinski, F. Frister, G. Schiefer & M. Malekzadeh Mahani (2025): Leveraging Large Language Models for Supporting Cyber Threat Analysis. – 2025 International Conference on Recent Advances in Information Systems (ICRAIS), September 10-12, 2025, Pointe aux Piments, Mauritius, Progress in IS, Springer: upcoming.

Prof. Dr. Indra Spiecker gen. Döhmann

- Chair for Law of Digitization at University of Cologne
- PhD in Law (U Bonn, 2000); Habilitation (U Osnabrück, 2007).
- Professor of Law (KIT, 2007–2013); U Frankfurt, 2013–2024; U Cologne, since 2024).

Data protection law, IT security law, environmental law, administrative law, legal theory.

U. Simon, I. Spiecker gen. Döhmann & U. v. Luxburg (2024): *Generative AI – Beyond Euphoria and Simple Solutions.* – In: German National Academy of Sciences Leopoldina (ed.): Discussion no. 34: 30 pp.

I. Spiecker gen. Döhmann, G. Hornung & Sp. Simitis (2025): *Datenschutzrecht. DSGVO/BDSG.* – 2nd ed.: 2.679 pp., Nomos.

Fellows

Selected Publications

Prof. Dr. Thorsten Strufe

- Research Group Privacy and Security (PS) at KIT
- PhD in Computer Science (TU Ilmenau, 2007).
- Professor of IT Security (KIT, since 2019).

Behavioral privacy, anonymous communication, network security.

S. Hanisch, P. Arias-Cabarcos, J. Parra-Arnau, T. Strufe (2025): *Anonymization Techniques for Behavioral Biometric Data: A Survey.* – ACM Computing Surveys, 57 (11): 272:1-272:5.

C. Coijanovic, L. Hetz, K.G. Paterson & T. Strufe (2025): *Sabot: Efficient and Strongly Anonymous Bootstrapping of Communication Channels.* – 32nd ACM Conference on Computer and Communications Security (CCS), Taipeh, Taiwan: 15 pp., accepted.

Prof. Dr. Ali Sunyaev

- Research Group Critical Information Infrastructures (cii) at KIT
- PhD in Computer Science (TU Munich, 2010).
- Professor of Information Infrastructures (TU Munich, since 2024).

Decentralized information systems, trustworthy internet-based systems, digital health.

T. Dehling & A. Sunyaev (2023): *A Design Theory for Transparency of Information Privacy Practices.* – Information Systems Research, 35 (3): 956–977.

D. Jin, N. Kannengießer, S. Rank & A. Sunyaev (2024). *Collaborative Distributed Machine Learning.* – ACM Computing Surveys, 57 (4): 95:1-95:36.

Prof. Dr. Melanie Volkamer

- Research Group SECUSO (Security · Usability · Society) at KIT
- PhD in Computer Science (U Koblenz-Landau, 2008).
- Professor of Security Engineering (KIT, since 2018).

Human factors in security and privacy, mental models, usable security and privacy, awareness, security education.

B.M. Berens, F. Schaub, M. Mossano & M. Volkamer (2024): *Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool.* – CHI '24: Proceedings of the CHI Conference on Human Factors in Computing Systems, 2024, art. no. 826: 1-60.

J. Petelka, B. Berens, C. Sugatan, M. Volkamer & F. Schaub (2025): *Restricting the Link: Effects of Focused Attention and Time Delay on Phishing Warning Effectiveness.* – Proceedings of the IEEE Symposium on Security and Privacy (SP), 2025: 55-73.

Fellows

Selected Publications

Prof. Dr. Marcus Wiens

- Chair of General Business Administration, in particular Innovation and Risk Management at TU Bergakademie Freiberg
- PhD in Economics (Bundeswehr University Munich, 2012); Habilitation in Business Administration (KIT, 2021).
- Chair of Business Administration (TU Bergakademie Freiberg, since 2021).

Economic and systemic risk and innovation management, critical infrastructure protection, cooperative approaches to resilience, risk, and innovation management.

H. Rajabzadeh & M. Wiens (2024): *Resilient and Sustainable Energy Supply Chains: Insights on Sourcing and Pricing Strategies in a Non-collaborative and Collaborative Environment.* – International Journal of Production Research, 62 (24): 9011-9042.

F.K. Kaiser, U. Dardik, A. Elitzur, P. Zilberman, N. Daniel, M. Wiens, F. Schultmann, Y. Elovici & R. Puzis (2023): *Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graphs.* – IEEE Transactions on Dependable and Secure Computing, 20 (6): 4793-4809.

Prof. Dr. Christian Wressnegger

- Research Group Artificial Intelligence & Security (IntelliSEC) at KIT
- PhD in Computer Science (TU Braunschweig, 2008).
- Professor of Computer Science (KIT, since 2025).

Security of (X)AI, AI for IT security.

M. Noppel & C. Wressnegger (2024): *SoK: Explainable Machine Learning in Adversarial Environments.* – 2024 IEEE Symposium on Security and Privacy (SP): 2441-2459.

Q. Zhao & C. Wressnegger (2025): *Two Sides of the Same Coin: Learning the Backdoor to Remove the Backdoor.* – Proceedings of the AAAI Conference on Artificial Intelligence, 39 (21): 22804-22812.

Prof. Dr. Martina Zitterbart

- Research Group at Institute of Telematics (TM) at KIT
- Doctoral degree in Computer Science (U Karlsruhe (TH), 1990).
- Professor of Computer Science (KIT, since 2001).

Computer networks, protocols and architectures, internet of things, network security, software-defined networking.

S. Kopmann & M. Zitterbart (2024): *Importance Analysis of Micro-Flow Independent Features for Detecting Distributed Network Attacks.* – IEEE Transactions on Network and Service Management, 21 (6), 5947-5957.

F. Neumeister & M. Zitterbart (2024): *TRUST Issues: Multicast and Integrity Protection for the TRUST Redundancy Mechanism.* – 2024 IEEE International Conference on Industrial Technology (ICIT): 6 pp.

Fellows

Selected Publications

Prof. Dr. J. Marius Zöllner

- Research Group Applied Technical Cognitive Systems at KIT
- PhD in Computer Science (U Karlsruhe (TH), 1990).
- Professor for Computer Science (KIT, since 2016).

Autonomous driving, service robotics, technical cognitive systems, machine learning.

S. Pavlitska, S. Müller & J.M. Zöllner (2024): *Evaluating Adversarial Attacks on Traffic Sign Classifiers beyond Standard Baselines.* – 2024 International Conference on Machine Learning and Applications (ICMLA): 1390–1395.

N. Polley, S. Pavlitska, Y. Boualili, P. Rohrbeck, P. Stiller, A.K. Bangaru & J.M. Zöllner (2024): *TLD-READY: Traffic Light Detection – Relevance Estimation and Deployment Analysis.* – 2024 IEEE 27th International Conference on Intelligent Transportation Systems (ITSC): 3800–3806.

TT-Prof. Dr. Frederike Zufall

- Chair for Public Law and Computer Science at the Center for Applied Legal Studies (ZAR), KIT
- PhD in Law (Humboldt U Berlin, 2015).
- Chair for Public Law and Computer Science (KIT, since 2023).

Computational law, AI and law

J. Tian-Zheng Wei, F. Zufall & R. Jia (2024): *Operationalizing Content Moderation "Accuracy" in the Digital Services Act.* – AIES '24: Proceedings of the 2024 AAAI/ACM Conference on AI, Ethics, and Society: 1527-1538.

F. Ludwig, T. Zesch & F. Zufall (2025): *Conditioning Large Language Models on Legal Systems? Detecting Punishable Hate Speech.* – arXiv: 2506.03009: 14 pp.

Impressions III

Demonstrator Setup and Preparation

Pascal Birnstill explaining the CARM demonstrator: '"Continuous Automated Risk Management System for Industrial Networks".

KIT
HELMHOLTZ
Continuous Automated Risk Management (CARM) System for Industrial Networks

Matin Fallahi and Philipp Matheis prepare for demonstrating "Risk-based Authentication for Virtual Reality Using Brainwave Biometrics".

Marc Leinweber, Andy Rupp, Hannes Hartenstein, and Matthias Grundmann discussing the demonstrator "Methods for Privacy-Preserving and Fair Ticketing for Europe-Scale Mobility-as-a-Service", May 2025.

Young Talents

A number of promising scientific careers have started in **KASTEL Security Research Labs** or are continuing in this productive research environment. Other scientists have been able to continue their careers at other reputable research institutions based on their skills and experience. We have highlighted some impressive examples in this section.

Prof. Dr. Patricia Arias Cabarcos

Patricia obtained her PhD in Telematic Engineering from the University Carlos III in Madrid in 2013 and stayed there as an assistant professor until 2018. By 2019, she was also a Humboldt Fellow at the University of Mannheim. After joining KASTEL, Patricia has been a **KASTEL SRL Fellow**, Topic ESS PI and **professor at the University of Paderborn** since 2021, where she heads the **IT Security Group**.

Dr. Alessandro Erba

As a **YIG Preparation Program Fellow 2025** at KIT, Alessandro works at KASTEL within the **IntelliSEC** and **ESS Mobility labs**, focusing on Cyber-Physical Systems Security. He earned his PhD from Saarland University (CISPA) before joining KIT. Named a CPS Rising Star in 2024, his research has received multiple Best Paper Awards. Alessandro has also held visiting research positions in the USA and Singapore.

Jun.-Prof. Dr. Emilia Grass

Emilia leads a **Helmholtz Investigator Group** "Building Network Resilience in Healthcare against Cyber-Attacks" as a junior professor in the Topic ESS and as a **KASTEL SRL Fellow**. With a background in business administration and mathematics, she completed her PhD on numerical algorithms in disaster management at TU Hamburg in 2018. Before joining KIT, she was a postdoc at the University of Mannheim and Imperial College London, where she remains a guest lecturer.

Prof. Dr. Robert Heinrich

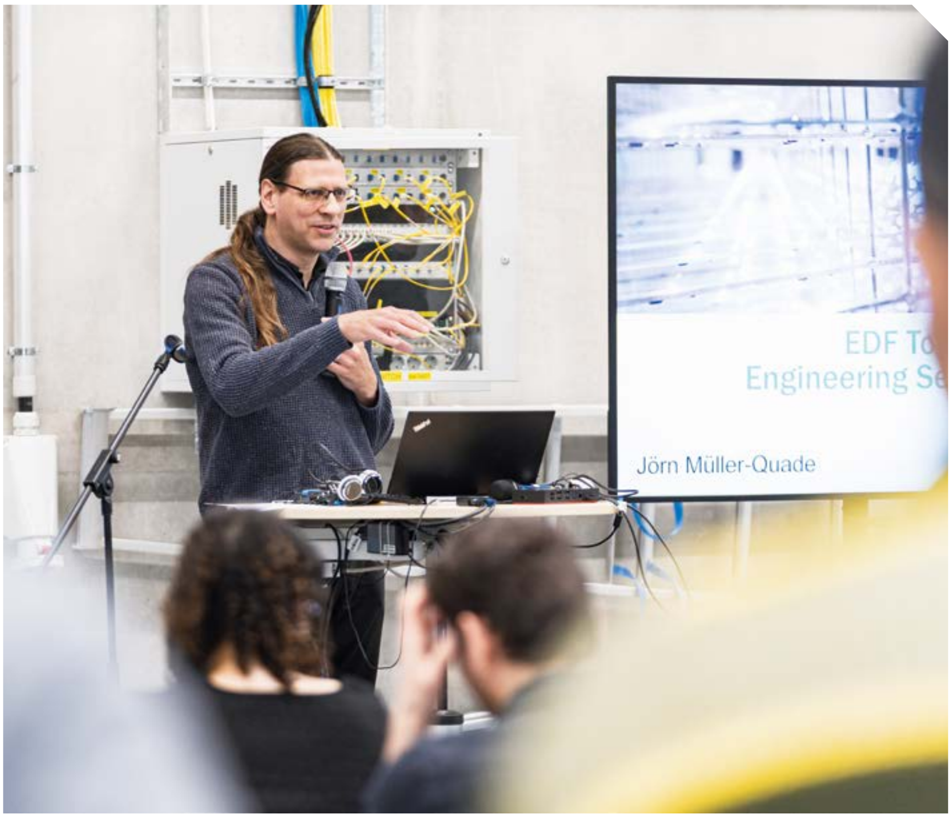
Robert received a doctoral degree from Heidelberg University and a habilitation from Karlsruhe Institute of Technology (KIT). He leads the **Quality-driven System Evolution research group** at KIT. Robert accepted an offer of the **W3-professorship for Software Engineering at Ulm University** starting in April 2025.

Prof. Dr.-Ing. Peter Mayer

As a postdoc, Peter held the role of a coordinator of the "Human and Societal Factors" Research Group at the Topic ESS. Since 2023, he is an **assistant professor for usable security at the University of Southern Denmark**. Peter is still associated researcher at KIT contributing with his research as a **KASTEL SRL Fellow** and a Topic ESS PI.

Prof. Dr. Christian Wressnegger

After beginning his career in cybersecurity in industry, Christian "switched sides" to academia and leads the **"Artificial Intelligence & Security" (IntelliSEC) group** at KIT, specializing in artificial intelligence applications in cybersecurity. From 2020 to 2024, he was tenured professor at KIT, and in 2025, he became **full professor for IT security** and **co-spokesperson of the Topic ESS**.



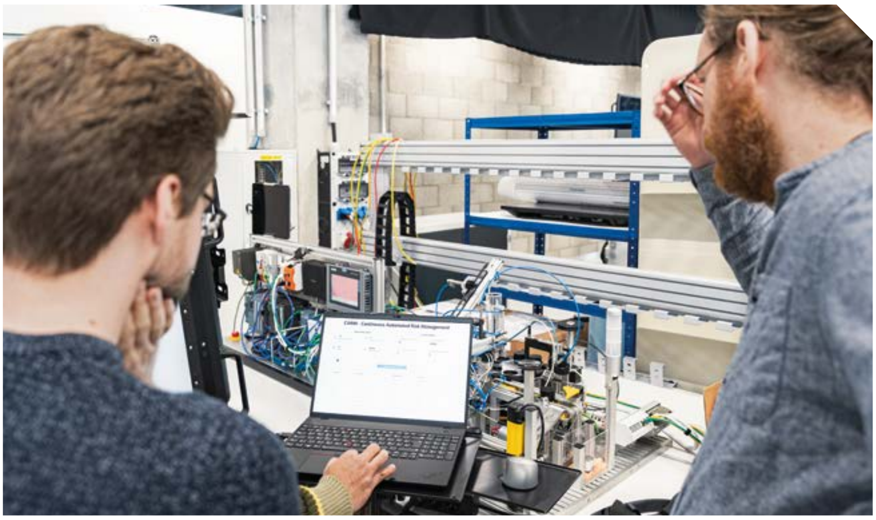
Topic Office manager Mario Strefler discussing the presentation of the research results, May 2025.

KASTEL

Highlights 2024|2025

Impressions IV

Demonstrators Illustrating Our IT Security Research



"Continuous Automated Risk Management (CARM) System for Industrial Networks".

Private Set Intersection

Idea

Private set intersection allows mutually distrusting parties to compute the intersection of two sets.

Participating in a private set intersection should not allow a corrupted party to learn anything about an honest party's input that it cannot compute from its own input and the intersection.

This can be achieved with cryptography or with security hardware.

"Secure Computations Using Not-so-Trusted Hardware".

NoPhish Concept and Awareness Measures
Touch the screen to start
KASTEL
KASTEL Security Research Labs

"NoPhish Concept and Awareness Measures".

Selection of 2024 …

CORE A* PAPER

Certified Everlasting Secure Collusion-Resistant Functional Encryption, and More

(Abstract) We study certified everlasting secure functional encryption (FE) and many other cryptographic primitives in this work. Certified everlasting security roughly means the following. A receiver possessing a quantum cryptographic object (such as ciphertext) can issue a certificate showing that the receiver has deleted the cryptographic object and information included in the object (such as plaintext) was lost. If the certificate is valid, the security is guaranteed even if the receiver becomes computationally unbounded after the deletion. Many cryptographic primitives are known to be impossible (or unlikely) to have information-theoretical security even in the quantum world. Hence, certified everlasting security is a nice compromise (intrinsic to quantum). In this work, we define certified everlasting secure versions of FE, compute-and-compare obfuscation, predicate encryption (PE), secret-key encryption (SKE), public-key encryption (PKE), receiver non-committing encryption (RNCE), and garbled circuits. We also present the following constructions:

- Adaptively certified everlasting secure collusion-resistant public-key FE for all polynomial-size circuits from indistinguishability obfuscation and one-way functions.
- Adaptively certified everlasting secure bounded collusion-resistant public-key FE for circuits from standard PKE.
- Certified everlasting secure compute-and-compare obfuscation from standard fully homomorphic encryption and standard compute-and-compare obfuscation.
- Adaptively (resp., selectively) certified everlasting secure PE from standard adaptively (resp., selectively) secure attribute-based encryption and certified everlasting secure compute-and-compare obfuscation.
- Certified everlasting secure SKE and PKE from standard SKE and PKE, respectively.
- Certified everlasting secure RNCE from standard PKE.
- Certified everlasting secure garbled circuits from standard SKE.

T. Hiroka, F. Kitagawa, T. Morimae, R. Nishimaki, T. Pal & T. Yamakawa (2024): Certified Everlasting Secure Collusion-Resistant Functional Encryption, and More. – In: M. Joye & G. Leander (eds.): Advances in Cryptology – EUROCRYPT 2024. Lecture Notes in Computer Science, vol. 14653: 434–456.

CORE A* PAPER

Complete Game Logic with Sabotage

(Abstract) Game logic with sabotage (GLs) is introduced as a simple and natural extension of Parikh's game logic with a single additional primitive, which allows players to lay traps for the opponent. GLs can be used to model infinite sabotage games, in which players can change the rules during game play. In contrast to game logic, which is strictly less expressive, GLs is exactly as expressive as the modal μ-calculus. This reveals a close connection between the entangled nested recursion inherent in modal fixpoint logics and adversarial dynamic rule changes characteristic for sabotage games. A natural Hilbert-style proof calculus for GLs is presented and proved complete using syntactic equiexpressiveness reductions. The completeness of a simple extension of Parikh's calculus for game logic follows.

N. Abou El Wafa & A. Platzer (2024): Complete Game Logic with Sabotage. – LICS '24: Proceedings of the 39th Annual ACM/IEEE Symposium on Logic in Computer Science, art. no. 1: 1–15.

CORE A* PAPER

Quantum Lattice Enumeration in Limited Depth

(Abstract) In 2018, Aono et al. (ASIACRYPT 2018) proposed to use quantum backtracking algorithms (Montanaro, TOC 2018; Ambainis & Kokainis, STOC 2017) to speedup lattice point enumeration. Quantum lattice sieving algorithms had already been proposed (Laarhoven et al., PQCRYPTO 2013), being shown to provide an asymptotic speedup over classical counterparts, but also to lose competitiveness at dimensions relevant to cryptography if practical considerations on quantum computer architecture were taken into account (Albrecht et al., ASIACRYPT 2020). Aono et al.'s work argued that quantum walk speedups can be applied to lattice enumeration, achieving at least a quadratic asymptotic speedup à la Grover search while not requiring exponential amounts of quantum accessible classical memory, as it is the case for sieving. In this work, we explore how to lower bound the cost of using Aono et al.'s techniques on lattice enumeration with extreme cylinder pruning, assuming a limit to the maximum depth that a quantum computation can achieve without decohering, with the objective of better understanding the practical applicability of quantum backtracking in lattice cryptanalysis.

N. Bindel, X. Bonnetain, M. Tiepelt & F. Virdia (2024): Quantum Lattice Enumeration in Limited Depth. – In: L. Reyzin & D. Stebila (eds.): Advances in Cryptology – CRYPTO 2024. Lecture Notes in Computer Science, vol. 14925: 72–106.

BEST PAPER AWARD

On Practical Realization of Evasion Attacks for Industrial Control Systems

(Abstract) In recent years, a number of evasion attacks for Industrial Control Systems have been proposed. During an evasion attack, the attacker attempts to hide ongoing process anomalies to avoid anomaly detection. Examples of such attacks range from replay attacks to adversarial machine learning techniques. Those attacks generally are applied to existing datasets with normal and anomalous data, to which the evasion attacks are added posthoc. This represents a very strong attacker, who is effectively able to observe and manipulate data from anywhere in the system, in real-time, with zero processing delay, and no computational constraints. Prior work has shown that such strong attackers are theoretically difficult to detect by most existing countermeasures. So far, it is unclear if such an attack could be practically realized, and if there are challenges that would impair the attacker. In this work, we systematically discuss options for an attacker to mount evasion attacks in real-world ICS, and show the constraints that result from those options. To validate our findings, we design and implement a framework that allows the realization of evasion attacks and anomaly detection for ICS emulation. We demonstrate practical constraints that arise from different settings, and their effect on attack performance. For example, we found that network packet replay might trigger network errors, which will result in unexpected spoofing patterns.

A. Erba, A.F. Murillo, R. Taormina, S. Galelli & N.O. Tippenhauer (2024): On Practical Realization of Evasion Attacks for Industrial Control Systems. – RICSS '24: Proceedings of the 2024 Workshop on Re-design Industrial Control Systems with Security: 9–25.

CORE A* PAPER

Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory.

(Abstract) We draw on the Protection Motivation Theory (PMT) to design interventions that encourage users to change breached passwords. Our online experiment (*n* = 1,386) compared the effectiveness of a threat appeal (highlighting the negative consequences after passwords were breached) and a coping appeal (providing instructions on changing the breached password) in a 2 × 2 factorial design. Compared to the control condition, participants receiving the threat appeal were more likely to intend to change their passwords, and participants receiving both appeals were more likely to end up changing their passwords. Participants' password change behaviors are further associated with other factors, such as their security attitudes (SA-6) and time passed since the breach, suggesting that PMT-based interventions are useful but insufficient to fully motivate users to change their passwords. Our study contributes to PMT's application in security research and provides concrete design implications for improving compromised credential notifications.

Y. Zou, K. Le, P. Mayer, A. Acquisti, A.J. Aviv & F. Schaub (2024): Encouraging Users to Change Breached Passwords Using the Protection Motivation Theory. – ACM Transactions on Computer-Human Interaction, 31 (5): 63:1–63:45.

CORE A* PAPER

Collaborative Distributed Machine Learning

(Abstract) Various collaborative distributed machine learning (CDML) systems, including federated learning systems and swarm learning systems, with different key traits were developed to leverage resources for the development and use of machine learning models in a confidentiality-preserving way. To meet use case requirements, suitable CDML systems need to be selected. However, comparison between CDML systems to assess their suitability for use cases is often difficult. To support comparison of CDML systems and introduce scientific and practical audiences to the principal functioning and key traits of CDML systems, this work presents a CDML system conceptualization and CDML archetypes.

D. Jin, N. Kannengießer, R. Rank & A. Sunyaev (2024): Collaborative Distributed Machine Learning. – ACM Computing Surveys, 57 (4): 95:1–95:36.

BEST PAPER AWARD

Model-Manipulation Attacks Against Black-Box Explanations

(Abstract) The research community has invested great efforts in developing explanation methods that can shed light on the inner workings of neural networks. Despite the availability of precise and fast, model-specific solutions (”white-box” explanations), practitioners often opt for model-agnostic approaches (”black-box” explanations). In this paper, we show that users must not rely on the faithfulness of black-box explanations even if requests verifiably originate from the model in question. We present Makrut, a model-manipulation attack against the popular model-agnostic, black-box explanation method LIME. Makrut exploits the discrepancy between soft and hard labels to mount different attacks. We (a) elicit uninformative explanations for the entire model, (b) ”fairwash” an unfair model, that is, we hide the decisive features in the explanation, and (c) cause a specific explanation upon the presence of a trigger pattern implementing a neural backdoor. The feasibility of these attacks emphasizes the need for more trustworthy explanation methods.

A. Hegde, M. Noppel & C. Wressnegger (2024): Model-Manipulation Attacks Against Black-Box Explanations. – 2024 Annual Computer Security Applications Conference (ACSAC): 974–987.

First ‘KASTEL Controversial’ Panel Discussion: Privacy-preserving Surveillance

Data retention is currently a big issue. How can we ensure that the private rights of citizens are protected in the case of online surveillance by law enforcement authorities? This question was discussed by experts at the first ‘KASTEL Controversial’ panel discussion:

- Tomke Beddies, Head of the Cybercrime Center Karlsruhe, founded in 2024,
- Jan Wacke, Deputy Data Protection Commissioner of Baden-Württemberg,
- Manuel Atug, net activist, and
- Jörn Müller-Quade, Spokesperson of KASTEL SRL.

The event took place on November 21, 2024 at the Chamber of Commerce and Industry (IHK) Karlsruhe and was hosted by KASTEL Security Research Labs.

Some of 2025 …

DISTINGUISHED PAPER AWARD

DUMPLING: Fine-grained Differential JavaScript Engine Fuzzing

(Abstract) Web browsers are ubiquitous and execute untrusted JavaScript (JS) code. JS engines optimize frequently executed code through just-in-time (JIT) compilation. Subtly conflicting assumptions between optimizations frequently result in JS engine vulnerabilities. Attackers can take advantage of such diverging assumptions and use the flexibility of JS to craft exploits that produce a miscalculation, remove bounds checks in JIT compiled code, and ultimately gain arbitrary code execution. Classical fuzzing approaches for JS engines only detect bugs if the engine crashes or a runtime assertion fails. Differential fuzzing can compare interpreted code against optimized JIT compiled code to detect differences in execution. Recent approaches probe the execution states of JS programs through ad-hoc JS functions that read the value of variables at runtime. However, these approaches have limited capabilities to detect diverging executions and inhibit optimizations during JIT compilation, thus leaving JS engines under-tested.

We propose DUMPLING, a differential fuzzer that compares the full state of optimized and unoptimized execution for arbitrary JS programs. Instead of instrumenting the JS input, DUMPLING instruments the JS engine itself, enabling deep and precise introspection. These extracted fine-grained execution states, coined as (frame) dumps, are extracted at a high frequency even in the middle of JIT compiled functions. DUMPLING finds eight new bugs in the thoroughly tested V8 engine, where previous differential fuzzing approaches struggled to discover new bugs. We receive $11,000 from Google's Vulnerability Rewards Program for reporting the vulnerabilities found by DUMPLING.

L. Wachter, J. Gremminger, C. Wressnegger, M. Payer & F. Toffalini (2025): DUMPLING: Fine-grained Differential JavaScript Engine Fuzzing. – Network and Distributed System Security (NDSS) Symposium 2025: 1–17.

CORE A* PAPER

Learning the Backdoor to Remove the Backdoor

(Abstract) The community has recently developed various training-time defenses to counter neural backdoors introduced through data poisoning. In light of the observation that a model learns poisonous samples responsible for the backdoor easier than benign samples, these approaches either use a fixed threshold of the training loss for splitting or iteratively learn a reference model as an oracle for identifying benign samples. In particular, the latter has proven effective for anti-backdoor learning. Our method, HARVEY, leverages a similar yet crucially different technique: learning an oracle for poisonous rather than benign samples. Learning a backdoored reference model is significantly easier than learning one on benign data. Consequently, we can identify poisonous samples much more accurately than related work identifies benign samples. This crucial difference enables near-perfect backdoor removal as we demonstrate in our evaluation. HARVEY substantially outperforms related approaches across attack types, datasets, and architectures, lowering the attack success rate to the very minimum at a negligible loss in natural accuracy.

Q. Zhao & C. Wressnegger (2025): Two Sides of the Same Coin: Learning the Backdoor to Remove the Backdoor. – Proceedings of the AAAI Conference on Artificial Intelligence, 39 (21): 22804–22812.

CORE A* PAPER

LiSSA: Toward Generic Traceability Link Recovery through Retrieval-Augmented Generation

(Abstract) There are a multitude of software artifacts which need to be handled during the development and maintenance of a software system. These artifacts interrelate in multiple, complex ways. Therefore, many software engineering tasks are enabled – and even empowered – by a clear understanding of artifact interrelationships and also by the continued advancement of techniques for automated artifact linking. However, current approaches in automatic Traceability Link Recovery (TLR) target mostly the links between specific sets of artifacts, such as those between requirements and code. Fortunately, recent advancements in Large Language Models (LLMs) can enable TLR approaches to achieve broad applicability. Still, it is a non-trivial problem how to provide the LLMs with the specific information needed to perform TLR. In this paper, we present LiSSA, a framework that harnesses LLM performance and enhances them through Retrieval-Augmented Generation (RAG). We empirically evaluate LiSSA on three different TLR tasks, requirements to code, documentation to code, and architecture documentation to architecture models, and we compare our approach to state-of-the-art approaches. Our results show that the RAG-based approach can significantly outperform the state-of-the-art on the code-related tasks. However, further research is required to improve the performance of RAG-based approaches to be applicable in practice.

D. Fuchß, T. Hey, J. Keim, H. Liu, N. Ewald, T. Thirolf & A. Koziolek (2025): LiSSA: Toward Generic Traceability Link Recovery through Retrieval-Augmented Generation. – 2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE): 1396–1408.

CORE A* PAPER

Parametric Falsification of Many Probabilistic Requirements under Flakiness

(Abstract) Falsification is a popular simulation-based testing method for Cyber-Physical Systems to find inputs that violate a formal requirement. It employs optimization algorithms to minimize a robustness metric that defines the satisfaction of a given property over an execution trace. Despite falsification representing an established approach, detecting violations considering many, possibly independent, requirements simultaneously, under flaky simulations is an open problem. We address this problem by proposing a novel approach that combines parametric model checking and many-objective optimization. We use parametric model checking to shift part of the complexity of the problem offline. We pre-compute numeric constraints for the satisfaction of all requirements on a parametric specification of the testing scenario. Flaky violations are then detected using many-objective optimization to explore the space of changing factors in the scenario and push the parameters out of all precomputed constraints. The results of our empirical evaluation using four open-source evaluation subjects with increasing complexity (number of requirements) show that our approach can falsify many requirements simultaneously, without hiding their individual contribution. The effectiveness, in terms of quantity and severity of violations, is significantly higher than random search as well as two selected state-of-the-art baseline approaches. Furthermore, the extra offline computation yields a negligible cost.

M. Camilli & R. Mirandola (2025): Parametric Falsification of Many Probabilistic Requirements under Flakiness. – 2025 IEEE/ACM 47th International Conference on Software Engineering (ICSE), 2025: 178–190.

‘EXCELLENT’

“Topic ESS Has Been Rated as Excellent”!

In May 2025, the Topic ESS underwent a Scientific Evaluation by the Helmholtz Research Field Information at KIT. The individual Programs and Topics as well as the Strategic Issues of thr research activities were presented in various sessions during three days. Here, the scientists of Topic ESS were also given the opportunity to present their successes in presentations and during the Scientific Visits at the Karlsruhe Research Factory (“Forschungsfabrik”). According to the review panel, we consider this a great success, particularly because the interdisciplinary approach of our research was highly rated: “Remarkable success in security metrics, combining technical and economic aspects with relevance for legal developments”.

CORE A* PAPER

Restricting the Link: Effects of Focused Attention and Time Delay on Phishing Warning Effectiveness

(Abstract) Phishing warning researchers have proposed two forms of hyperlink restrictions for reducing phishing click-through rates: focused attention, which prevents users from proceeding to a suspicious URL until they click the uncovered link inside the warning; and time delay, which disables link clicking for a short period of time. Both measures aim to draw user attention to the warning and nudge them to carefully evaluate the respective link's URL. However, the effectiveness of these measures has so far not been comparatively evaluated. We conducted a mixed-methods online experiment (n = 1,320) to understand differences in the effectiveness of focused attention and time delay both independently and together. Our study used an instrumented email inbox environment, in which participants were asked to assess emails and email hyper-links. We found that, while both focused attention and time delay reduced click-through rates independently, the strength of these effects were significantly different from each other with focused attention being more effective than time delay. Combining both measures reduced CTR even further. We also found that participants who saw a warning with a time delay were more likely to hover over hyperlinks for longer than those who saw a focused attention warning. We discuss the implications of our findings for the design of anti-phishing warnings.

J. Petelka, B. Berens, C. Sugatan, M. Volkamer & F. Schaub (2025): Restricting the Link: Effects of Focused Attention and Time Delay on Phishing Warning Effectiveness. – 2025 IEEE Symposium on Security and Privacy (SP): 55–73.

CORE A* PAPER

Anonymization Techniques for Behavioral Biometric Data: A Survey

(Abstract) Our behavior – the way we talk, walk, act, or think – is unique and can be used as a biometric trait. It also correlates with sensitive attributes such as emotions and health conditions. With more and more behavior tracking techniques (e.g., fitness trackers, mixed reality) entering our everyday lives, more of our behavior is captured and processed. Hence, techniques to protect individuals' privacy against unwanted inferences are required before such data is processed. To consolidate knowledge in this area, we are the first to systematically review suggested anonymization techniques for behavioral biometric data. We taxonomize and compare existing solutions regarding privacy goals, conceptual operation, advantages, and limitations. Our categorization allows for the comparison of anonymization techniques across different behavioral biometric traits. We review anonymization techniques for the behavioral biometric traits of voice, gait, hand motions, eye gaze, heartbeat (ECG), and brain activity (EEG). Our analysis shows that some behavioral traits (e.g., voice) have received much attention, while others (e.g., eye gaze, brain activity) are mostly neglected. We also find that the evaluation methodology of behavioral anonymization techniques can be further improved.

S. Hanisch, P. Arias-Cabarcos, J. Parra-Arnau & T. Strufe (2025): Anonymization Techniques for Behavioral Biometric Data: A Survey. – ACM Computing Surveys, 57 (11), 272-1–272-54.

CORE A* PAPER

On the Usability of Next-Generation Authentication: A Study on Eye Movement and Brainwave-based Mechanisms

(Abstract) Passwords remain a widely-used authentication mechanism, despite their well-known security and usability limitations. To improve on this situation, next-generation authentication mechanisms, based on behavioral biometric factors such as eye movement and brainwaves have emerged. However, their usability remains relatively under-explored. To fill this gap, we conducted an empirical user study (n = 32 participants) to evaluate three brain-based and three eye-based authentication mechanisms, using both qualitative and quantitative methods. Our findings show good overall usability according to the System Usability Scale for both categories of mechanisms, with average SUS scores in the range of 78.6–79.6 and the best mechanisms rated with an "excellent" score. Participants identified brainwave authentication as particularly more secure yet more privacy-invasive and effort-intensive compared to eye movement authentication.

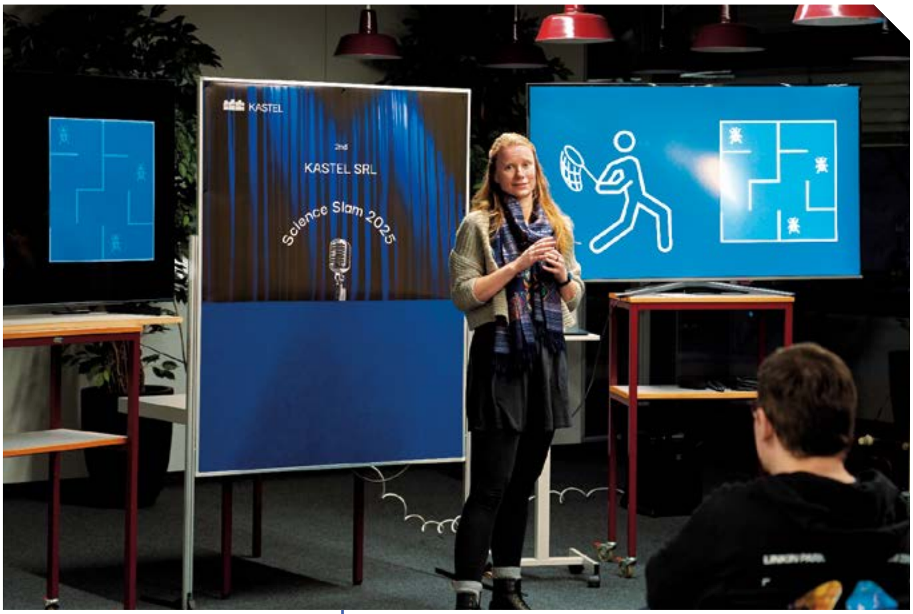
M. Fallahi, P. Arias-Cabarcos & T. Strufe (2025): On the Usability of Next-Generation Authentication: A Study on Eye Movement and Brainwave-based Mechanisms. – CHI EA '25: Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, art. no. 420: 14 pp.

CORE A* PAPER

It's a Match – Enhancing the Fit between Users and Phishing Training through Personalization

(Abstract) Effective training is essential for enhancing users' ability to detect phishing attempts. Personalized training offers huge potential to more closely align training content with individuals' needs and skill levels. In an online study, we assigned N = 342 participants to personalized training or a random training variant to compare their effectiveness. The personalization was based on a phishing proficiency score calculated from factors such as detection ability, knowledge, and security attitude. After training, the participants demonstrated greater proficiency, with an increased ability to detect phishing emails and higher security attitudes. These effects were most pronounced in the personalized condition, demonstrating the potential of personalization to improve training outcomes. Overall, personalized training levelled the playing field, efficiently bringing all groups, regardless of their initial proficiency, to a comparable and desired post-training phishing proficiency level. Finally, we derived recommendations for designing personalized phishing training content and assigning users to suitable training programmes.

L. Schöni, N. Roch, H. Sievers, M. Strohmeier, P. Mayer & V. Zimmermann (2025): It's a Match – Enhancing the Fit between Users and Phishing Training through Personalisation. – CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systemsa, art. no. 592, 25 pp.

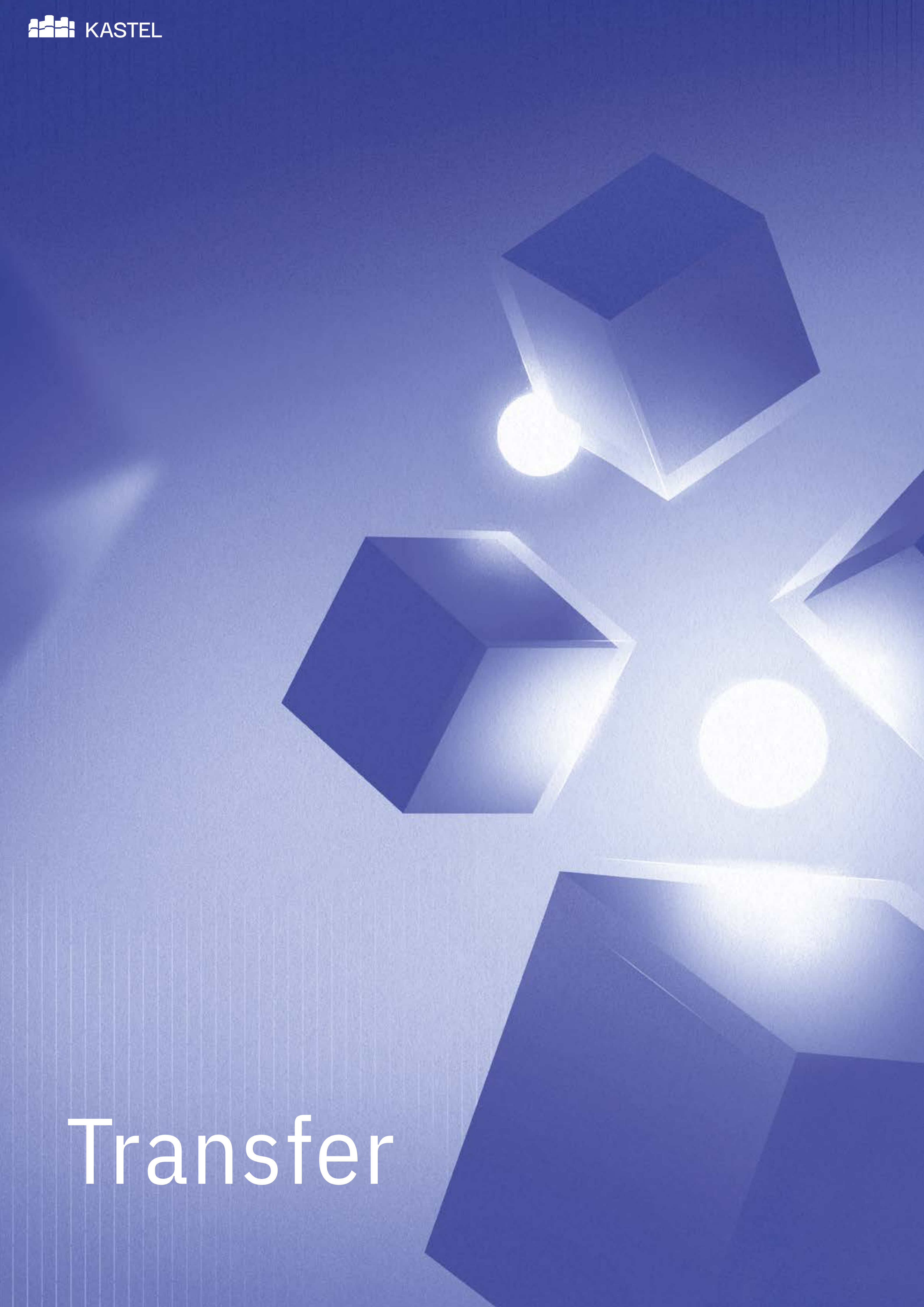


SCIENCE TO TOUCH!

KASTEL SRL Winter Colloquium 2025

'Science to touch' was our idea for the KASTEL SRL Winter Colloquium on January 20, 2025. We started with Marcel Tiepelt's presentation "Sharks, Dinosaurs and Mammals – A History of Cryptography".

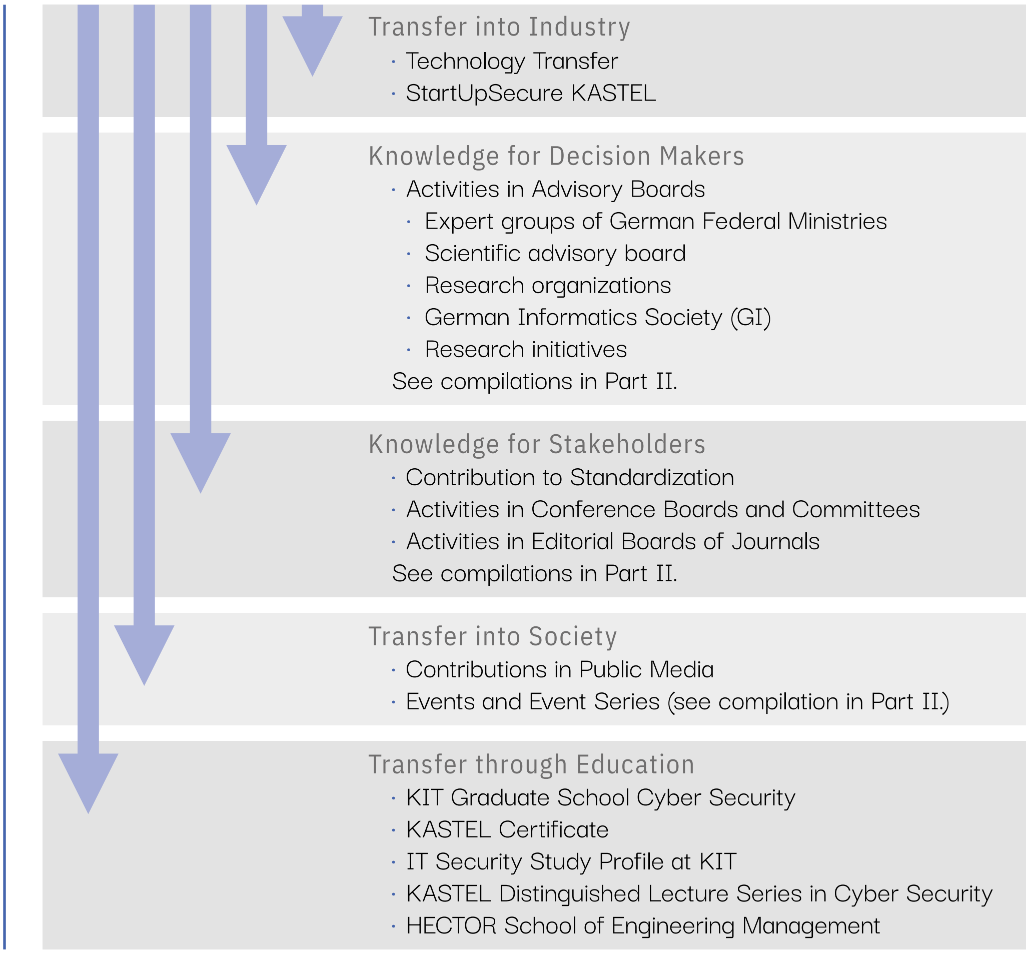
This was followed by the Science Slam with the contributions: "A Fish Called Markov: Illuminating the Path for Blackbox Fuzzers" (Anne Borcherding, photo above), "Consistency Preserving SPLE" (Dirk Neumann), "Behind the Scenes: How Can Contextual Insights Secure Modern Energy Systems?" (Sine Canbolat), and "AI Security: Money, Power (Grid) & Respect" (Gustavo Sanchez Collado). A thrilling evening of exchanging ideas!



Transfer

KASTEL Security Research Labs and Transfer

Research at **KASTEL Security Research Labs** is not just about gaining important insights for the expert community. We are committed to implementing the results of our activities for the immediate benefit of society. This is achieved not only through structural integration into application domains, but also through an explicit focus on the transfer of knowledge to the societal level. We emphasize transfer as a key performance indicator.



Transfer into Industry

- Technology Transfer
- StartUpSecure KASTEL

Knowledge for Decision Makers

- Activities in Advisory Boards
  - Expert groups of German Federal Ministries
  - Scientific advisory board
  - Research organizations
  - German Informatics Society (GI)
  - Research initiatives

See compilations in Part II.

Knowledge for Stakeholders

- Contribution to Standardization
- Activities in Conference Boards and Committees
- Activities in Editorial Boards of Journals

See compilations in Part II.

Transfer into Society

- Contributions in Public Media
- Events and Event Series (see compilation in Part II.)

Transfer through Education

- KIT Graduate School Cyber Security
- KASTEL Certificate
- IT Security Study Profile at KIT
- KASTEL Distinguished Lecture Series in Cyber Security
- HECTOR School of Engineering Management

Impressions V

KASTEL Security Labs

KASTEL Security Lab Energy: Cybersecurity evaluation.

KASTEL Security Lab Mobility: Traffic light recognition at KIT's Campus East.

KASTEL Security Lab Production: Risk management for industrial networks.

Transfer into Industry

Technology Transfer

An important aspect of transfer in KASTEL Security Research Labs is to enable and to accelerate with our research and application areas specific and innovative industrial applications and products. This technology transfer can be impressively illustrated by the following examples.

BSI demonstrators

Demonstrators of current research results have already been transferred and are in use by the Federal Office for Information Security (BSI).

"IIP 2.0"

The projects "IIP 2.0" with S.A.F.E. e.V. (Software Alliance for E-mobility) led to the successful certification resp. legal review of Topic-ESS-developed privacy-enhanced techniques and subsequent broad practical use and impact.

"ISuTest"

Automated vulnerability assessment framework for industrial automation components, see p. 27.

Security architecture of LDACS

In collaboration with the German Aerospace Center (DLR), we analyzed the security architecture of LDACS, Europe's next-generation civil aviation communication system. LDACS not only establishes a reliable data link between civilian aircraft and ground stations but also enables critical functionalities such as positioning and navigation. Our analysis reveals that the protocol achieves a mutually authenticated key exchange that is robust against even the threats posed by quantum computers. This milestone demonstrates LDACS's readiness to meet the evolving security challenges of the aviation industry, ensuring secure and future-proof communication for decades to come.

"Privacy Friendly Apps"

Our societal impact is further attested by the Consumer Protection Award of the German Consumer Protection Organisation for our contributions to e-mail and password security, the Digital Autonomy Award 2022 of the Digital Autonomy Hub for "Privacy Friendly Apps" increasing individual digital sovereignty. Over 60 reference users and organizations refer to NoPhish anti-phishing materials, e.g., the Federal Chancellery, the BSI, the Consumer Organisation NRW e.V., Ruhr University Bochum, and the Police Headquarters in Baden-Württemberg.

Training courses

The expertise built up in security of industrial automation is transferred into training courses for the Fraunhofer Cybersecurity Training Lab, the German Engineering Federation (VDMA), and the International Society of Automation (ISA Europe), in cooperation with the BSI.

"VINKRYPTOR"

In a cooperation, called "VINKRYPTOR", between KIT, FZI, and Mercedes-Benz, a method for the pseudonymization of Vehicle Identification Numbers (VINs) has been developed. The VIN is a unique identifier storing the data associated with the vehicle which should not be passed to third parties. This data protection problem is solved with the new development.

StartUpSecure KASTEL –

An Incubator for Cybersecurity and Privacy

StartUpSecure KASTEL is the KIT-incubator that focuses on start-up projects in the field of IT security. The program aims to provide ongoing support to start-ups from across Germany throughout their entire development cycle. Key areas of support include financial assistance, qualification programs, and raising awareness of cybersecurity issues, aligned with the interests of network partners, potential pilot customers, and investors. In addition, regular events are organized to facilitate networking within the community and to highlight relevant topics and dedicated speakers. StartUpSecure KASTEL works in close cooperation with the KIT-Gründerschmiede, which coordinates and supports all start-up and spin-off activities at KIT.

Supported by:

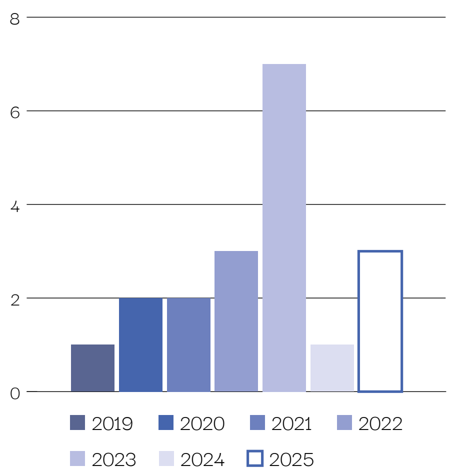
- Federal Ministry of Research, Technology and Space (BMFTR)
- KASTEL Security Research Labs (SRL) / Topic ESS
- KIT-Gründerschmiede

Support for start-ups:

- Consulting for regional & national teams
- Continuing education & technology check: KASTEL SRL / Topic ESS
- Networking with industry, government & start-up ecosystem
- Community management & networking events

Supporting start-ups throughout their entire life cycle!

StartUpSecure KASTEL: Approved projects



StartUpSecure KASTEL & KASTEL Security Research Labs

After a successful initial consultation, researchers and young, innovative startups prepare an abstract outlining their business idea, technology, and more. Experts from the KASTEL SRL and the Helmholtz Topic ESS then assess its alignment with the IT security research program, level of innovation, and market potential, supported by the research coordination of the Topic ESS. If funding is recommended, the founding team receives guidance on funding opportunities and drafts a project outline, with StartUpSecure KASTEL providing active support. Following a successful evaluation, the project outline is submitted to the funding agency along with a positive statement.

Since the incubator's founding, KASTEL SRL has recommended 19 research projects, including three KIT spin-offs. For more information visit:

Transfer into Society

Contributions in Public Media 2024/2025

Interviews, statements, comments, and citations on current topics by KASTEL SRL Fellows and Members in public media, e.g.:

- ***ARD Mittagsmagazin*** *(Mitteldeutscher Rundfunk).* – "*Warum Spanien und Portugal so lange keinen Strom hatten*" (Why Spain and Portugal had no electricity for so long). Veit Hagenmeyer: May 4, 2025.
- ***ARD Tagesschau*** *(Südwestrundfunk).* – "*Vor 40 Jahren: Erste E-Mail erreicht Deutschland*" (40 years ago: First e-mail reaches Germany). Melanie Volkamer: August 3, 2024.
- ***Behörden Spiegel*.** – "*Tipps zur sicheren E Mail-Nutzung*" (Tips for secure e-mail use). Melanie Volkamer: July 30, 2024.
- ***BR24 Deutschland & Welt*** *(Bayerischer Rundfunk).* – "*#Faktenfuchs: Was wissen wir zum Stromausfall in Spanien?*" (What do we know about the electricity blackout in Spain?). Veit Hagenmeyer: May 9, 2024.
- ***Deutschlandfunk Kultur*** – "*Warum wir in Deutschland keine digitalen Wahlen haben*" (Why we don't have digital elections in Germany). Melanie Volkamer: March 1, 2025.
- ***ee news. Das Fachmagazin für Erneuerbare Energien*.** – "*KIT: Die Energiewende verstehen – wie Modelle Zukunft formen*" (KIT: Understanding the energy transition – how models shape the future). Veit Hagenmeyer: March 14, 2025.
- ***Heise online*.** – "*Wie sich Nutzer und Firmen vor Phishing schützen können*" (How users and companies can protect themselves against phishing). Melanie Volkamer: February 26, 2025.
- ***idw Nachrichten. Informationsdienst Wissenschaft*.** – "*KIT-Expertin zum 40. Geburtstag der deutschen E-Mail: 'Cyberangriffe nehmen zu, aber die Schutzmaßnahmen werden besser'*" (KIT expert on the 40th anniversary of German e-mail: 'Cyberattacks are increasing, but protective measures are improving'). Melanie Volkamer: July 29, 2024.
- ***Kabinett online. Journal der Bundesstadt Bonn, Domstadt Köln und Bundeshauptstadt Berlin*.** – "*KIT-Experte zu aktuellem Thema. Einfluss von KI auf demokratische Wahlen. 'Um Missbrauch zu verhindern, bedarf es technologischer und rechtlicher Maßnahmen sowie Stärkung der KI-Kompetenz'*" (KIT expert on current topic. Influence of AI on democratic elections. 'Preventing misuse requires technological and legal measures and strengthening AI expertise'). Thorsten Strufe: January 30, 2025.
- ***Neue Energie. Das Magazin für Klimaschutz und Erneuerbare Energien*.** – "*Cyberattacken bedrohen die Energieversorgung. Dezentrale Strukturen Bergen dabei Risken – und bieten Chancen*" (Cyberattacks threaten the energy supply. Decentralized structures bear risks – and offer opportunities). Ghada Elbez: December 1, 2024.
- ***Science Media Center Germany*.** – "*Stromausfall in Spanien*" *(Electricity blackout in Spain).* Veit Hagenmeyer: April 29, 2025.
- ***Süddeutsche Zeitung*.** – "*Apps, die das Leben schöner machen*" (Apps that make life more beautiful). Melanie Volkamer: February 24, 2025.
- ***SWR Kultur*** *(Südwestrundfunk).* – "*Sichere E-Mails: Das empfiehlt die Forschung*" (Secure e mails: what research recommends). Melanie Volkamer: August 2, 2024.
- ***SWR Kultur*** *(Südwestrundfunk).* – "*Gefahr durch Deepfakes: Wie KI den Wahlkampf beeinflusst*" (Danger from deepfakes: how AI influences the election campaign). Thorsten Strufe: February 19, 2025.
- ***ZfK. Zeitung für kommunale Wirtschaft*.** – "*Blackout in Spanien: Mehr Details zum Ablauf bekannt*" (Blackout in Spain: More details on the course of events known). Veit Hagenmeyer: May 13, 2025.

Transfer through Education

KIT Graduate School Cyber Security

The KIT Graduate School Cyber Security is the central hub of doctoral researchers working across different cybersecurity disciplines within and beyond **KASTEL Security Research Labs** and the Helmholtz Topic ESS. As such, we actively facilitate the exchange of ideas among doctoral researchers and foster connections to postdoctoral and senior researchers.

We organize regular community and networking events:

- KASTEL Distinguished Lecture Series
- Security & Privacy Lunch
- CyberSec Seminar Series

Additionally, we collaborated on organizing the

- MyPhD Workshop

bringing together researchers from 16 German universities and the

- WinterHack 2024 Winter School.

In addition to fostering a vibrant community, we aim to equip our currently 30 members with technical, scientific, and interdisciplinary skills, enabling them to respond effectively to present and future security challenges.

In cooperation with the Karlsruhe House of Young Scientists (KHYS) at KIT, we hence offer workshops on, for instance, interdisciplinary thinking and scientific presentations, and organize writing support measures and dedicate voice coaching to help doctoral researchers make a strong appearance.

The KASTEL Certificate

Karlsruhe Institute of Technology

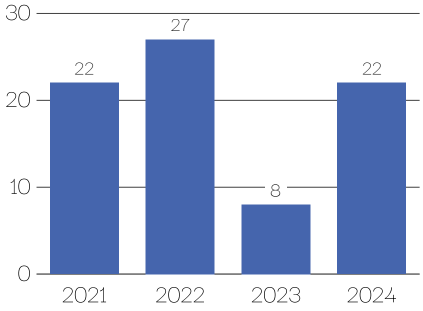
KASTEL

KASTEL Certificate

The requirements of the economy on computer scientists are highly diverse. KIT offers students the opportunity to specialize in various fields. Therefore, it is necessary to issue a certificate that is meaningful to employers and reflects special qualifications that go beyond the choice of "*Vertiefungsfächer*" (specialization areas).

The KASTEL Certificate was introduced in 2013 to provide students with proof of specialization in the field of IT security. It was then partially replaced in 2018 by the introduction of specialization profiles in the Master's degree course in Computer Science, but continues to provide a qualified certificate for graduates of related courses, such as the Master's in Business Informatics. The KASTEL Certificate thus makes it possible to complete a broad, general course of study and at the same time obtain proof of specialization in the field of IT security. The certificate therefore documents a qualification comparable to a specialized Master's degree and enhances the students' competitiveness on the job market.

Number of KASTEL Certificates per year



IT Security Study Profile at KIT

The IT Security study profile focuses on cryptographic processes and especially on their use in complex IT systems. Security plays a central role in this, as do legal aspects such as data protection, privacy, and the needs and limits of state surveillance in the use of security systems. Graduates of the "IT Security" study profile should acquire knowledge of cryptographic procedures and, above all, their use in complex IT systems. Through additional competencies, e.g., from law, legal boundary conditions of IT security such as data protection, privacy, as well as demands and limits of state monitoring in the use of security systems are taught; graduates are enabled to assess these and take them into account in the development of IT security systems.

The "IT Security" study profile supports Master's students by offering courses in the relevant topics. A complete list of lectures, seminars, practical courses, and practice by **KASTEL Security Research Labs** Fellows and Members is compiled in Part II.

KASTEL Distinguished Lecture Series in Cyber Security

KASTEL Security Research Labs and the KIT Graduate School Cyber Security jointly organize the "KASTEL Distinguished Lecture Series in Cyber Security". Several times a year, we invite outstanding national and international speakers who provide insight into their cutting-edge research.

The research issues covered in the presentations are manifold, spanning the breadth of all disciplines and research domains involved in cybersecurity research at KIT. Additionally, the Lecture Series is designed to

- appeal to the interests of a diverse audience,
- advocate for interdisciplinary research, and
- strike a balance between academic and industry perspectives.

Since 2021, we have been able to recruit eight experienced scientists to speak on current research topics and thus give KASTEL SRL scientists insight into specific problem areas.

Program 2025 and beyond

- February 12, 2025:
  Andreas Zeller
  (CISPA Helmholtz Center for Information Security and Saarland University, Saarbrücken):
  Personalized Fuzzing.
- November 19, 2025:
  Stefan Katzenbeisser
  (University of Passau, Chair for Computer Engineering)
- February 2026:
  Kenneth Paterson
  (University of Passau, Chair for Computer Engineering)
- April 17, 2026:
  Alvaro A. Cardenas
  (University of California, Santa Cruz, USA, Professor of Computer Science and Engineering)

HECTOR School of Engineering Management

The "HECTOR School of Engineering & Management" is the Technology Business School of the KIT. The Master's program "Information Systems Engineering and Management" also focuses on the issues of "artifical intelligence & data law" and "IT security & privacy".

KASTEL Security Research Labs Fellows and Members actively support the program 2024/2025, e.g., as lecturers:

- Ralf Reussner (Program Director)
- Patricia Arias Cabarcos
- Robert Heinrich
- Jörn Müller-Quade
- Indra Spiecker gen. Döhmann
- Thorsten Strufe
- Ali Sunyaev
- Melanie Volkamer
- Martina Zitterbart
- J. Marius Zöllner

Impressions IV

Demonstrators Illustrating IT Security Research

for Europe-Scale Mobility-as-a-Service
Vision: Seamless Travel Through Europe
Digitalization is the solution and the challenge
Our Contributions

KASTEL SRL research teams at scientific presentations of their work results, May 2025.

More about KASTEL Security Research Labs …

KASTEL Security Research Labs website <kastel-labs.de>

KASTEL Security Research Labs corporate video

Our Downloads

KASTEL Security Research Labs "Insight"

- 2021|2022|2023
- 2023|2024
- Special Issue 2025: Focus on Topic ESS

"KASTEL explains"

- Taurus Wiretapping Affair (03/2024)

"KASTEL konkret"

- Distributed Usage Control in Interactive Assembly Assistance Systems (10/2024)

Follow us on …

… Mastodon
<social.kit.edu/@kastel>

… LinkedIn
<www.linkedin.com/in/kastel-security-research-labs-987793217/>

… Bluesky
<kastel-labs.bsky.social>

KASTEL Security Research Labs

Contact:
KASTEL – Institute of Information Security and Dependability
Topic “Engineering Secure Systems”
Am Fasanengarten 5, 76131 Karlsruhe, Germany
www.kastel-labs.de

KASTEL

Part I: Research & Researchers