KASTEL Security Research Labs

Insight

2023|2024

KASTEL

Part II: Facts & Numbers

Editorial Notes

Published by

KASTEL – Institute of Information Security and Dependability,
Engineering Secure Systems
Head of institute: 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. 21
Karlsruhe Institute of Technology (KIT): p. 5

September 2024

CONTENTS

Part I: Research & Researchers

Part II: Facts & Numbers

Our Success in “Facts & Numbers”

In Part II of our annual report “Insight 2023| 2024” of **KASTEL Security Research Labs**, we would like to present our successes in quantitative terms – in “Facts & Numbers”. The essence of our work is collaboration within the scientific community, which we maintain through joint projects and cooperation initiatives with our partners.

As a new section in this year’s report, we included “Conference boards and committees” and “Editorial boards of journals”. The entries in this section demonstrate the commitment of the Fellows and Members of **KASTEL Security Research Labs** in this field.

Our particular concern, however, is the transfer of our results and knowledge to stakeholders outside of academia. This is why we especially emphasize the transfer of knowledge to society, politics, and the economy. Our involvement in boards and committees, in which we contribute our expertise by providing advice on socially relevant issues serves as an exemplary indicator of our success. Other examples include our contribution to standardization committees and participation in various types of events through which citizens, representatives of politics and industry are informed and trained.

The different chapters presented here are intended to illustrate our engagement and give an impression of the spectrum of our activities.

Prof. Dr. Jörn Müller-Quade

Spokesperson of
KASTEL Security Research Labs

KASTEL

Publications & Awards

Publications

(Number of Researchers 2024 – 174)

	2021	2022	2023
Total number of publications	161	171	182

	2021	2022	2023
Number of peer-reviewed publications	*108*	*123*	*143*
· thereof WoS-/Scopus-indexed publications	*79*	*94*	*105*
· thereof A*-/A-ranked publications (CORE)	*18*	*27*	*34*
· thereof other peer-reviewed publications	*29*	*29*	*38*

	2021	2022	2023
Number of non-peer-reviewed publications	*53*	*48*	*39*

Awards

- "Notable Reviewer Award", IEEE Conference on Secure and Trustworthy Machine Learning (SaTML 2023), February 8–10, 2023, Raleigh, North Carolina, USA: Christian Wressnegger.
- "Most Influential Paper Award", 7th International Conference on the Art, Science, and Engineering of Programming (<Programming> 2023), March 13–17, 2023, Tokyo, Japan.

  S. Schulze, O. Richers & I. Schaefer (2013): Refactoring Delta-oriented Software Product Lines. – AOSD'13: Proceedings of the 2013 ACM on Aspect-Oriented Software Development, Fukuoka, Japan: 73–84.
- "Best Poster Award", 2. Community Congress by StartUpSecure KASTEL, May 11, 2023, Karlsruhe.

  À. Miranda-Pascual & P. Guerra-Balboa (2023): Differentially Private Trajectory Data.
- "EDPL Young Scholar Award", European Data Protection Law Review, 16th International Conference Computers, Privacy & Data Protection (CPDP2023), May 24–26, 2023, Brussels, Belgium: Mona Winau.
- "Best Reviewer Award", 14th ACM International Conference on Future Energy Systems (ACM e-Energy 2023), June 20–23, 2023, Orlando, Florida, USA: Veit Hagenmeyer.
- "First Prize in the PhD 1 category", 2nd Network Engineering Day (NErD'23), July 4, 2023, Universitat Politècnica de Catalunya – BarcelonaTech, Spain: Àlex Miranda-Pascual.
- "Teaching Award 2023, Master in Information Systems Engineering and Management", HECTOR School of Engineering and Management, July 5, 2023, Karlsruhe, 2nd place: Ralf Reussner, 3rd place: Robert Heinrich.
- *"Fellowship für Lehrinnovationen und Unterstützungsangebote in der digitalen Hochschullehre Baden-Württemberg 2023"* (Fellowship for teaching innovations and support services in digital university teaching), Ministry of Science, Research and Arts Baden-Württemberg; Stifterverband für die Deutsche Wissenschaft e.V., July 2023: Anne Koziolek.
- "Best Paper Award", 19th European Conference on Modelling Foundations and Applications (ECMFA 2023), July 20–21, 2023, Leicester, UK.

  J.W. Wittler, T. Saglam & T. Kühn (2023): Evaluating Model Differencing for the Consistency Preservation of State-Based Views. – The Journal of Object Technology, 22 (2): 1–14.
- "Poster Award", 19th Symposium on Usable Privacy and Security (SOUPS 2023), August 6–8, 2023, Anaheim, California, USA.

  A. Hennig, L. Schmidt-Enke, M. Mutter & P. Mayer (2023): Beware of Website Hackers: Developing an Awareness Video to Warn for Website.
- "Distinguished Reviewer Award", 32nd USENIX Security Symposium (USENIX Security '23), August, 9–11, 2023, Anaheim, California, USA: Christian Wressnegger.
- "Best Paper Award", 14th International Conference on Network of the Future (NoF), October 4–6, 2023, Izmir, Turkey.

  S. Kopmann & M. Zitterbart (2023): eMinD: Efficient and Micro-Flow Independent Detection of Distributed Network Attacks. – 2023 14th International Conference on Network of the Future (NoF), Izmir, Turkiye: 159–167.
- "Best Presentation Award", 7th International Conference on System Reliability and Safety (ICSRS 2023), November 22–24, 2023, Bologna, Italy.

  M. Ramadan, G. Elbez & V. Hagenmeyer (2023): Verifiable Certificateless Signcryption Scheme for Smart Grids. – 2023 7th International Conference on System Reliability and Safety (ICSRS), Bologna, Italy: 181–189.
- *"Public Service Fellowship Preis"*, *Alfons- und Gertrud-Kassel-Stiftung*, November 2023, Frankfurt/Main: Indra Spiecker gen. Döhmann.
- "Top Reviewer Award", ACM Conference on Computer and Communications Security (CCS 2023), November 26–30, 2023, Austin, Texas, USA: Patricia Arias Cabarcos.
- "Top Reviewer Award", Annual Computer Security Applications Conference (ACSAC 2023), December 4–8, 2023, Austin, Texas, USA: Christian Wressnegger.
- *"Dissertationspreis"* (Thesis award), Gesellschaft für Datenschutz und Datensicherheit (GDD), November 2023, Cologne.

  S. Thiebes (2022): A Socio-Technical Analysis of Genetic Privacy and its Role in Genetic Data Sharing. – PhD thesis. Department of Economics and Management, KIT, Karlsruhe.
- "YoungWomen4OR Award (YW4OR2023)", WISDOM (Women in Society: Doing Operational Research and Management Science), December 2023: Emilia Grass.
- "IT Innovation Award 2023", Fujitsu NEXT e.V., December 2023, Düsseldorf.

  Y. Erb (2023): From Affordances to Business Value – How Can Organizations Use Fog Computing to Create Business Value? – Master's thesis. Department of Economics and Management, KIT, Karlsruhe.
- "FameLab Germany", Competition for Science Communication, April 12, 2024, Karlsruhe. Silver medal and Audience Prize. Presentation about differential privacy and the anonymization of trajectories: Patricia Guerra Balboa.
- "Distinguished Paper Award", NDSS Symposium on Usable Security and Privacy (USEC 2024), February 26–March 1, 2024, San Diego, California, USA.

  F. Sharevski, M. Mossano, M.F. Veit, G. Schiefer & M. Volkamer (2024): Exploring Phishing Threats through QR Codes in Naturalistic Settings.
- "Most Influential Paper Award", 15th ACM/SPEC International Conference on Performance Engineering (ICPE 2024), May 7–11, 2024, South Kensington, London, UK.

  D. Perez-Palacin & R. Mirandola (2014): Uncertainties in the Modeling of Self-adaptive Systems: a Taxonomy and an Example of Availability Evaluation. – ICPE'14: Proceedings of the 5th ACM/SPEC International Conference on Performance Engineering, Dublin, Ireland: 3–14.

Transfer in Economy & Society

Activities in Advisory Boards

Expert groups of German Federal Ministries

- **Scientific Working Group of the National Cybersecurity Council** (*Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat, Cyber-SR*), headed by the Federal Ministry of the Interior and Community, BMI, and the Federal Ministry for Education and Research, BMBF. Member: Jörn Müller-Quade.
- **Federal Ministry for Economic Affairs and Climate Action, BMWK: Expert group "Transformation of the Automotive Industry"** (*Expertenkreis "Transformation der Automobilwirtschaft"*). Co-chair: Ina Schaefer.
- **Federal Ministry for Economic Affairs and Climate Action, BMWK: "Initative IT Security in Enterprises"** (*Initiative IT-Sicherheit in der Wirtschaft*). Member of Steering Committee: Melanie Volkamer.

Scientific advisory boards

- **acatech – National Academy of Science and Engineering**:
  - **Topic network Safety and Security**. Speaker: Jörn Müller-Quade; Deputy Speaker: Jürgen Beyerer; Member: Indra Spiecker gen. Döhmann.
  - **Topic network Healthcare Technologies**. Member: Indra Spiecker gen. Döhmann.
- **acatech: *Lernende Systeme* – Germany's Platform for Artificial Intelligence** (funded by the BMBF):
  - **Working group "IT Security, Privacy, Legal and Ethical Framework"**, Section "IT-Security and Privacy". Working Group Management: Jörn Müller-Quade; Member: Bernhard Beckert.
  - **Working group "Learning Robotic Systems"**. Working Group Management: Jürgen Beyerer.
  - **Working group "Mobility and Intelligent Transport Systems"**. Member: J. Marius Zöllner.
- **acatech, German National Academy of Sciences Leopoldina, and Union of the German Academies of Sciences and Humanities**:
  - **Initiative "Energy Systems of the Future"** (funded by the BMBF). Member of the Board of Directors: Indra Spiecker gen. Döhmann.
  - **Working Group "Energy prices and security of supply"**. Participant: Indra Spiecker gen. Döhmann.
  - **Working Group "Centralised vs. Decentralised Power Supply"**. Participant: Veit Hagenmeyer.
- **Électricité de France**, Paris, France. Member of the Scientific Advisory Board: Veit Hagenmeyer.
- **Fraunhofer Segment for Defense and Security VVS**. Chairman: Jürgen Beyerer.
- **German National Academy of Sciences Leopoldina**: Focus group Digitisation. Member: Indra Spiecker gen. Döhmann.
- **German Research Foundation** (DFG):
  - **Review Board "Computer Science"**, Subject area "Software Engineering and Programming Languages", Member: Ina Schaefer; Subject area "Data Management, Data-Intensive Systems, Computer Science Methods in Business Informatics", Member: Ali Sunyaev.
  - **Commission for Pandemic Research**. Scientific Member: Jörn Müller-Quade.
- **HRK German Rectors' Conference**, Standing Committee "Digitization". Member: Hannes Hartenstein.

Research organizations

- **ATHENE National Research Center for Applied Cybersecurity**, Darmstadt. Coordinator "Legal Aspects of Privacy and IT Security (LeAP)": Indra Spiecker gen. Döhmann.
- **Center for Critical Computational Studies** (C3S), Goethe University, Frankfurt/Main. Managing Director: Indra Spiecker gen. Döhmann.
- **EIFER – European Institute for Energy Research by EDF and KIT**, Karlsruhe. Member of the Board of Directors: Veit Hagenmeyer.
- **Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB**, Karlsruhe. Head of Institute: Jürgen Beyerer; Members of the Advisory Board: Ralf Reussner, Indra Spiecker gen. Döhmann.
- **FZI Research Center for Information Technology**, Karlsruhe. Member of the Boards of Trustees: Jürgen Beyerer; Members of the Board of Scientific Directors: Bernhard Beckert, Jörn Müller-Quade, Oliver Raabe, Ralf Reussner, Ina Schaefer, J. Marius Zöllner. Research Division "Cybersecurity and Law": Jörn Müller-Quade (Spokesperson), Ingmar Baumgart (Division Manager).
- **ineges – Institute for European Health Care Policy**, Frankfurt/Main. Associated Member: Indra Spiecker gen. Döhmann.
- **Research Center for Data Protection**, Goethe University Frankfurt/Main. Director: Indra Spiecker gen. Döhmann.

Scientific societies

- **German Informatics Society** (GI):
  - Member of Steering Committee and of the Board of Directors: Ali Sunyaev.
  - ***Fachbereich "Sicherheit"*** (security, special field of GI). Member of Steering Committee: Christian Wressnegger.
    - **Special Interest Group "Formal Methods in Software Engineering, Safety and Security"** (FoMSESS). Member of Steering Committee: Bernhard Beckert.
    - **Special Interest Group "Security – Intrusion Detection and Response"** (SIDAR). Member of Steering Committee: Christian Wressnegger.
  - ***Fachbereich "Wirtschaftsinformatik"*** (information systems, special field of GI). Spokesperson: Ali Sunyaev.
  - **Special Interest Group "Communication and Distributed Systems"** (KuVS), GI, *Fachbereich "Betriebssysteme, Kommunikationssysteme, Verteilte Systeme"* (SYS), and *Informationstechnische Gesellschaft im VDE* (ITG). Members of the Extended Steering Board: Thorsten Strufe, Martina Zitterbart.

Research initiatives

- **"AIDOaRt – AI-augmented Automation for DevOps, a model-based framework for continuous development at RunTime in cyber-physical systems"**. EU-project, program Horizon Europe. Member of the Advisory Board: Raffaela Mirandola.
- **e-mobil BW GmbH – State Agency for New Mobility Solutions and Automotive Baden-Württemberg**. Member of the Board of Advisors: J. Marius Zöllner.
- **Fraunhofer Strategic Research Field Artificial Intelligence**. Spokesman: Jürgen Beyerer.
- **"ENSURE"**. Kopernikus project, funded by the Federal Ministry for Education and Research, BMBF. Director: Veit Hagenmeyer.

- **"MEDI:CUS"** – Platform headed by the Ministry of the Interior, Digitalisation and Local Government Baden-Württemberg. Member of the Advisory Board: Emilia Grass.
- **National Research Data Infrastructure for and with Computer Science** (NFDIxCS) (consortium funded by German Research Foundation, DFG, in cooperation with German National Research Data Infrastructure, NFDI). Member of the Executive Board: Anne Koziolek.
- **"RED ROSES – Responsive, Data ecosystem for Resilient and Operational Security Strategies"**. EU-project, program Horizon Europe. Member of the Advisory Board: Marcus Wiens.
- **Schloss Dagstuhl, Leibniz Center for Informatics**, Wadern. Member of Scientific Directorate: Martina Zitterbart; Member of the Advisory Board: Hannes Hartenstein.
- **Test Area Autonomous Driving Baden-Württemberg**. Spokesperson: J. Marius Zöllner.

Contributions to Standardization

National

- ***VDI-Gesellschaft Energie und Umwelt*** (VDI-Association for Energy and Environment): *Fachbereich Energie- und Umwelttechnik: Expertenrat im Richtlinienausschuss* (VDI-EE 4603 Part 3 – Project "*IT-Sicherheit und Informationssicherheit für Betriebsmanagementsysteme in der Energiewirtschaft*" (IT security and information security for operational management systems in the energy industry).
- **Industrial Digital Twin Association e.V.** (IDTA): IDTA Working Group Security, Standardization Asset Administration Shell (AAS) Security.
- **Federal Office for Information Security** (BSI): BSI-CC-PP-0121 Protection Profile for E-Voting Systems for Non-Political Elections: development of common criteria, and protection profile for online voting products.
- ***Deutsche Kommission Elektrotechnik Elektronik Informationstechnik*** (DKE, German Commission for Electrical, Electronic, and Information Technologies): DKE/AK 901.0.42 *KI in der Energietechnik* (AI in energy technology). DKE/AK 952.0.15 *DKE-ETG-ITG Informationssicherheit in der Netz- und Stationsleittechnik* (Information security in network and substation control technology).

International

- **European Committee on Democracy and Governance** (CDDG): Guidelines on the use of information and communication technology (ICT) in electoral processes in Council of Europe member states.
- **OPC Foundation**, Arizona, USA: OPC UA Working Group Secure Elements (SecElem), specification of OPC UA extensions for the use of hardware trust anchors.
- **International Society of Automation** (ISA Europe): ISA99 standards committee (ISA 99 Industrial Automation and Control Systems Security). Training courses for ISA/IEC 62443 series of standards.
- **International Electrotechnical Commission** (IEC): IEC/TC 57: Power systems management and associated information exchange – Data and communication security – standard series IEC 60870-5, IEC 60870-6, IEC 61850, IEC 61970, IEC 61968, and IEC 62351.
- **Digital Governance Standards Institute** (DGSI), Canada: CAN/DGSI 111-1: Online Electoral Voting – Part 1: Implementation of Online Voting in Canadian Municipal Elections.

Conference Boards and Committees

2023

- **IEEE Conference on Secure and Trustworthy Machine Learning** (SaTML 2023), February 9–10, 2023, Raleigh, North Carolina, USA. Member of Program Committee: Christian Wressnegger.
- **GI-Software Engineering** (SE 2023), February 20–24, 2023, Paderborn. Steering Committee Chair: Ralf Reussner; Member of Organization Committee: Robert Heinrich.
- **21st International Conference on Pervasive Computing and Communications** (PerCom 2023), March 13–17, 2023, Atlanta, USA. Member of Program Committee: Patricia Arias Cabarcos.
- **20th IEEE International Conference on Software Architecture** (ICSA 2023), March 13–17, 2023, L'Aquila, Italy. Members of Steering Committee: Anne Koziolek, Ralf Reussner; Member of Organizing Committee: Robert Heinrich; Members of Program Committee: Anne Koziolek, Ralf Reussner, Robert Heinrich.
- **First International Workshop on the Art, Science, and Engineering of Quantum Programming** (QP 2023), March, 13–17, 2023 Tokyo, Japan. Member of Program Committee: Ina Schaefer.
- **2nd International workshop on "Open Source Modelling and Simulation of Energy Systems"** (OMSES 2023), March 27–29, 2023, Jülich. Member of Organizing Committee, Tutorial Chair: Veit Hagenmeyer.
- **14th ACM/SPEC International Conference on Performance Engineering** (ICPE 2023), April 15–19, 2023, Coimbra, Portugal. Members of Program Committee: Anne Koziolek, Ralf Reussner.
- **2023 ACM Web Conference**, April 30–May 4, 2023, Austin, Texas, USA. Member of the Board of Reviewers: Thorsten Strufe.
- **45th International Conference on Software Engineering** (ICSE 2023), May 14–20, 2023, Melbourne, Australia. Members of Track Committee Software Engineering in Practice: Anne Koziolek, Ina Schaefer.
- **16th European Workshop on Systems Security** (EuroSec 2023), May 8–12, 2023, Rome, Italy. Member of Program Committee: Christian Wressnegger.
- **44th IEEE Symposium on Security and Privacy**, May 22–25, 2023, San Francisco, California, USA. Member of Program Committee: Christian Wressnegger.
- **6th Deep Learning Security and Privacy Workshop**, May 25, 2023, San Francisco, California, USA. Member of Program Committee: Christian Wressnegger.
- **IEEE International Conference on Communications** (ICC 2023), May 28–June 1, 2023, Rome, Italy. Member of Technical Program Committee: Ingmar Baumgart.
- **Workshop *"Sicherheit trotz KI"*** (security despite AI), June 1, 2023, Karlsruhe. Member of Program Committee: Christopher Gerking.
- **ACM Symposium on Access Control Models and Technologies** (SACMAT 2023), June 7–9, 2023, Trento, Italy. Member of Technical Program Committee: Hannes Hartenstein.
- **European Interdisciplinary Cybersecurity Conference** (EICC 2023), June 14–15, 2023, Stavanger, Norway. Member of Program Committee: Peter Mayer.
- **14th ACM International Conference on Future Energy Systems** (ACM e-Energy 2023), June 20–23, 2023, Orlando, Florida, USA. Member of Technical Program Committee: Veit Hagenmeyer.
- **5th Interdisciplinary Summerschool on Privacy** (ISP 2023), June 25–30, 2023, Nijmegen, the Netherlands. Member of Steering Committee: Thorsten Strufe.
- **29th International Conference on Automated Deduction** (CADE-29), July 1–4, 2023, Rome, Italy. Trustee: André Platzer.
- **2nd Workshop on Robust Malware Analysis** (WoRMA), July 7, 2023, Delft, the Netherlands. Member of Program Committee: Christian Wressnegger.

- 8th ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2023), July 7–10, 2023, Melbourne, Australia. Member of Program Committee: Thorsten Strufe.
- 23th Privacy Enhancing Technologies Symposium (PETS 2023), July 10–15, 2023, Bristol, UK. Members of Program Committee / Editorial Board: Peter Mayer, Andy Rupp.
- 20th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2023), July 12–14, 2023, Hamburg. Member of Program Committee: Christian Wressnegger.
- 8th Workshop on Inclusive Privacy and Security (WIPS), July 30, 2023, online. Member of Program Committee: Peter Mayer.
- Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023), August 6–8, 2023, Anaheim, California, USA. Member of Technical Papers Committee: Peter Mayer.
- 32nd USENIX Security Symposium, August 9–11, 2023, Anaheim, California, USA. Members of Program Committee: Patricia Arias Cabarcos, Christian Wressnegger; Member of Artifact Evaluation Committee: Yilin Ji.
- 27th ACM International Systems and Software Product Line Conference (SPLC 2023), August 28–September 1, 2023, Tokyo, Japan. Member of Program Committee: Ina Schaefer.
- International Conference on Availability, Reliability, and Security (ARES), August 29–September 1, 2023, Benevento, Italy. Member of Steering Committee: Melanie Volkamer; Members of Program Committee: Ingmar Baumgart, Christian Haas.
- 38th IEEE/ACM International Conference on Automated Software Engineering (ASE 2023), September 11–15, 2023, Kirchberg, Luxembourg. Member of Program Committee: Anne Koziolek.
- 3rd International Workshop on Quantum Software Engineering and Technology (QSET), September 17–22, 2023, Bellevue, Washington, USA. Member of Program Committee: Ina Schaefer.
- 3rd International Workshop on Designing and Measuring Security in Software Architectures (DeMeSSA 2023), September 18–19, 2023, Istanbul, Turkey. Member of Program Committee: Christopher Gerking.
- 17th European Conference on Software Architecture (ECSA 2023), September 18–22, 2023, Istanbul, Turkey. Member of Steering Committee: Raffaela Mirandola; Members of Program Committee: Robert Heinrich, Anne Koziolek, Raffaela Mirandola.
- 4th IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS 2023), September 25–29, 2024, Toronto, Canada. Member of Program Committee: Raffaela Mirandola.
- 28th European Symposium on Research in Computer Security (ESORICS 2023), September 25–29, 2023, The Hague, the Netherlands. Member of Program Committee: Thorsten Strufe.
- ACM/IEEE 26th International Conference on Model-Driven Engineering Languages and Systems (MODELS 23), October 1–6, 2023, Västerås, Sweden. Member of Track Committee Foundations Track: Anne Koziolek.
- Eight International Joint Conference on Electronic Voting (E-Vote-ID 2023), October 3–6, 2023, Luxembourg. Members of Programme Commitee: General Chair: Melanie Volkamer; Track Chair Poster and Demo Session: Michael Kirsten; Track Security, Usability and Technical Issues: Bernhard Beckert.
- The 2023 European Symposium on Usable Security (EuroUSEC 2023), October 16–17, 2023, Copenhagen, Denmark. Members of Steering Committee: Peter Mayer, Melanie Volkamer; Publicity Chair: Anne Hennig; Member of Program Committee: Patricia Arias Cabarcos.
- International Conference on Cooperative Information Systems (CoopIS 2023), October 30–November 3, 2023, Groningen, the Netherlands. Member of Program Committee: Ingmar Baumgart.
- 14th Symposium on Software Performance (SSP 2023), November 6–8, 2023, Karlsruhe. Members of Steering Committee: Anne Koziolek, Ralf Reussner; Members of Organizing Committee: Anne Koziolek, Ralf Reussner (General Chairs), Robert Heinrich (Program Chair).

- Workshop on Privacy in the Electronic Society (WPES), November 26, 2023, Copenhagen, Denmark. Members of Program Committee: Peter Mayer, Thorsten Strufe.
- ACM Conference on Computer and Communications Security (CCS 2023), November 26–30, 2023, Copenhagen, Denmark. Members of Program Committees: Patricia Arias Cabarcos, Andy Rupp, Thorsten Strufe, Christian Wressnegger.
- 16th ACM Workshop on Artificial Intelligence and Security (AISec 2023), November 30, 2023, Copenhagen, Denmark. Member of Program Committee: Christian Wressnegger.
- Annual Computer Security Applications Conference (ACSAC 2023), December 4–8, 2023, Austin, Texas, USA. Member of Organizing Committee: Peter Mayer; Member of Program Committee: Christian Wressnegger.
- 9th International Symposium on Security in Computing and Communications (SSCC), December 18–20, 2023, Bengaluru, India. Member of Technical Program Committee: Ingmar Baumgart.

2024

- GI Software Engineering (SE 2024), February 26–March 1, 2024, Linz, Austria. Steering Committee Chair: Ralf Reussner; Member of Program Committee: Anne Koziolek.
- First International Workshop on the Art, Science, and Engineering of Quantum Programming (QP 2024), March 11–15, 2024, Lund, Sweden. Member of Program Committee: Ina Schaefer.
- 22nd International Conference on Pervasive Computing and Communications (PerCom 2024), March 11–15, 2024, Biarritz, France. Member of Program Committee: Thorsten Strufe.
- 5th International Workshop on Formal Methods for Blockchains (FMBC 2024), April 7, 2024, Luxembourg. Member of Program Committee: Bernhard Beckert.
- 39th ACM/SIGAPP Symposium on Applied Computing (SAC 2024), April 8–12, 2024, Avila, Spain. Member of Technical Program Committee: Thorsten Strufe.
- 2nd IEEE Conference on Secure and Trustworthy Machine Learning (SaTML 2024), April 9–11, 2024, Toronto, Canada. Member of Program Committee: Christian Wressnegger.
- GI SICHERHEIT 2024, April 9–11, 2024, Worms. Program Co-Chair: Christian Wressnegger; Members of Program Committee: Hannes Hartenstein, Rald Reussner; Member of Doctoral Candidates Forum: Peter Mayer.
- FormaliSE 2024, April 12–21, 2024, Lisbon, Portugal. Member of Program Committee: Ina Schaefer.
- 19th International Conference on Software Engineering for Adaptive and Self-Managing Systems (SEAMS 2024), April 14–16, 2024, Lisbon, Portugal. Member of Steering Committee and of Program Committee: Raffaela Mirandola.
- 46th International Conference on Software Engineering (ICSE 2024), April 14–20, 2024, Lisbon, Portugal. Member of Research Track Committee: Raffaela Mirandola.
- 2nd International Workshop on Responsible AI Engineering (RAIE'24), April 16, 2024, Lisbon, Portugal. Member of Program Committee: Niclas Kannengießer.
- Dagstuhl Seminar 24182: Resilience and Antifragility of Autonomous Systems, April 28–May 3, 2024, Wadern. Member of Organizing Committee: Raffaela Mirandola.
- 15th ACM/SPEC International Conference on Performance Engineering (ICPE 2024), May 7–11, 2024, South Kensington, London, UK. Member of Steering Committee: Raffaela Mirandola; Members of Program Committees: Anne Koziolek, Raffaela Mirandola.
- ACM CHI Conference on Human Factors in Computing Systems (CHI 2024), May 11–16, 2024, Honolulu, Hawaii, USA. Associate Chair of Subcommittee Privacy and Security: Melanie Volkamer.
- 2024 ACM Web Conference, May 13–17, 2024, Singapore. Member of the Board of Reviewers: Thorsten Strufe.

- ACM Symposium on Access Control Models and Technologies (SACMAT 2024), May 15–17, 2024, San Antonio, Texas, USA. Member of Technical Program Committee: Hannes Hartenstein.
- 45th IEEE Symposium on Security and Privacy, May 20–23, 2024, San Francisco, California, USA. Members of Program Committee: Thorsten Strufe, Christian Wressnegger.
- 7th Deep Learning Security and Privacy Workshop, May 23, 2024, San Francisco, California, USA. Member of Program Committee: Christian Wressnegger.
- Eurocrypt 2024, May 26–30, 2024, Zurich, Switzerland. Member of Program Committee: Andy Rupp.
- The 20th International Wireless Communications & Mobile Computing Conference (IWCMC 2024), May 27–31, 2024, Ayia Napa, Cyprus. Member of Technical Program Committee: Ingmar Baumgart.
- International Workshop on Privacy and Security in Augmented, Virtual, and eXtended Realities, June 4–7, 2024, Perth, Australia. Program Chair: Thorsten Strufe; Members of Technical Programme Committee: Patricia Arias Cabarcos, Indra Spiecker gen. Döhmann; Web Chair: Simon Hanisch.
- 15th ACM International Conference on Future and Sustainable Energy Systems (ACM e-Energy 2024), June 4–7, 2024, Singapore. Technical Program Committee Chair: Veit Hagenmeyer.
- 21st IEEE International Conference on Software Architecture (ICSA 2024), June 4–8, 2024, Hyderabad, India. Members of Steering Committee: Anne Koziolek, Raffaela Mirandola, Ralf Reussner; Members of Organizing Committee: Anne Koziolek, Raffaela Mirandola; Members of Program Committee: Robert Heinrich, Anne Koziolek, Raffaela Mirandola, Ralf Reussner.
- European Interdisciplinary Cybersecurity Conference (EICC 2024), June 5–6, 2024, Xanthi, Greece. Member of Program Committee: Peter Mayer.
- IEEE International Conference on Communications (ICC 2024), June 9–13, 2024, Denver, Colorado, USA. Member of Technical Program Committee: Ingmar Baumgart.
- International Conference on Evaluation and Assessment in Software Engineering (EASE 2024), June 18–21, 2024, Salerno, Italy. Member of Program Committee: Anne Koziolek.
- International Joint Conference on Automated Reasoning (IJCAR 2024), July 1–6, 2024, Nancy, France. Member of Program Committee: André Platzer.
- 9th IEEE European Symposium on Security and Privacy (EuroS&P), July 8–12, 2024, Vienna, Austria. Member of Organzing Committee: Christian Wressnegger.
- 6th IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS 2024), July 15–18, 2024, Shanghai, China. Member of Program Committee: Jonas Schiffl.
- 24th Privacy Enhancing Technologies Symposium (PETS 2024), July 15–20, 2024, Bristol, UK. Member of Program Committee / Editorial Board: Peter Mayer.
- International Conference on Availability, Reliability, and Security (ARES), July 30–August 2, 2024, Vienna, Austria. Member of Steering Committee: Melanie Volkamer; Members of Program Committee: Ingmar Baumgart, Benjamin Berens, Pascal Birnstill, Christian Haas, Anne Hennig, Maximilian Noppel.
- 1st Workshop on Societal & User-Centered Privacy in AI (SUPA), August 11, 2024, Philadelphia, Pennsylvania, USA. Member of Program Committee: Benjamin Berens.
- Twentieth Symposium on Usable Privacy and Security (SOUPS 2024), August 11–13, 2024, Philadelphia, Pennsylvania, USA. Member of Technical Papers Committee: Peter Mayer; Members of Poster Jury: Anne Henig, Maxime Veit.
- 33rd USENIX Security Symposium, August 14–16, 2024, Philadelphia, Pennsylvania, USA. Member of Program Committee: Christian Wressnegger; Member of Artifact Evaluation Committee: Yilin Ji.

- 50th Euromicro Conference on Software Engineering and Advanced Applications (SEAA 2024), August 28–30, 2024, Paris, France. Member of Program Committee: Christopher Gerking.
- 18th European Conference on Software Architecture (ECSA 2024), September 2–6, 2024, Luxembourg. Member of Steering Committee: Raffaela Mirandola; Member of Organizing Committee: Robert Heinrich; Members of Program Committee: Robert Heinrich, Anne Koziolek, Raffaela Mirandola.
- 26th International Symposium on Formal Methods (FM24), September 9–13, 2024, Milan, Italy. Member of Organizing Committee (PC Chair): André Platzer.
- 5th IEEE International Conference on Autonomic Computing and Self-Organizing Systems (ACSOS 2024), September 16–20, 2024, Aarhus, Denmark. Member of Program Committee: Raffaela Mirandola.
- 29th European Symposium on Research in Computer Security (ESORICS 2024), September 16–20, 2024, Bydgoszcz, Poland. Members of Program Committee: Hannes Hartenstein, Thorsten Strufe.
- First International Workshop on Model Management (MoM), September 22–24, 2024, Linz, Austria. Members of Program Committee: Robert Heinrich, Anne Koziolek.
- The 2024 European Symposium on Usable Security (EuroUSEC 2024), September 30–October 1, 2024, Karlstad, Sweden. Member of Steering Committee: Melanie Volkamer; Members of Program Committee: Patricia Arias Cabarcos, Anne Hennig.
- Ninth International Joint Conference on Electronic Voting (E-Vote-ID 2024), October 2–4, 2024, Tarragona, Spain. Members of Programme Committee including: General Chair: Melanie Voilkamer; Track Chair Poster and Demo Session: Michael Kirsten; Track Security, Usability, and Technical Issues: Bernhard Beckert.
- 49th IEEE Conference on Local Computer Networks (LCN), October 8–10, 2024, Caen, France. Member of Technical Program Committee: Martina Zitterbart.
- Workshop on Privacy in the Electronic Society (WPES), October 14, 2024, Salt Lake City, Utah, USA. Member of Program Committee: Thorsten Strufe.
- ACM Conference on Computer and Communications Security (CCS 2024), October 14–18, 2024, Salt Lake City, Utah, USA. Members of Program Committee: Patricia Arias Cabarcos, Tapas Pal, Thorsten Strufe, Christian Wressnegger.
- 17th ACM Workshop on Artificial Intelligence and Security (AISec 2024), October 18, 2024, Salt Lake City, USA. Members of Program Committee: Maximilian Noppel, Christian Wressnegger.
- 1st International Workshop on Security and Privacy Aspects of Integrated Sensing and Communication (ISAC) in 6G, October 21–24, 2024, Paris, France. Co-Chair: Thorsten Strufe.
- 15th Symposium on Software Performance (SSP 2024), November 6–7, 2024, Linz, Austria. Members of Steering Committee: Anne Koziolek, Ralf Reussner; Member of Program Committee: Robert Heinrich.
- 39. AIK-Symposium Security and Privacy made in Karlsruhe, November 8, 2024, Karlsruhe. Program Chair: Melanie Volkamer.
- 30th International Conference on Cooperative Information Systems (CoopIS 2024), November 19–21, 2024, Porto, Portugal. Member of Program Committee: Ingmar Baumgart.
- 3rd International Conference on Security & Privacy (ICSP 2024), November 20–21, 2024, Jamshedpur, India. Member of Technical Program Committee: Tapas Pal.
- Annual Computer Security Applications Conference (ACSAC 2024), December 9–13, 2024, Waikiki, Hawaii, USA. Member of Organizing Committee: Peter Mayer; Member of Program Committee: Christian Wressnegger.
- Indocrypt 2024, December 18–21, 2024, Chennai, India. Member of Program Committee: Tapas Pal.

Editorial Boards of Journals

- **ACM Formal Aspects of Computing** (FAC). Member of the Editorial Board: André Platzer.
- **ACM Transactions on Privacy and Security** (TOPS). Member of the Editorial Board: Melanie Volkamer.
- **ACM Transactions on Autonomous and Adaptive Systems** (TAAS). Member of the Editorial Board: Raffaela Mirandola.
- **Acta Informatica**, Springer. Member of the Editorial Board: André Platzer.
- **AIRe – Journal of AI Law and Regulation**, Lexxion. Member of the Editorial Board: Indra Spiecker gen. Döhmann.
- ***at – Automatisierungstechnik***, De Gruyter. Member of the Advisory Board: Jürgen Beyerer.
  - Special Issue: Cybersecurity for Industrial Automation and Control Systems (vol. 71, no. 9, 2023). Guest Editors: Jürgen Beyerer, Christian Haas.
- **Business & Information Systems Engineering** (BISE), Springer. Members of the Editorial Board: Ali Sunyaev, Scott Thiebes.
- **Energy Technology**, Wiley. Member of the Editorial Advisory Board: Veit Hagenmeyer.
- **IEEE Transactions on Information Forensics and Security** (TIFS). Member of the Editorial Board (2023): Thorsten Srufe.
- **IEEE Transactions on Software Engineering** (TSE). Member of the Editorial Board: Raffaela Mirandola.
- ***Informatik-Spektrum***, Springer. Member of the Editorial Board: Ralf Reussner.
- **International Journal of Applied Economics, Finance and Accounting**, Online Academic Press. Member of the Editorial Board: Marcus Wiens.
- **Journal of Automated Reasoning**, Springer. Member of the Editorial Board: André Platzer.
- **Journal of Systems and Software**, Elsevier. Special Issues Editor: Raffaela Mirandola.
  - Special Issue: Systems and Software Product Lines of the Future (vol. 199, 2023). Guest Editor: Ina Schaefer.
- ***tm – Technisches Messen***, De Gruyter. Member of the Advisory Board: Jürgen Beyerer.

Further Transfer Activities (selected projects)

Event series and regular activities

- **Project StartupSecure KASTEL** supporting start-ups and spin-offs. Technical expertises of project outlines, in cooperation with incubators at ATHENE, Darmstadt, and CISPA, Saarbrücken.
- **"Cybersecurity Training Lab"** *(Lernlabor Cybersicherheit,* funded by the BMBF) by Fraunhofer Academy. Advanced training for companies in the field of industrial cybersecurity. Trainer: Christian Haas.
- **Seminars** on "Cybersecurity in Accordance with IEC 62443". Association of the German Machinery and Equipment Manufacturing Industry *(Verband Deutscher Maschinen- und Anlagenbau,* VDMA), Institute of Mechanical Engineering. Seminar leader: Christian Haas.
- **Knowledge transfer initiatives "NoPhish" and "Privacy Friendly Apps"**: These initiatives ensure that the findings from research are also incorporated into programs or measures that directly help users. Apps/add-ons are developed that lead to increased security (phishing detection) or improved privacy (PFAs), Research group SECUSO.

- **"VIP Lecture Series"** by KASTEL Mobility Lab with speakers from industry, Karlsruhe.
- **Lectures at KIT "HECTOR School of Engineering Management"** for the Master of Science in Information Systems Engineering and Management, covering information security topics, Karlsruhe.
- **"IT Security Profile"** for Master (M.Sc.) in Informatics at KIT: studies focusing on cryptographic processes and, above all, on their use in complex IT systems, Karlsruhe.
- **"KASTEL Certificate"** for studies in IT security at KIT. The certificate attests that graduates have a special qualification (Diploma, M.Sc., PhD), which is of great interest for future career: 192 certificates have been issued since 2013 (thereof 8 in 2023), Karlsruhe.
- **Interviews, statements, and comments** on current issues by KASTEL SRL Fellows in television and radio stations, as well as for online and print media in Germany, e.g., *ARD Tagesthemen, NDR Plusminus, SWR Aktuell, ZDF "1, 2 oder 3", Baden TV; SWR2, SWR3, WDR 1Live; BR24*, Euractiv.com; *Frankfurter Rundschau, Handelsblatt, Lausitzer Rundschau, Märkische Oderzeitung, Schwäbisches Tagblatt, Südwest Presse, Wirtschaftswoche.*

Events (chronological)

- **Event organization:** "*Datenschutz: Recht haben und Recht bekommen.*" (Data protection: being right and getting right.) Summer Academy of the *Studienstiftung des deutschen Volkes e.V.* (German Academic Scholarship Foundation): Indra Spiecker gen. Döhmann, 2023.
- **"5th Interdisciplinary Summerschool on Privacy"** (ISP 2023), Nijmegen, the Netherlands. Member of Steering Committee: Thorsten Strufe, June 2023.
- **"Disinformation – Danger to Democracy and Technological Countermeasures"**. Moderation of acatec topic conference: Jörn Müller-Quade, December 2023.
- **"*Sichere digitale Teilhabe in der hypervernetzten Welt – Benutzbare IT-Sicherheit*"** (Secure digital participation in the hyperconnected world – Usable IT security). Expert discussion at BMBF: Melanie Volkamer, September 2023.
- **Selection of award winners as a member of the jury**. CAST award *(Förderpreis)* 2023. Competence Center for Applied Security Technology, CAST e.V., Darmstadt: Andy Rupp, October 2023.
- **Research lecture**: "Artificial Intelligence and Regulation, Digitalization and Democracy: A Brazil-European Dialogue", Frankfurt/Main: Indra Spiecker gen. Döhmann, October 2023.
- **Research lecture**: "*Digitalización y cambios constitucionales: fake news y otros desafíos*" (Digitalization and the constitution: fake news and other challenges). Supremo Tribunal Federal (Constitutional Court Brazil), Brasília: Indra Spiecker gen. Döhmann, November 2023.
- **Research lecture**: *"Palestra de abertura – Democracia e digitalização: cibersegurança, proteção de dados e desinformação como novos desafios"* (Democracy and digitization: cybersecurity, data protection, and disinformation). *Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa* (IDP), Brasília: Indra Spiecker gen. Döhmann, November 2023.
- **"*SECUSO NoPhish Quiz: Erkennen Sie betrügerische E-Mails?*"** (SECUSO NoPhish Quiz: Can you recognize fraudulent e-mails?). Digital Citizen Science project, February 2024.
- **Impulse lecture**: "*Kryptographie. Sicherheit sichtbar machen*" (Cryptography. Making security visible). *Digitalisierung im Dialog* (project digilog@bw): "*Zwischen Risiko und Sicherheit: Den digitalen Wandel gestalten*" (Digitalization in dialogue: Between risk and security: shaping the digital transformation). ZKM – Center for Art and Media Karlsruhe: Jörn Müller-Quade, February 2024.
- **Knowledge transfer initiative "NoPhish"-videos in sign language.** Research group SECUSO, February 2024.
- **Trade show participation**: "ANYMOS – *Anonymisierung für vernetzte Mobilitätssysteme"* (Anonymization for Networked Mobility Systems). Hannover Messe 2024 – Shaping the Future with Technology, March/April 2024.

- **Contribution to exhibition**: “The Ignorant Voting Machine”. *Digitalisierung im Dialog* (project digilog@bw): “Digiloglounge N°3: But Is It safe?” ZKM – Center for Art and Media Karlsruhe: Jörn Müller-Quade, February–July 2024.
- **Research talk**: “Cybergeddon in Healthcare”. Seminar series for the PhDs in Operations Research, University of Zurich: Emilia Grass, April 2024.
- **Art-Science Talk**: “*Wie wählen wir?”* (How do we vote?). ZKM – Center for Art and Media Karlsruhe: Jörn Müller-Quade, May 2024.
- **Panel discussion**: “Navigating the Future of Cyber Security: Combating AI-Powered Attacks for Securing Critical Infrastructure”. 25th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2024), Perth, Australia. Member of the panel: Thorsten Strufe, June 2024.
- **School cass visit**: “How easy is it to crack passwords? What actually makes a password secure? What is ‘phishing’? And how can I tell whether a message is genuine or fake? What does ‘shoulder surfing’ mean? And how can I protect myself against it?” *Realschule am Rennbuckel*, Karlsruhe, visits SECUSO Research Group, June 2024.
- **Impulse lecture**: “*Datenschutz – von der Technik zu rechtssicheren Lösungen*” (Data protection – from technology to legally compliant solutions). *EFFEKTE-Reihe 2024/25* – “*Freiheit im Wandel – Chancen und Grenzen für Wissenschaft und Gesellschaft”* (Freedom in transition – opportunities and limits for science and society), Karlsruhe: Jörn Müller-Quade, June 2024.
- **Presentation of criteria catalog for data protection-compliant school information systems**: Project “DIRECTIONS – Data Protection Certification for Educational Information Systems”: Ali Sunyaev, July 2024.
- **Lecture**: “*Der menschliche Faktor in der Cybersicherheit, Wirkung und Nutzen von Awarenessmaßnahmen*” (The human factor in cybersecurity, impact, and benefits of awareness measures). *Sicherheitsforum Baden-Württemberg “25 Jahre ganzheitliche Sicherheit – Rückblick, gegenwärtige Herausforderungen, Ausblick”* (25 years of holistic security – review, current challenges, outlook), *Allianz für Sicherheit in der Wirtschaft Baden-Württemberg e.V.*: Melanie Volkamer, July 2024.
- **Impulse lecture**: “The Invisible Threat: Building Awareness of Attacks on ML Algorithms”. Dialogue Day – Economy and Technology 2024. KIT Department for Economics and Management, Karlruhe: Raphael Morisco, July 2024.
- **Impulse lecture**: “*Allgemein, unmittelbar, frei, gleich und geheim: Was sind sichere Wahlen?”* (General, direct, free, equal, and secret: what are secure elections?). *Digitalisierung im Dialog* (project digilog@bw). ZKM – Center for Art and Media Karlsruhe: Felix Dörre, Michael Kirsten, August 2024.

KASTEL

Projects

Third-Party Funding (participation, selected projects)

(Sorted by funding organization, alphabetical)

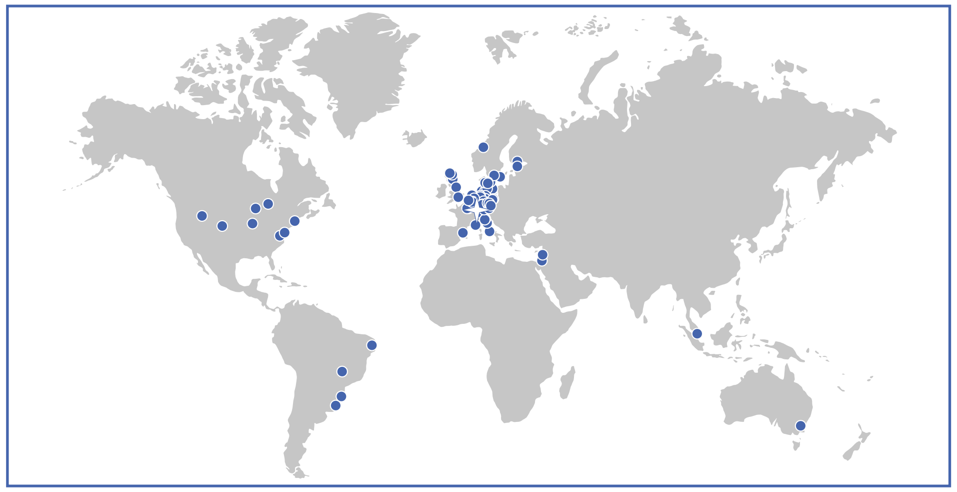
- **“ANYMOS – *Anonymisierung für vernetze Mobilitätssysteme*”** (Anonymization for Networked Mobility Systems). Project funded by the Federal Ministry for Education and Research, BMBF.
- **“DATACARE – *Datensouveränität und informierte Zustimmung als Grundlage für eine patientenorientierte KI-gesteuerte klinische Forschung*”** (Data Sovereignty and Informed Consent as the Basis for Patient-centered and AI-driven Clinical Research). BMBF-funded collaborative project.
- **“DataChainSec – *Sicherheit für KI-Anwendungen in der Lebensmittelversorgung*”** (Safety for AI Applications in Food Supply). BMBF-funded project.
- **“DIRECTIONS – *Datenschutzzertifizierung für Bildungsinformationssysteme”*** (Data Protection Certification for Educational Information Systems). BMBF-funded project.
- **“HardShiP – *Langfristige IT-Sicherheit für die Hardware von Produktionsanlagen*”** (Long-term IT Security for Production Plant Hardware). BMBF-funded project.
- **“INSPECTION – *Externe Erkennung von gehackten Webseiten im Umfeld von betrügerischen Online-Shops”*** (External Detection of Hacked Websites in the Context of Fraudulent Online Stores). BMBF-funded project.
- **“KARL – *Künstliche Intelligenz für Arbeit und Lernen in der Region Karlsruhe*”** (Artificial Intelligence for Work and Learning in the Karlsruhe Region). BMBF-funded competence cluster.
- **“Propolis – Privacy for Smart Cities”**. Project funded by the BMBF and the Agence Nationale de la Recherche.
- **“QuBRA – *Quantenmethoden und Vergleichspunkte zur Ressourcenvergabe*”** (Quantum Methods and Benchmarks for Resource Allocation). BMBF-funded project.
- **“Sec4IoMT – *Sicherheit im Internet der Dinge für medizinische Endgeräte*”** (Security for the Internet of Medical Things). BMBF-funded project.
- **“SynthiClick – *Synthetische Datenerzeugung anhand von Nutzungsverhalten im World Wide Web*”** (Synthetic Data Generation based on User Behavior in the World Wide Web). BMBF-funded project.
- **“VE ASCOT – *Neuartige sichere Elektronikkomponenten für die ‘Chain of Trust’*”** (Advanced Security for the Chain of Trust). BMBF-funded project.
- **“C2CBridge – Country to City Bridge”**. Project funded by the Federal Ministry for Digital and Transport, BMDV.
- **“SPECK – *Systemische Optimierung der Wertschöpfungskette Fleisch am Beispiel der Schweinehaltung durch Entwicklung und Einbettung digitaler Werkzeuge*”** (Systemic optimization of the meat value chain using the example of pig farming through the development and embedding of digital tools). Project funded by the Federal Ministry of Food and Agriculture, BMEL, and the Federal Office for Agriculture and Foods.
- **“CanConnect – *Zusammenführung von Krebsregisterdaten und multimodalen, melderbasierten Diagnostikdaten zur KI-basierten Biomarker-Detektion*”** (Merging Cancer Registry Data and Multimodal, Reporter-based Diagnostic Data for AI-based Biomarker Detection). Project funded by the Federal Ministry of Health, BMG.
- **“AUDITOR – European Cloud Service Data Protection Certification”.** Project funded by the Federal Ministry for Economic Affairs and Climate Action, BMWK.
- **“FLAIROP: Federated Learning for Robot Picking”**. BMWK-funded project.
- **“Intelligent Security Handwerk”**. BMWK-funded project.
- **“ProvidedQ – Quantum Readiness for Optimization Providers”**. BMWK-funded project.
- **“SofDCar – Software-Defined Car”**. BMWK-funded project.

- "CyberSec4Europe". European Framework on Cybersecurity Research. EU-funded project.
- "Building Network Resilience in Healthcare against Cyber-Attacks". Project funded by the Helmholtz Association.
- "COOLedger – A COnfiguration toOL for Distributed Ledgers". Project funded by the Helmholtz Association.
- "HIDSS4Health – Helmholtz Information & Data Science School for Health". Project funded by the Helmholtz Association.
- "ROCK-IT (remote, operando controlled, knowledge-driven, IT-based)". Project funded by the Helmholtz Association.
- "Change aPS – Static Analysis to Support Change Management in Variant-rich Legacy Control Software for Machine and Plant Engineering Companies". Project funded by the German Research Foundation, DFG.
- "Convide – Consistency in the View-Based Development of Cyber-Physical Systems" (SFB 1608). DFG-funded Collaborative Research Centre.
- "GRK 2050: Privacy and Trust for Mobile Users". DFG-funded project.
- "KeY – A Deductive Software Analysis Tool for the Research Community". DFG-funded project.
- "NFDIxCS – National Research Data Infrastructure for and with Computer Science". Consortium funded by the DFG, in cooperation with the German National Research Data Infrastructure (NFDI).
- "Resilient Network Embeddings for Friend-to-Friend Networks". DFG-funded project.
- "*Automatisch benachteiligt – Das Allgemeine Gleichbehandlungsgesetz und der Schutz vor Diskriminierung durch algorithmische Entscheidungssysteme*" (Automatically disadvantaged – The General Act on Equal Treatment and protection against discrimination by algorithmic decision-making systems). Legal opinion on protection against discrimination through algorithmic decision-making systems provided for Federal Anti-Discrimination Agency, August 2023.
- "DiTraRe – Digital Transformation of Research". Leibniz ScienceCampus, funded by the Leibniz Association.
- "EVIDENTT – *Einsatz verteilter Technologien zur beweissicheren Dokumentation von Verbraucherschutzverstößen auf Online-Plattformen*" (Use of distributed technologies for the evidentiary documentation of consumer protection violations on online platforms). Project funded by the *Baden-Württemberg Stiftung*.
- "JuBot – Stay Young with Robots". Project funded by the *Carl-Zeiss-Stiftung*.

Cooperation

Selected Cooperation Projects with Research Institutions & Organizations

- "Assessing the Impact of Technology Partners on the Level of Cyberattack Damage in Hospitals". Cooperation with Detecon International GmbH, University of Greifswald, and APOLLON University for Health Care Management.
- "ConTrust: Trust in Conflict – Political Life under Conditions of Uncertainty". Research initiative with Peace Research Institute Frankfurt.
- "Cyber Threat Intelligence". Cooperation with Ben-Gurion University of the Negev.
- "*Effektive Security Awareness am KIT*". Project with Technical University of Darmstadt.
- "End-to-End Verifiable and Secret Online Elections at KIT". Project with Scientific Computing Center (SCC) at KIT, Karlsruhe.
- "Everlasting Security for Quantum Cryptographic Protocols for Encrypted Computing". Cooperation project with CISPA Helmholtz Center for Information Security.
- "MANTRA – *Graphen-basierte Informationsaggregation zur Verbesserung des Cybersicherheitsmanagements in kritischen Infrastrukturen*" (Graph-based information aggregation to improve cybersecurity management in critical infrastructures). Joint project with Asvin GmbH, *Ostbayerische Technische Hochschule*, Massachusetts Institute of Technology, Fraunhofer AISEC, and Fraunhofer IAO, for *Agentur für Innovation in der Cybersicherheit GmbH*.
- "MEDI:CUS". Platform headed by the Ministry of the Interior, Digitalisation and Local Government Baden-Württemberg.
- Principles of Machine Learning in Computer Security". Cooperation with University College London, King's College London, Ruhr-Universität Bochum, and Technical University of Berlin.
- "Test Area Autonomous Driving Baden-Württemberg". Consortium funded by the Ministry of Transport and Ministry of Science, Research and Arts Baden-Württemberg.
- "Use of AI in Risk and Resilience Research". Cooperation with MINES ParisTech.
- "Web Measurements". Joint project with CISPA Helmholtz Center for Information Security, *Westfälische Hochschule*, University of Applied Sciences, and secunet Security Networks AG.



75 National (German) institutions

30 European

16 International

Cooperation Partners: Research Institutions & Organizations

- Aalto University, Finland.
- Abertay University, Dundee, UK.
- APOLLON University for Health Care Management, University of Applied Sciences, Bremen.
- ATHENE National Research Center for Applied Cybersecurity, Darmstadt.
- Baden-Württemberg Institut für Nachhaltige Mobilität, Karlsruhe.
- Ben-Gurion University of the Negev, Beer-Sheva, Israel.
- Berufsförderungswerk des Handwerks gGmbH, Korbach.
- Bremen Cancer Registry.
- Bundesnetzagentur, Bonn.
- Centre for Tactile Internet with Human-in-the-Loop, CeTi – Cluster of Excellence, Dresden.
- Centre Responsible Digitality (ZEVEDI), Darmstadt.
- Centrum Wiskunde & Informatica (CWI), Amsterdam, the Netherlands.
- CISPA Helmholtz Center for Information Security, Saarbrücken.
- DePaul University, Chicago, Illinois, USA.
- Deutsches Elektronen-Synchrotron DESY, Hamburg.
- Digital Society Institute, Berlin.
- Dresden University of Technology.
- EIFER – European Institute for Energy Research, Karlsruhe.
- Eindhoven University of Technology, the Netherlands.
- EURECOM – Graduate School and Research Centre in Digital Science, Biot Sophia Antipolis, France.
- FIZ Karlsruhe – Leibniz Institute for Information Infrastructure GmbH.
- FKFS Forschungsinstitut für Kraftfahrwesen und Fahrzeugmotoren Stuttgart.
- Forschungszentrum Jülich GmbH.
- Fraunhofer Center for International Management and Knowledge Economy IMW, Leipzig.
- Fraunhofer Institute for Applied and Integrated Security AISEC, Garching.
- Fraunhofer Institute for Chemical Technology ICT, Munich.
- Fraunhofer Institute for Computer Graphics Research IGD, Darmstadt.
- Fraunhofer Institute for Digital Medicine MEVIS, Bremen.
- Fraunhofer Institute for Industrial Engineering IAO, Stuttgart.
- Fraunhofer Institute for Secure Information Technology SIT, Darmstadt.
- Fraunhofer Institute for Systems and Innovation Research ISI, Karlsruhe.
- Fraunhofer-Gesellschaft zur Förderung der angewandten Forschung e.V., Munich.
- Freie Universität Berlin.
- Friedrich-Alexander-Universität Erlangen-Nürnberg.
- The George Washington University, Washington, DC, USA.
- German Cancer Research Center, Heidelberg.
- German Center for Future Mobility (DZM), Munich.
- Gesellschaft für Informatik e.V., Bonn.
- Goethe University Frankfurt/Main.
- Hahn-Schickard-Gesellschaft für angewandte Forschung e.V., Villingen-Schwenningen.
- Heidelberg University.
- Heilbronn University of Applied Sciences.
- Helmholtz Information & Data Science Academy, Berlin.
- Helmholtz-Zentrum Berlin für Materialien und Energie GmbH.
- Helmholtz-Zentrum Dresden-Rossendorf e.V.
- Hochschule Darmstadt, University of Applied Sciences.
- Hochschule Osnabrück, University of Applied Sciences.
- Idaho National Lab, Idaho Falls, USA.
- Imperial College London, Centre of Excellence for Active Security and Resilience, UK.
- INRIA – National Institute for Research in Digital Science and Technology, Le Chesnay, France.
- Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, Brazil.
- IT University of Copenhagen, Denmark.
- Johannes Gutenberg-Universität Mainz.
- Karlsruhe University of Applied Sciences.
- King's College London, UK.
- KU Leuven, Belgium.
- Leibniz Institute for Prevention Research and Epidemiology – BIPS GmbH, Bremen.
- Leibniz University Hannover.
- Leuphana University Lüneburg.
- Linnaeus University, Kalmar and Växjö, Sweden.
- Ludwig-Maximilians-Universität München, Munich.
- Massachusetts Institute of Technology, Cambridge, USA.
- Max Planck Institute for Software Systems, Saarbrücken.
- Mines ParisTech, France.
- Norwegian University of Science and Technology, Trondheim, Norway.
- OFFIS e.V., Oldenburg.
- Ostbayerische Technische Hochschule, Regensburg.
- OWL University of Applied Sciences and Arts, Lemgo.
- Peace Research Institute Frankfurt (PRIF), Frankfurt/Main.
- Pforzheim University.
- Politecnico di Milano, Italy.
- Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, Brazil.
- Robert Koch Institute, Berlin.
- Royal Holloway University of London, UK.
- Ruhr-Universität Bochum.
- RWTH Aachen University.
- Schloss Dagstuhl. Leibniz-Zentrum für Informatik GmbH, Wadern.
- Singapore University of Technology and Design, Singapore.
- Tallinn University of Technology, Estonia.
- Technical University of Berlin.
- Technical University of Braunschweig.
- Technical University of Darmstadt.
- Technical University of Denmark, Kongens Lyngby, Denmark.
- Technical University of Munich.
- Technische Universität Bergakademie Freiberg.
- Tel-Aviv University, Israel.
- Tor Vergata University of Rome, Italy.
- Trust in Digital Life, Waregem, Belgium.
- Uniklinik RWTH Aachen.
- Universidade de São Paulo, Brazil.
- Universidade Federal de Campina Grande, Brazil.
- Università di Bologna, Italy.
- Universität Bielefeld.
- Universität Duisburg-Essen.
- Universität Hamburg.
- Universität zu Lübeck.
- Universitat Politècnica de Catalunya – BarcelonaTech, Spain.
- University College London, UK.
- University of Bamberg.
- University of Bayreuth.
- University of Bergamo, Italy.
- University of Canberra, Australia.
- University of Cologne.
- University of Denver, Colorado, USA.
- University of Edinburgh, UK.
- University of Greifswald.
- University of Illinois at Urbana-Champaign, USA.
- University of Kassel.
- University of Luxembourg.
- University of Mannheim.
- University of Maryland, USA.
- University of Michigan, USA.
- University of Paderborn.
- University of Potsdam.
- University of Southern Denmark, Odense, Denmark.
- University of Stirling, UK.

- University of Strathclyde, UK.
- University of Stuttgart.
- University of Waterloo, Canada.
- University of York, UK.
- University of Zurich, Switzerland.
- Vrije Universiteit Brussel, Belgium.
- Zentrum für Sonnenenergie- und Wasserstoff-Forschung Baden-Württemberg (ZSW), Stuttgart.

Selected Cooperation Projects with Business & Industry

- **"Auditable Security"**. Project with Huawei Research Germany.
- **"Automotive Security"**. Cooperation with ETAS GmbH.
- **"ChemCrypt" – Suitability of a specific approach for a physical Proof of Work**. Consulting, BASF AG.
- **"Design Methodologies for Cloud-native Systems in the Context of Industrial Automation"**. Project with ABB Asea Brown Boveri Ltd.
- **"Development of Platform for Smart Grid Cybersecurity R&D"**. Collaborative research project with Illinois at Singapore Pte Ltd, Advanced Digital Sciences Center (ADSC).
- **"EMPC – Efficient Secure Multi-Party Computations"**. Project with Huawei Research Germany.
- **"EVerest"**. Cooperation with PIONIX GmbH.
- **"Group Verifiable Random Functions"**. Project with IBM Research Europe.
- **"IIP 2.0" – Transparency software for e-counters**. Contracted by S.A.F.E. e.V.
- **"Repliable Onion Routing"**. Project with NEC Laboraties Europe.
- **"SECML – Secure and Robust Machine Learning for IoT Systems"**. Project with SAP SE.
- **"Security & Compliance Automation"**. Project with SAP SE.
- **"SFML – Secure Federated Machine Learning"**. Project with SAP SE.
- **"VINCRYPTOR – Pseudonomization of Vehicle Identification Numbers"**. Contract by Mercedes Benz AG.
- **"Vulnerability Discovery in Web Applications"**. Project with SAP SE.

Cooperation Partners: Business & Industry

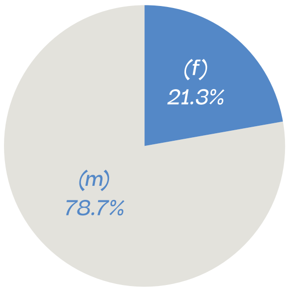
- 4flow AG, Berlin.
- ABB Asea Brown Boveri Ltd, Zurich, Switzerland.
- ADAC Nordbaden e.V., Karlsruhe.
- adesso SE, Dortmund.
- AI4BD Deutschland GmbH – Location Dresden.
- ArtiMinds Robotics GmbH, Karlsruhe.
- Ascora GmbH, Ganderkesee.
- van Asten Tierzucht Neumark GmbH & Co. KG, Neumark.
- Asvin GmbH, Stuttgart.
- AVL Deutschland GmbH, Karlsruhe.
- BASF AG, Ludwigshafen.
- BDO AG Wirtschaftsprüfungsgesellschaft, Hamburg.
- Blanc & Fischer Familienholding GmbH, Oberderdingen.
- BooleWorks GmbH, Munich.
- Bosch GmbH, Stuttgart.
- Bosch Rexroth AG, Horb am Neckar.
- CarByte GmbH, Stuttgart.
- C.R.S. iiMotion GmbH, Villingen-Schwenningen.
- C & S Computer und Software GmbH, Augsburg.
- cantamen GmbH, Hannover.
- CAS Software AG, Karlsruhe.
- Cloud&Heat Technologies GmbH, Dresden.
- corvolution GmbH, Ettlingen.
- Datalyxt GmbH, Karlsruhe.
- datenschutz cert GmbH, Bremen.
- DeepCare GmbH, Ludwigsburg.
- Detecon International GmbH, Cologne.
- DPS Engineering GmbH, Leinfelden.
- DResearch Fahrzeugelektronik GmbH, Berlin.
- ecsec GmbH, Michelau.
- EDI GmbH, Karlsruhe.
- Électricité de France, Paris, France.
- elevait GmbH & Co. KG, Location Dresden.
- e-mobil BW GmbH, State Agency for New Mobility Solutions and Automotive Baden-Württemberg, Stuttgart.
- EnBW Energie Baden-Württemberg AG, Karlsruhe.
- e-Netz Südhessen AG, Darmstadt.
- ETAS GmbH, Stuttgart.
- EuroCloud Deutschland_eco e.V., Cologne.
- Exxeta AG, Karlsruhe.
- GAMS Software AG, Frechen.
- Gesellschaft für wissenschaftliche Datenverarbeitung mbH, Göttingen.
- GoDaddy, Inc., Scottsdale, Arizona, USA.
- Huawei Research Germany, Darmstadt.
- IBM Research Europe – Zurich, Rüschlikon, Switzerland.
- Illinois at Singapore Pte Ltd, Advanced Digital Sciences Center, Singapore.
- Infineon Technologies AG, Neubiberg.
- INFOnline GmbH, Bonn.
- init innovation in traffic systems SE, Karlsruhe.
- INIT Mobility Software Solutions GmbH, Karlsruhe.
- inTec automation GmbH, Baunatal.
- Karlsruher Verkehrsverbund GmbH.
- Kinemic GmbH, Karlsruhe.
- LAVRIO.solutions GmbH, Karlsruhe.
- Mercedes-Benz AG, Stuttgart.
- microTEC Südwest e.V., Freiburg.
- mindUp Web + Intelligence GmbH, Konstanz.
- NEC Laboratories Europe, Heidelberg.
- Omicron electronics GmbH, Klaus, Austria.
- Optimum datamanagement solutions GmbH, Karlsruhe.
- Orolia Switzerland SA, Neuchâtel, Switzerland.
- P3 digital services GmbH, Hamburg.
- PIONIX GmbH, Bad Schönborn.
- QGroup GmbH, Wehrheim.
- Raummobil GmbH, Karlsruhe.
- Robert Bosch GmbH, Gerlingen.
- SaarLB Landesbank Saar, Saarbrücken.
- S.A.F.E. e.V., Berlin.
- SAP SE, Walldorf.
- SAP Research, Walldorf.
- Schäffler AG, Herzogenaurach.
- Schölly Fiberoptic GmbH, Denzlingen.
- Secorvo Security Consulting GmbH, Karlsruhe.
- secunet Security Networks AG, Essen.
- SICK AG, Waldkirch.
- Siemens AG, Munich.
- Siemens AG, Niederlassung Karlsruhe.
- Siemens Energy Global GmbH & Co KG, Munich.
- Softwarezentrum Böblingen/Sindelfingen e.V., Böblingen.
- Stadtwerke Ettlingen GmbH.
- STA-Serviceteam Alsfeld GmbH, Alsfeld.
- teamtechnik Maschinen und Anlagen GmbH, Freiburg.
- T-Systems International GmbH, Frankfurt/Main.
- Urban Software Institute GmbH, Chemnitz.
- Vector Informatik GmbH, Stuttgart.
- Volkswagen AG, Wolfsburg.
- WIBU Systems AG, Karlsruhe.
- YellowMap AG, Karlsruhe.
- ZF Friedrichshafen AG.

KASTEL

Diversity

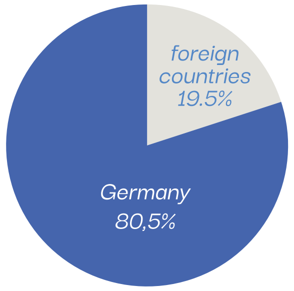
Gender Statistics

	Number of Individuals	(m)	(f)	Ratio of Female Individuals
Total number	174	137	37	21.3%
Fellows	25	19	8	32.0%
Researchers	149	118	29	19.5%



Statistics on International Participation

	Number of Individuals	Number of Foreign Individuals	Ratio of Foreign Individuals
Total number	174	34	19.5%
Fellows	25	3	12.0%
Researchers	149	31	20.8%



Represented Nations
Number of Individuals

6 China	6 India	5 Spain
4 Iran	2 France	2 Italy
1 Austria	1 Brazil	1 Denmark
1 Pakistan	1 Romania	1 Sudan
1 Tunesia	1 Turkey	1 Uruguay

KASTEL Security Research Labs

Contact:
KASTEL – Institute of Information Security and Dependability
Am Fasanengarten 5, 76131 Karlsruhe, Germany
www.kastel-labs.de

KASTEL

Part II: Facts &
Numbers