KASTEL Security Research Labs

Insight

2023|2024

KASTEL

Part I: Research & Researchers

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. 5; Patricia Arias Cabarcos: p. 39;
CRC 1608 Convide, KIT: pp. 42, 63; Federal Ministry of Education and Research: p. 9;
Fraunhofer IOSB: pp. 58, 61, 62; Emilia Grass: p. 36;
National Research Center for Applied Cybersecurity ATHENE: p. 10;
Karlsruhe Institute of Technology (KIT): pp. 7, 35, 39-41, 43-45, 47, 49, 53-57, 59, 64-67;
Peter Mayer: p. 42; Raffaela Mirandola: p. 37; André Platzer: p. 43; Ralf Reussner: p. 44;
Andy Rupp: p. 45; Gunther Schiefer: p. 46; Indra Spiecker gen. Döhmann: p. 46;
Ali Sunyaev: p. 47; Melanie Volkamer: p. 48; Marcus Wiens: p. 48;
Christian Wressnegger: p. 49; J. Marius Zöllner: p. 50; Frederike Zufall: p. 38;

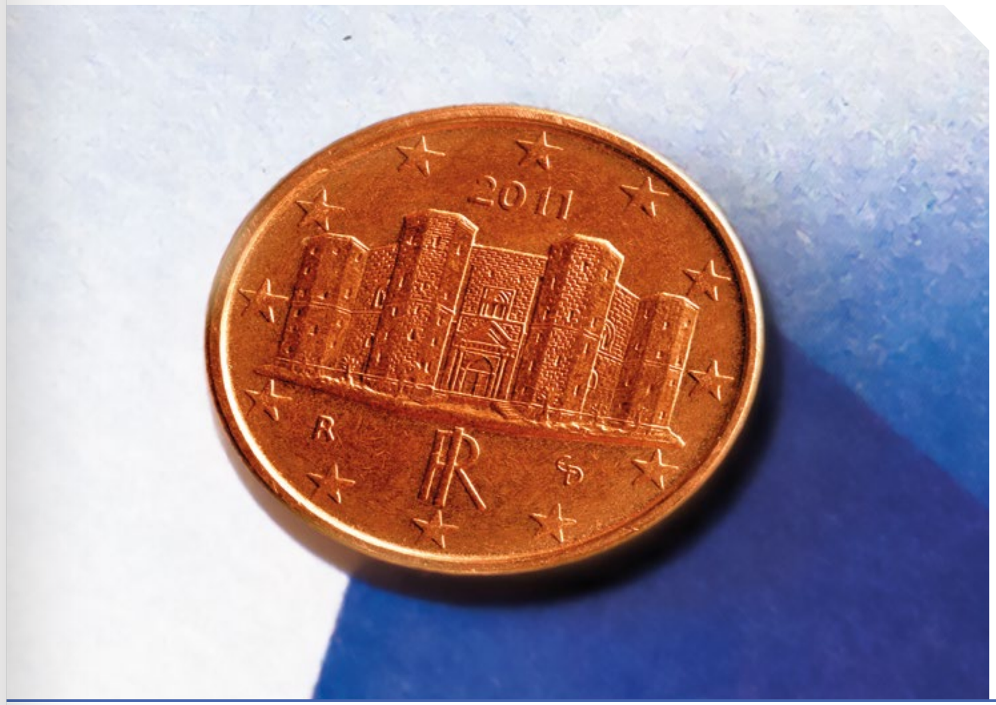
September
2024

CONTENTS

Part I: Research & Researchers

Part II: Facts & Numbers

Castel del Monte



In 1996, the EU Council of Economics and Finance Ministers decided that euro coins should have a common European side and a national side freely chosen by the member states. The common European side of the 1-, 2-, and 5-cent coins schematically shows the position of Europe on a globe. In Italy, the designs of the national sides were assessed by a committee of technicians and artists before being presented to the public. For each coin denomination, a different design was chosen from the various works of art by Italy’s most famous artists.[1]

The Italian 1-cent coin shows Castel del Monte in Apulia, which was built in the 13th century by the Hohenstaufen emperor Frederick II (coin design: Eugenio Driutti)[2]. The Castel del Monte still stands today on a hill near the city of Andria in the southern Italian province of Barletta-Andria-Trani.

The logo of **KASTEL Security Research Labs** shows a stylized Castel del Monte, whose sophisticated architecture can serve as a metaphor for a secure design. This means that even attackers who are already inside the castle cannot reach their target directly, even after overcoming massive protective walls – a concept that, figuratively speaking, is also of great importance in today’s cybersecurity.

[1] Cf. Bank of Italy. <www.bancaditalia.it/compiti/emissione-eu-ro/monete/index.html?com.dotmarketing.htmlpage.language=1> (last access: June 4, 2024).

[2] Cf. Deutsche Bundesbank. <www.bundesbank.de/en/tasks/cash-management/euro-coins/regular-coins/italy-623666> (last access: June 4, 2024).

Editorial & Opening Messages

Cybersecurity in a World of Multiple Crises

In the last decade our society has been struck by several momentous crises: climate change, a global pandemic, and war on the European continent, as well as other armed conflicts, triggered societal and economic shocks. In this context, digitalization has proven to be a necessary means of effectively countering the consequences of such crises.

To combat climate change, current energy and mobility transformations are focused on a transition to renewable energies and a consistent increase in the efficiency of energy use. For this, digitalization plays a central role in managing and securing the energy supply and new forms of sustainable mobility, e.g., ride sharing enabled by autonomous driving. However, the progressive networking of systems also significantly expands their attack surface. Notable examples include the penetration tests of the Stadtwerke Ettlingen (municipal utilities) in 2014, the 2015 Jeep Hack, or the ongoing hacks into Ukrainian power plants. These and other examples show that cybersecurity must be a top priority in order to guard our infrastructures effectively.

The pandemic also clearly showed how vulnerable our community is. The globalized economy has proven to be highly susceptible to the potential occurrence of shortages in the supply of vital products or components, especially IT components or medical products. As a direct result of the pandemic, the use of online conferencing significantly expanded. The Taurus wiretapping scandal, among others, has shown that even extremely security-conscious professionals can make mistakes that can be exploited by adversarial agents. The pandemic has also led to the wider use of online elections. Therefore, it is necessary to establish systems with provable security guarantees to ensure correctness of results and the confidentiality of votes.

Ongoing political and open military conflicts have made it clear how government organizations work to disrupt our critical infrastructures, as well as the way our digitally connected societies function today. The effects and tendencies of targeted influence on public opinion and the course of democratic elections and processes are already being observed, e.g., due to adversarial troll factories or networks of social bots. The currently massive increase in AI applications can also play an important role here, e.g., through the ability to create convincing (fake) videos or images that can be used for disinformation.

The research field of cybersecurity has thus become even more essential to the functioning of our society: We must be able to protect not only our energy and mobility systems, and production facilities from attacks but also our society from unwanted influence.

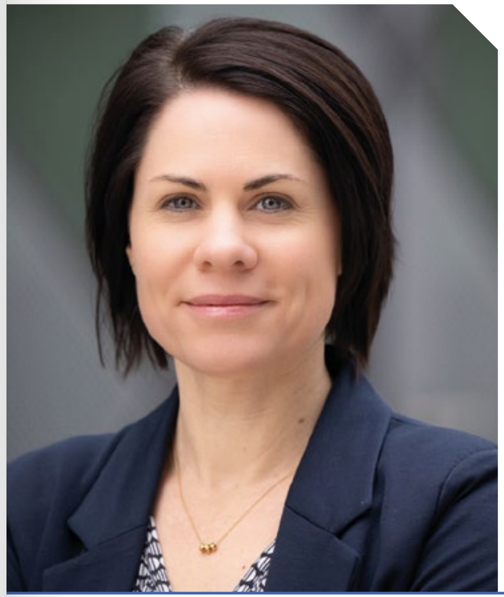
The mission of KASTEL Security Research Labs is to conduct basic and applied research contributing to these new challenges and to bridge the gap between academic research and the needs of society and industry – with the development of protection concepts that can be implemented in sensitive energy, mobility, and production systems. This is made possible through the close collaboration of FZI Research Center for Information Technology, Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB, and Karlsruhe Institute of Technology (KIT) using the existing infrastructures at the research location Karlsruhe.

Based on our experience, it is important to assess measures and evaluate their level of security for systems and processes, in order to be able to make the right choice when implementing protection systems. Therefore, we stringently advance the quantification of (cyber-)security from method development to implementation in the application domains.

I invite you to follow our current activities with the KASTEL Security Research Labs' annual report "Insight 2023/2024" and get an impression of our interdisciplinary research.

Prof. Dr. Jörn Müller-Quade

Spokesperson of
KASTEL Security Research Labs



DR. TINA KLÜWER

- **Federal Ministry of Education and Research**
- **Head of Directorate-General "Research for Technological Security and Innovation"**

Federal Ministry of Education and Research (BMBF)

Almost every aspect of our lives is affected by information and communication systems. Anything of such key importance to society, economy, and the state must be protected well. This protection must not be left to third parties – we ourselves must be in a position to understand, create, and develop security for our IT systems.

It is with this aim in mind that the Federal Ministry of Education and Research (BMBF) is funding the KASTEL Security Research Labs. Launched in 2011 as one of three competence centres, KASTEL has now firmly established in the German research landscape as a cyber security stronghold.

With conscientious research, internationally renowned publications, up-to-date analyses, and a start-up incubator from the BMBF initiative StartUpSecure, KASTEL Security Research Labs are constantly and successfully driving forward the transfer of outstanding research into application.

I wish you continued success in this endeavour.

Dr. Tina Klüwer

PROF. DR. MICHAEL WAIDNER

- Director of the National Research Center for Applied Cybersecurity ATHENE
- Professor at the Technical University of Darmstadt
- Director of the Fraunhofer Institute for Secure Information Technology SIT

National Research Center for Applied Cybersecurity ATHENE, Darmstadt

Ladies and Gentlemen,

As director of the National Research Center for Applied Cybersecurity ATHENE in Darmstadt, it is a particular pleasure for me to express my appreciation and commendation to the Competence Center for Applied Security Technology KASTEL in Karlsruhe – KASTEL Security Research Labs (SRL) – for its many years of very successful research and development work.

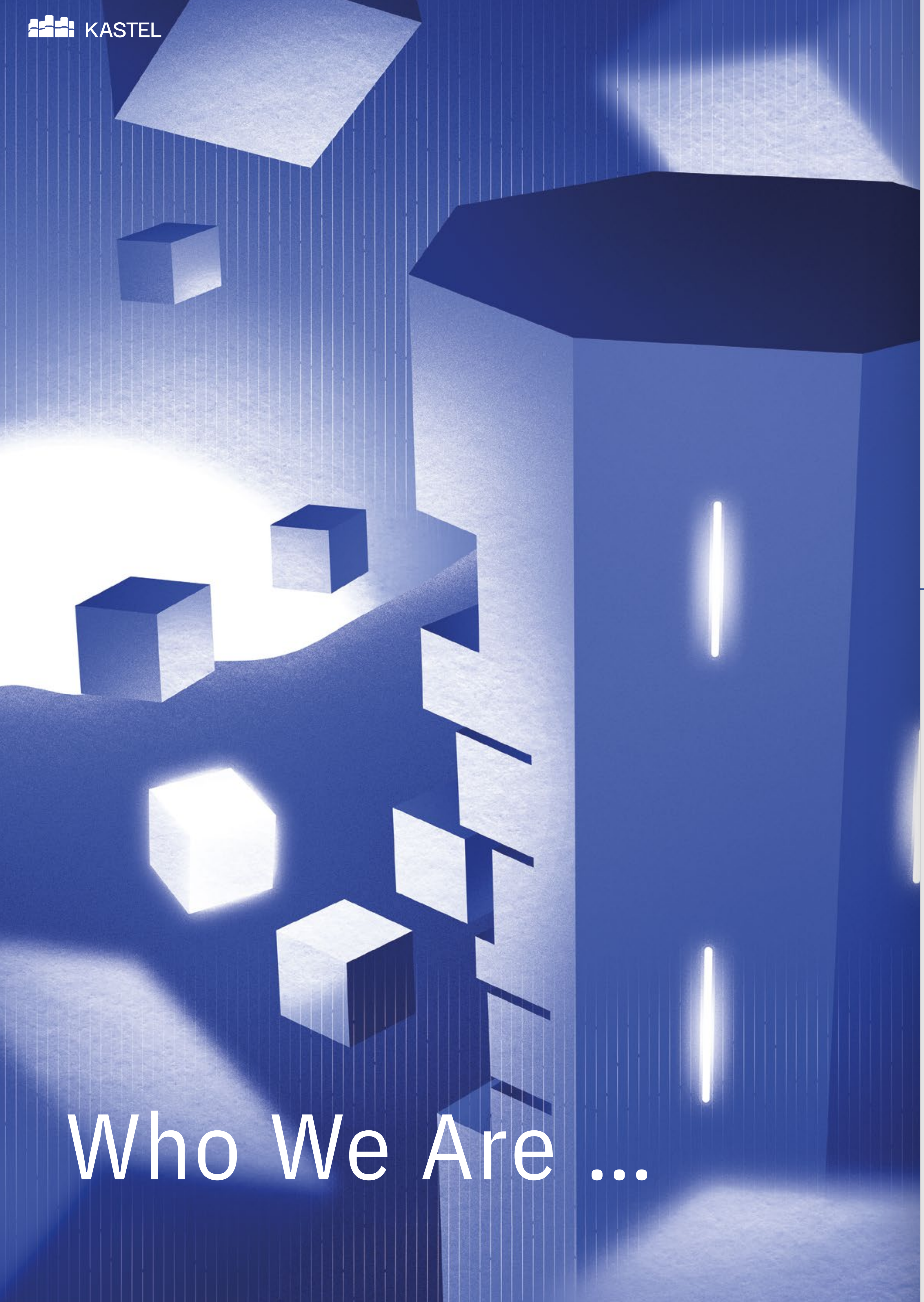
Our two centers are linked by many years of fruitful collaboration. We started together in 2011 as national competence centers funded by the Federal Ministry of Education and Research and have been in close scientific exchange ever since. This exchange has proven to be extremely valuable in order to effectively address the challenges in the dynamic field of cybersecurity. I am delighted that what started out small in 2011 has now developed into a key component of Germany's cybersecurity architecture.

At a time when digital security is of utmost importance, it's up to all of us to bundle our national expertise to develop specific solutions with great benefits for our communities. The research in KASTEL SRL, like that in ATHENE, is aimed at effectively countering current and future threats in cyberspace and developing innovative security concepts.

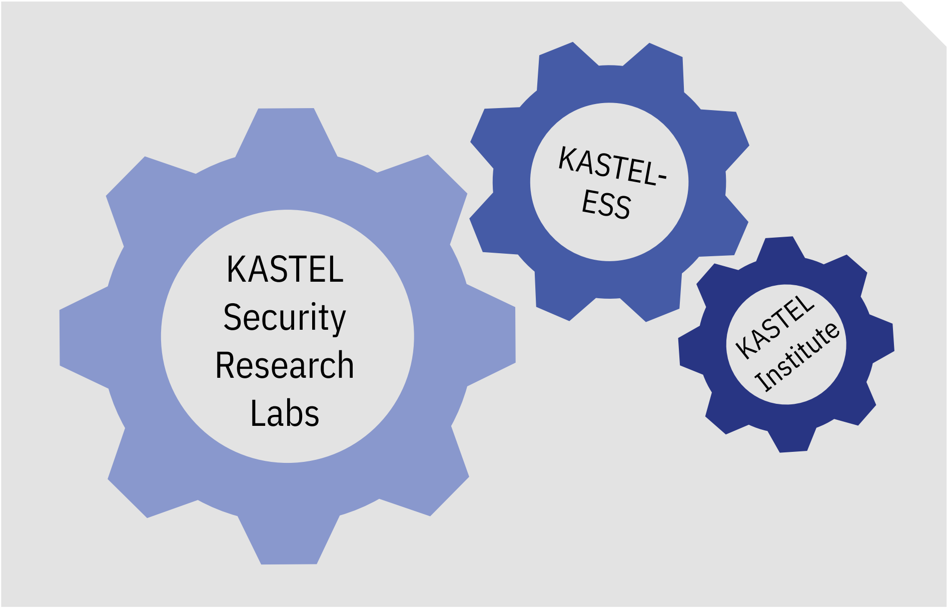
One particularly exciting area of our collaboration is the promotion of start-ups. Together, we support young companies in transforming promising research results into marketable products and services. In this way, we contribute not only to security, but also to our country's innovative capacity.

I am convinced that the close partnership between KASTEL SRL and ATHENE will continue to make an important contribution to cybersecurity in Germany in the future. Let's continue working together on solutions that make our digital world more secure. Society needs us and our contributions.

Prof. Dr. Michael Waidner



Who We Are …



KASTEL – a Brand with a Wide Scope

In 2021, **KASTEL Security Research Labs** took over the baton from the **"Competence Center for Applied Security Technology KASTEL"**, one of three National Competence Centers founded and funded by the Federal Ministry of Education and Research (BMBF) in 2011. As a consequence, the research priorities have been adapted with the aim of strengthening our interdisciplinary network of scientists who together address the challenges of cybersecurity research and work on them in joint projects in an application-oriented manner.

"KASTEL" – The Network

KASTEL Security Research Labs has the unique opportunity to benefit from the extensive and wide-ranging expertise at the Karlsruhe research location due to the institutional partnership of the Karlsruhe Institute of Technology (KIT), the FZI Research Center for Information Technology and the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB. Across the institutions, the team works on fundamental and applied research issues in cybersecurity, covering the further development of fundamental methods as well as the security of concrete applications.

"KASTEL" – The Helmholtz Topic

KASTEL-ESS: In 2021, KASTEL became – through the **Topic "Engineering Secure Systems"** (ESS) – an integral part of the research program "Engineering Digital Futures" funded by the Helmholtz Association. In this configuration, cybersecurity research can be pursued in the long term in order to provide continuous as well as anticipatory support to society in light of the urgent need for action.

"KASTEL" – The KIT Institute

KASTEL Institute at KIT: At the same time as the Topic ESS was initiated, the **"KASTEL – Institute for Information Security and Dependability"** was founded as an organization unit at KIT. The KASTEL Institute now serves as a joint home for university and large-scale research tasks in the field of cybersecurity.

KASTEL Security Research Labs

6 Research Foci

The research foci characterize the range of KASTEL Security Research Labs' research topics in the field of cybersecurity. These are worked on by the individual research groups under the leadership of the KASTEL SRL Fellows. Common cross-cutting themes connect elements that mark concrete milestones towards our overarching goal: Increasing security in the digital world.

Research Focus "Network Security & Distributed Systems"

The internet is the prime example for a communication network, connecting billions of nodes and enabling services like Peer-to-Peer (P2P) networks, blockchains, and social media. Security research in this area spans a wide spectrum from network resilience and intrusion detection over access control and identity management to smart contracts and privacy-aware protocols.

Research Focus "Formal & Data Security"

Algorithms and protocols are the building blocks of information systems. We need to have strong confidence in their security, which is impossible without a thorough analysis. Formal verification and cryptographic proofs support the development of practical and efficient systems with real-world applications that offer comprehensive security and privacy guarantees.

Research Focus "Applied Security"

Applied security is crucial because security advances can only have real-world impact if they involve consideration of real-world systems. This includes finding vulnerabilities in software and embedded devices, assessing the privacy impact of apps, and analyzing real systems for conceptual flaws, as well as improving machine learning methods and applying them to computer security.

Research Focus "Software Security"

Engineering dependable and secure software is a huge challenge. It requires bringing together model-based software engineering and agile methods to deal with changing requirements. Tools can be used to assist in software architecture-based analysis of issues concerning confidentiality, vulnerability, and maintainability. A structured approach helps to leverage software diversity and handle legacy software.

Research Focus "Human & Societal Factors in Security"

IT systems exist within a societal, legal, and economic context, but they also influence that context. A complete analysis of any IT system needs to consider all of these aspects. When users interact with the system, they should be aware of security and privacy implications. In addition, economic risk needs to be modeled and General Data Protection Regulation (GDPR) aspects considered.

Research Focus "Application Domains"

Our future society will depend on networked critical infrastructures such as smart grids, autonomous mobility, and intelligent production facilities. All of these have features that go beyond classical computer systems. Therefore, real-time requirements, fluid system boundaries, and possible physical consequences of IT system failures require additional expertise from engineers.

Highlights 2023|2024

Selection of 2023 …

French-German Ph.D. Workshop on the Potential of AI in IT Security and Resilience Research

In this workshop, doctoral students from the universities MINES Paris Tech, TU Bergakademie Freiberg, and Karlsruhe Institute of Technology developed approaches for using AI to secure critical infrastructures and critical processes, particularly in the area of IT security. Approaches related to forensics, cyber threat intelligence, and intelligent early warning systems played a special role. The workshop took place on March 20–22, 2023 at the Technical University Bergakademie Freiberg and was sponsored by the Franco-German University.

Further Development of a Legal Framework for IT Security in Intelligent Transport Systems

Based on the work from the previous year, the legal framework for IT security in Intelligent Transport Systems (ITS) was further developed. The central goal was to ensure end-to-end IT security in distributed systems with multiple participants through an appropriate regulatory methodology. This goal was achieved and published in a legal journal using the example of the virtual blue light.

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

Increasing the Robustness of Perceptive Deep Neural Networks

(Abstract) Deep neural networks are used in the field of autonomous vehicles primarily for perception-based tasks. Our research analyzes to what extent the robustness of these models can be increased, especially against realistic, targeted attacks. The current focus is on the robustness of networks for recognizing traffic signs and traffic lights. In addition, new Mixture-of-Experts CNN architectures have been developed, which enable improved interpretability compared to conventional architectures. The individual expert subnets focus on different domains. For this purpose, new training methods were designed and evaluated that enable a trade-off between precision and interpretability. Ultimately, these findings will be used to develop advanced detectors.

S. Pavlitska, C. Hubschneider, L. Struppek & J.M. Zöllner (2022): **Sparsely-gated Mixture-of-Expert Layers for CNN Interpretability.** – 2023 International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia: 1-10.

S. Pavlitska, N. Lambing & J.M. Zöllner (2023): **Adversarial Attacks on Traffic Sign Recognition: A Survey.** – 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Tenerife, Spain: 6 pp.

Evaluating Model Differencing for the Consistency Preservation of State-based Views

BEST PAPER AWARD

(Abstract) While developers and users of modern software systems usually only need to interact with a specific part of the system at a time, they are hindered by the ever-increasing complexity of the entire system. Views are projections of underlying models and can be employed to abstract from that complexity. When a view is modified, the changes must be propagated back into the underlying model without overriding simultaneous modifications. Hence, the view needs to provide a fine-grained sequence of changes to update the model minimally invasively. Such fine-grained changes are often unavailable for views that integrate with existing workflows and tools. To this end, model differencing approaches can be leveraged to compare two states of a view and derive an estimated change sequence. However, these model differencing approaches are not intended to operate with views, as their correctness is judged solely by comparing the input models. For views, the changes are derived from the view states, but the correctness depends on the underlying model. This work introduces a refined notion of correctness for change sequences in the context of model-view consistency. Furthermore, we evaluate state-of-the-art model differencing regarding model-view consistency. Our results show that model differencing largely performs very well. However, incorrect change sequences were derived for two common refactoring operation types, leading to an incorrect model state. These types can be easily reproduced and are likely to occur in practice. By considering our change sequence properties in the view type design, incorrect change sequences can be detected and semi-automatically repaired to prevent such incorrect model states.

J.W. Wittler, T. Sağlam & T. Kühn (2023): **Evaluating Model Differencing for the Consistency Preservation of State-based Views.** – The Journal of Object Technology, 22 (2): 2:1–2:14.

German Voters' Attitudes Towards Voting Online with a Verifiable System

(Abstract) A representative study concluded that more than 63% of German voters would have liked to cast their vote for the federal election in 2021 online. In this paper, we aimed to investigate why Germans might be in favour or against online voting, conducting an online survey. We furthermore aimed to study the reactions of people being in favor of online voting if confronted with a verifiable remote voting system, as well as with interventions aimed at communicating that it is important to follow all the steps to verify. Our findings show that the majority of our participants were generally willing to vote online. Convenience emerged as the most popular reason for voting online. The reaction to the verifiable remote voting system was diverse, from our participants being irritated from the complexity, to very positive reactions due to high security level. Nonetheless, the majority of the participants did not change their willingness to vote online after seeing the proposed system. The different interventions had no effect. Furthermore, the majority agreed on the importance of verifiability being in place.

O. Kulyk, M. Volkamer, N. Fuhrberg, B. Berens & R. Krimmer (2023): **German Voters' Attitudes Towards Voting Online with a Verifiable System.** – In: S. Matsuo, L. Gudgeon, A. Klages-Mundt, D. Perez Hernandez, S. Werner, T. Haines, A. Essex, A. Bracciali & M. Sala (eds.): Financial Cryptography and Data Security. FC 2022 International Workshops. Lecture Notes in Computer Science, vol. 13412: 335–350.

Fiat-Shamir Transformation of Multi-Round Interactive Proofs

(Abstract) The celebrated Fiat-Shamir transformation turns any public-coin interactive proof into a non-interactive one, which inherits the main security properties (in the random oracle model) of the interactive version. While originally considered in the context of 3-move public-coin interactive proofs, i.e., so-called Σ-protocols, it is now applied to multi-round protocols as well. Unfortunately, the security loss for a $(2\mu+1)$-move protocol is, in general, approximately Q^{μ}, where Q is the number of oracle queries performed by the attacker. In general, this is the best one can hope for, as it is easy to see that this loss applies to the μ-fold sequential repetition of Σ protocols, but it raises the question whether certain (natural) classes of interactive proofs feature a milder security loss. In this work, we give positive and negative results on this question. On the positive side, we show that for $(k_1, \ldots, k_{\mu})$-special-sound protocols (which cover a broad class of use cases), the knowledge error degrades linearly in Q, instead of Q^{μ}. On the negative side, we show that for t-fold parallel repetitions of typical $(k_1, \ldots, k_{\mu})$-special-sound protocols with $t \geq \mu$ (and assuming for simplicity that t and Q are integer multiples of μ), there is an attack that results in a security loss of approximately $\frac{1}{2}Q^{\mu}/\mu^{\mu+1}$.

T. Attema, S. Fehr & M. Klooß (2023): **Fiat-Shamir Transformation of Multi-Round Interactive Proofs (Extended Version).** – Journal of Cryptology, 36, art. no. 36: 45 pp.

Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head

(Abstract) We present a new method for transforming zero-knowledge protocols in the designated verifier setting into public-coin protocols, which can be made non-interactive and publicly verifiable. Our transformation applies to a large class of ZK protocols based on oblivious transfer. In particular, we show that it can be applied to recent, fast protocols based on *vector oblivious linear evaluation* (VOLE), with a technique we call *VOLE-in-the-head,* upgrading these protocols to support public verifiability. Our resulting ZK protocols have linear proof size, and are simpler, smaller and faster than related approaches based on MPC-in-the-head. To build VOLE-in-the-head while supporting both binary circuits and large finite fields, we develop several new technical tools. One of these is a new proof of security for the SoftSpokenOT protocol (Crypto 2022), which generalizes it to produce certain types of VOLE correlations over large fields. Secondly, we present a new ZK protocol that is tailored to take advantage of this form of VOLE, which leads to a publicly verifiable VOLE-in-the-head protocol with only 2x more communication than the best, designated-verifier VOLE-based protocols. We analyze the soundness of our approach when made non-interactive using the Fiat-Shamir transform, using round-by-round soundness. As an application of the resulting NIZK, we present FAEST, a post-quantum signature scheme based on AES. FAEST is the first AES-based signature scheme to be smaller than SPHINCS+, with signature sizes between 5.6 and 6.6 kB at the 128-bit security level. Compared with the smallest version of SPHINCS+ (7.9 kB), FAEST verification is slower, but the signing times are between 8x and 40x faster.

C. Baum, L. Braun, C. Delpech de Saint Guilhem, M. Klooß, E. Orsini, L. Roy & P. Scholl (2023): **Publicly Verifiable Zero-Knowledge and Post-Quantum Signatures from VOLE-in-the-Head.** – In: H. Handschuh & A. Lysyanskaya (eds.): Advances in Cryptology – CRYPTO 2023. Lecture Notes in Computer Science, vol. 14085: 581–615.

New Design-oriented Theory on Transparency and Privacy Publishing Practices

Companies usually publish privacy notices to establish transparency of information privacy practices (TIPP). However, privacy notices yield, at best, not much value for establishing TIPP and often make it even worse. In an article published in Information Systems Research, we presented an information systems design theory clarifying what to build instead.

T. Dehling & A. Sunyaev (2023): **A Design Theory for Transparency of Information Privacy Practices.** – Information Systems Research, articles in advance: 22 pp.

BEST POSTER AWARD

Beware of Website Hackers: Developing an Awareness Video to Warn for Website Hacking

(Abstract) Websites that are not well maintained can be vulnerable to hackings. One type of hacking that might occur is embedding redirects to fake shops into legitimate websites. We created an awareness video to address these hacking. We first conducted a content analysis to collect relevant information. We then created a video based on this information and evaluated the video with four focus group interviews with overall 13 participants from different areas of expertise. The constructive feedback from the experts allowed us to improve the video.

A. Hennig, L. Schmidt-Enke, M. Mutter & P. Mayer (2023): **Beware of Website Hackers: Developing an Awareness Video to Warn for Website Hacking.** – 19th Symposium on Usable Privacy and Security (SOUPS 2023), Anaheim, California, USA: poster.

Lessons Learned on Machine Learning for Computer Security

We identified 10 generic pitfalls that can affect the experimental outcome of AI driven solutions for computer security. We found that they are prevalent in the literature and provide recommendations for overcoming them in the future.

D. Arp, E. Quiring, F. Pendlebury, A. Warnecke, F. Pierazzi, C. Wressnegger, L. Cavallaro & K. Rieck (2023): **Lessons Learned on Machine Learning for Computer Security.** – IEEE Security & Privacy, 21 (5): 72–77.

Let It TEE: Asynchronous Byzantine Atomic Broadcast with $n > 2f$

(Abstract) Many decentralized systems can be modeled as replicated state machines, i.e., multiple stateful programs that maintain consistency by processing operations in the same order. To be practical and resilient, protocols to realize replicated state machines among n replicas have to cope with f faulty or malicious replicas (called "byzantine"). Asynchronous Byzantine Atomic Broadcast (ABAB) is one such protocol that usually tolerates only a third of replicas to be byzantine ($n > 3f$). By using Trusted Execution Environments (TEEs), a trusted hardware component commonly available in cloud infrastructure, we improved an existing ABAB protocol to tolerate up to half of its replicas to be byzantine ($n > 2f$) and prove that its security properties can be maintained. Additionally, our construction also significantly reduced the necessary communication between replicas.

M. Leinweber & H. Hartenstein (2023): **Brief Announcement: Let It TEE: Asynchronous Byzantine Atomic Broadcast with n ≥ 2f + 1.** – 37th International Symposium on Distributed Computing (DISC 2023). Leibniz International Proceedings in Informatics (LIPIcs), 281: 43:1–43:7, Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

BEST PAPER AWARD

eMinD: Efficient and Micro-Flow Independent Detection of Distributed Network Attacks

(Abstract) Network infrastructures are critical and, therefore, subject to harmful attacks against their operation and the availability of their provided services. Detecting such attacks, especially in high-performance networks, is challenging considering the detection rate, reaction time, and scalability. Attack detection becomes even more demanding concerning networks of the future facing increasing data rates and flow counts. With eMinD, we present an approach that scales well to high data rates and large amounts of data flows. eMinD investigates aggregated traffic data, i.e., it is not based on micro-flows and their inherent scalability problems. We evaluate eMinD with real-world traffic data, compare it to related work, and show that eMinD outperforms micro-flow-based approaches regarding the reaction time, scalability, and the detection performance. We reduce required state space by 99.97%. The average reaction time is reduced by 90%, while the detection performance is even increased, although highly aggregating arriving traffic. We further show the importance of micro-flow-overarching traffic features, e.g., IP address and port distributions, for detecting distributed network attacks, i.e., DDoS attacks and port scans.

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.

Fooling XAI with Explanation-Aware Backdoors

(Abstract) The overabundance of learnable parameters in recent machine-learning models renders them inscrutable. Even their developers can not explain their exact inner workings anymore. For this reason, researchers have developed explanation algorithms to shed light on a model's decision-making process. Explanations identify the deciding factors for a model's decision. Therefore, much hope is set in explanations to solve problems like biases, spurious correlations, and more prominently attacks like neural backdoors. In this paper, we present explanation-aware backdoors, which fool both, the model's decisions and the explanation algorithm in the presence of a trigger. Explanation-aware backdoors therefore can bypass explanation-based detection techniques and "throw a red herring" at the human analyst. While we have presented successful explanation-aware backdoors in our original work, "Disguising Attacks with Explanation-Aware Backdoors", in this paper, we provide a brief overview and a focus on the dataset "German Traffic Sign Recognition Benchmark" (GTSRB). We evaluate a different trigger and target explanation compared to the original paper and present results for GradCAM explanations. Supplemental material is publicly available at <https://intellisec.de/research/xai-backdoor>.

M. Noppel & C. Wressnegger (2023): **Poster: Fooling XAI with Explanation-Aware Backdoors.** – CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security: 3612–3614.

Self-adaptive Software Intensive Systems

Software-intensive systems must operate effectively in uncertain real-world conditions, where potential uncertainties arise from changes in the operational environment and user goals. A prominent strategy to address uncertainties is self-adaptation, typically implemented through a feedback loop. This loop collects additional data during operation, uses the data to resolve uncertainties, and makes decisions to modify it in response to changing conditions. Engineering self-adaptive systems poses new challenges, particularly in the context of microservice-based applications. To address these challenges, we have developed RAMSES, a Reusable Autonomic Manager for microServices. RAMSES employs a feedback control loop model to ensure the satisfaction of user-defined dependability attributes for a microservice application at runtime. RAMSES's control loop components are implemented as microservices themselves, and the design emphasizes ease of reuse across different microservice applications. Extensions of self-adaptive systems to include the antifragility property are under investigation.

V. Riccio, G. Sorrentino, M. Camilli, R. Mirandola & P. Scandurra (2023): **Engineering Self-adaptive Microservice Applications: An Experience Report.** – In: F. Monti, S. Rinderle-Ma, A. Ruiz Cortés, Z. Zheng & M. Mecella (eds.): Service-Oriented Computing. ICSOC 2023. Lecture Notes in Computer Science, vol. 14419: 227–242.

V. Riccio, G. Sorrentino, E. Zamponi, M. Camilli, R. Mirandola & P. Scandurra (2024): **RAMSES: An Artifact Exemplar for Engineering Self-adaptive Microservice Applications.** – SEAMS '24: Proceedings of the 19th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, 2024: 161–167.

"I just stopped using one and started using the other": Motivations, Techniques, and Challenges when Switching Password Managers

(Abstract) This paper explores what motivates password manager (PM) users in the US to switch from one PM to another, the techniques they employ when switching, and challenges they encounter throughout. Through a screener (*n* = 412) followed by a main survey (*n* = 54), we find that browser-based PMs are the most widely used, with most of these users motivated to use the PM due to convenience. Unfortunately, password reuse remains high. Most participants that switch PMs do so for usability reasons, but are also motivated by cost, as third-party PMs' full suite of features often require a subscription fee. Some PM-switchers are also motivated by recent security breaches, such as what was reported at LastPass in the Fall of 2022, with some participants losing trust in LastPass and PMs generally as a result. Those that switch mostly employ manual techniques of moving their passwords, e.g., copying and pasting their credentials from their previous to their new PM, despite most PMs offering ways to automatically transfer credentials in bulk across PMs. Assistance during the switching process is limited, with less than half of participants that switched receiving guidance during the switching process. From these findings, we make recommendations to PMs that can improve their overall user experience and use, including eliciting and acting on regular feedback from users as well as making PM settings more easily reachable and customizable by end-users.

C.W. Munyendo, P. Mayer & A.J. Aviv (2023): **"I just stopped using one and started using the other": Motivations, Techniques, and Challenges when Switching Password Managers.** – CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security: 3123–3137.

Towards Practical Brainwave-based User Authentication

(Abstract) Brainwave measuring devices have transitioned from specialized medical tools to user-friendly and economically accessible consumer products. This shift has opened new avenues for pervasive services, with applications spanning brain-computer interfaces (BCIs), disease detection, criminal trials, and, notably, authentication in computer security. Electroencephalography (EEG) signals, being difficult to steal and revocable, present an attractive biometric option. However, the practical deployment of these signals is hindered by security threats, usability issues, and privacy concerns. To this end, we expect to improve the overall performance of authentication systems using consumer-grade devices, gain a better understanding of user attitudes toward this type of authentication, and protect the user's privacy against unauthorized use of samples collected during enrollment and verification.

M. Fallahi, P. Arias-Cabarcos & T. Strufe (2023): **Poster: Towards Practical Brainwave-based User Authentication.** – CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security: 3627–3629.

Framework for Interaction with Explainable Artificial Intelligence in Natural Language

RIXA (Real-time Explainable Artificial Intelligence) is a framework that supports interaction in natural language with AI models and methods of eXplainable Artificial Intelligence (XAI). By integrating large language models (LLM) with XAI methods, a wide variety of end user groups can interact with AI models and explanations of model behavior. RIXA can be thought of as ChatGPT for AI models, i.e., a chat bot that can be used to request explanations and have them explained to varying degrees of detail. This increases the transparency of data processing through AI. The approach will also be used in production systems in the future. The framework is available on GitHub, can be operated completely locally and in a data protection-friendly manner, and is suitable for conducting studies by other scientists thanks to its flexible expandability using plugins.

M. Becker, F. Schwall, V. Vishvesh, S. Wu, P. Birnstill & J. Beyerer (2023): **RIXA – Explaining Artificial Intelligence in Natural Language.** – 2023 IEEE International Conference on Data Mining Workshops (ICDMW), Shanghai, China: 875–884.

Vulnerabilities Analysis and Risk Assessment in Energy Systems

Vulnerability analysis in energy systems includes assessing different types of testbeds, i.e., physical, virtual, and hybrid ones for Smart Grids (SGs) from different perspectives of cybersecurity. Preliminary work on the characterization of these testbeds based upon the MITRE ICS Attack Matrix was published. First, the evaluation was based upon different qualitative metrics such as costs, fidelity, and flexibility. The second contribution was focused on the applicable tactics and techniques for each testbed, assessing how well attack experiments can be realistically simulated using them. It was successfully highlighted how different implementations of testbeds come with their own limitations and challenges, which must be considered by a researcher while selecting a testbed for a specific use case. In agreement with previous assessment of testbeds based on the MITRE ICS matrix, the current research was focused on in-depth assessments of testbeds from IT and OT perspectives, which could serve as foundations for the development of defensive techniques. Different vulnerabilities of components at "KASTEL Security Lab Energy" and EPIC testbed were tabulated. Some of them were exploited to showcase the adversarial impact on each testbed. Additionally, the work also covered exploiting the limitations of industrial protocols, such as Modbus TCP, S7, and MMS. To further analyze the different vulnerabilities, a hybrid risk assessment process using fuzzy analytical hierarchy processes was developed.

A. Mumrez, M.M. Roomi, H.C. Tan, D. Mashima, G. Elbez & V. Hagenmeyer (2024): **Comparative Study on Smart Grid Security Testbeds Using MITRE ATT&CK Matrix.** – 2023 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), Glasgow, UK: 1–7.

S. Canbolat, G. Elbez & V. Hagenmeyer (2023): **A New Hybrid Risk Assessment Process for Cyber Security Design of Smart Grids Using Fuzzy Analytic Hierarchy Processes.** – at-Automatisierungstechnik, 71 (9): 779–788.

The World's Fastest Protocol for Private Set Intersection

Many important tasks such as paternity testing, genetic compatibility testing or contact tracing can be performed in a privacy-preserving way using private set intersection. In more detail, private set intersection allows parties A and B, which each hold a set S_A resp. S_B, to compute the intersection of their sets in a way that only the intersection is learned, but nothing about the elements not in the intersection. At KASTEL, we developed the world's fastest protocol for private set intersection. To this end, we relied on trusted hardware in the form of so-called secure enclaves. In contrast to previous protocols, we require much less trust in the secure enclaves, making them a viable practical assumption. With our protocol, we can compute the intersection of two sets with 224 elements each in 5.5 seconds, making it the fastest protocol for private set intersection. This work was published at ASIACRYPT 2023 and presented at the 2023 Lindau Nobel Laureate Forum.

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.

Auditable Cyber-Surveillance: Enforcing the Lawfulness in Lawful Interception

KASTEL researchers Valerie Fetzer, Michael Klooß, Markus Raiber, Jörn Müller-Quade, and Andy Rupp proposed security protocols that facilitate the surveillance of encrypted or anonymous communication while enabling the detection of mass and unlawful surveillance at the same time. Lawful Interception systems are required by law all over the world (e.g., by the European Council Resolution on the Lawful Interception of Telecommunications) and should allow law enforcement agencies with a valid warrant to surveil the communication of a suspect. Currently deployed systems, however, lack strong technical mechanisms for auditing the lawfulness of surveillance actions. First results of this research project were presented at ASIACRYPT 2023, one of the three flagship conferences organized by the International Association for Cryptologic Research (IACR).

V. Fetzer, M. Klooß, J. Müller-Quade, M. Raiber & A. Rupp (2023): Universally Composable Auditable Surveillance. – In: J. Guo & R. Steinfeld (eds.): Advances in Cryptology – ASIACRYPT 2023. Lecture Notes in Computer Science, vol. 14439: 453–487.

Collaborative Research Center 1608 Convide

Since its start in October 2023, Convide has reached several early milestones, indicating that the ambitious project has started successfully. With a majority of the researcher positions filled, all sub-projects have commenced work. At several large-scale meetings, over fifty participants developed roadmaps for the first funding period and discussed preliminary research results. Particularly noteworthy, the supplementary proposal submitted by Jun.-Prof. Maike Schwammberger was granted by the DFG, extending research area A by an additional project.

Selection of 2024 ...

Successful Pre-project MEDI:CUS – Sustainable Health Care for Baden-Württemberg

Emilia Grass is on the advisory board of MEDI:CUS, a study on a cloud-based health data infrastructure to enhance healthcare in Baden-Württemberg. The "health cloud" aims to unify stakeholders and leverage digitalization. MEDI:CUS seeks to bridge health data gaps with a secure, research-compatible system, promoting data-driven medical progress. Integration into the European health data space promises better outcomes, efficiency, and cost savings. An implementation project has been commissioned based on MEDI:CUS findings.

<https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/baden-wuerttemberg-baut-cloudplattform-medicus-fuer-gesundheitsdaten-auf>.

Exploring Phishing Threats through QR Codes in Naturalistic Settings

DISTINGUISHED PAPER AWARD

(Abstract) QR codes, designed for convenient access to links, have recently been appropriated as phishing attack vectors. As this type of phishing is relatively and many aspects of the threat in real conditions are unknown, we conducted a study in naturalistic settings (*n* = 42) to explore how people behave around QR codes that might contain phishing links. We found that 28 (67%) of our participants opened the link embedded in the QR code without inspecting the URL for potential phishing cues. As a pretext, we used a poster that invited people to scan a QR code and contribute to a humanitarian aid. The choice of a pretext was persuasive enough that 22 (52%) of our participants indicated that it was the main reason why they scanned the QR code and accessed the embedded link in the first place. We used three link variants to test if people are able to spot a potential phishing threat associated with the poster's QR code (every participant scanned only one variant). In the variants where the link appeared legitimate or it was obfuscated by a link shortening service, only two out of 26 participants (8%) abandoned the URL when they saw the preview in the QR code scanner app. In the variant when the link explicitly contained the word "phish" in the domain name, this ratio rose to 7 out of 16 participants (44%). We use our findings to propose usable security interventions in QR code scanner apps intended to warn users about potentially phishing links.

F. Sharevski, M. Mossano, M.F. Veit, G. Schiefer & M. Volkamer (2024): **Exploring Phishing Threats through QR Codes in Naturalistic Settings.** – Symposium on Usable Security and Privacy (USEC) 2024, San Diego, California, USA: 17 pp.

Recovering Trace Links between Software Documentation and Code

(Abstract) Software development involves creating various artifacts at different levels of abstraction and establishing relationships between them is essential. Traceability link recovery (TLR) automates this process, enhancing software quality by aiding tasks like maintenance and evolution. However, automating TLR is challenging due to semantic gaps resulting from different levels of abstraction. While automated TLR approaches exist for requirements and code, architecture documentation lacks tailored solutions, hindering the preservation of architecture knowledge and design decisions. This paper presents our approach TransArC for TLR between architecture documentation and code, using component-based architecture models as intermediate artifacts to bridge the semantic gap. We create transitive trace links by combining the existing approach ArDoCo for linking architecture documentation to models with our novel approach ArCoTL for linking architecture models to code. We evaluate our approaches with five open-source projects, comparing our results to baseline approaches. The model-to-code TLR approach achieves an average F1-score of 0.98, while the documentation-to-code TLR approach achieves a promising average F1-score of 0.82, significantly outperforming baselines. Combining two specialized approaches with an intermediate artifact shows promise for bridging the semantic gap. In future research, we will explore further possibilities for such transitive approaches.

J. Keim, S. Corallo, D. Fuchß, T. Hey, T. Telge & A. Koziolek (2024): **Recovering Trace Links between Software Documentation and Code.** – ICSE '24: Proceedings of the IEEE/ACM 46th International Conference on Software Engineering, 2024, art. no. 215: 13 pp.

Labeling NIDS Rules with MITRE ATT&CK Techniques Using ChatGPT

(Abstract) A typical analyst spends much time and effort investigating alerts from network intrusion detection systems (NIDS). Available NIDS rules for enterprise and industrial control systems are not always accompanied by high-level explanations that allow for building valid hypotheses about the attacker's techniques and intentions. The plethora of rules and the lack of high-level information necessitates new automated methods for alert enrichment. Large language models, such as ChatGPT, encompass a vast amount of knowledge, including cyber threat intelligence such as ports and protocols (low-level) and MITRE ATT&CK techniques (high-level). Despite being a very new technology, ChatGPT is increasingly used in order to automate processes that experts previously performed. In this paper, we explore the ability of ChatGPT to reason about NIDS rules while labeling them with MITRE ATT&CK techniques. We discuss prompt design and present results on ChatGPT-3.5, ChatGPT-4, and a keyword-based approach. Our results indicate that both versions of ChatGPT outperform a baseline that relies on a-priori frequencies of the techniques. ChatGPT-3.5 is much more precise than ChatGPT-4, with a little reduction in recall.

N. Daniel, F.K. Kaiser, A. Dzega, A. Elyashar & R. Puzis (2024): **Labeling NIDS Rules with MITRE ATT&CK Techniques Using ChatGPT.** – In: S. Katsikas et al. (eds.): Computer Security. ESORICS 2023 International Workshops. ESORICS 2023. Lecture Notes in Computer Science, vol. 14399: 76–91.

A Conceptual and Architectural Characterization of Antifragile Systems

Antifragility, a recently emerged term, directs the design of ICT systems to ensure trustworthiness despite dynamic and evolving operating contexts. We have presented a characterization of antifragility within a well-known dependability taxonomy, aiming to conceptually clarify its implications as a design guideline and its relationships with other approaches sharing similar objectives. Building upon this characterization, we have presented a framework fostering the engineering of antifragile systems.

V. Grassi, R. Mirandola & D. Perez-Palacin (2024): **A Conceptual and Architectural Characterization of Antifragile Systems.** – Journal of Systems and Software, 213, art. no. 112051: 15 pp.

Detecting Automatic Software Plagiarism via Token Sequence Normalization

(Abstract) While software plagiarism detectors have been used for decades, the assumption that evading detection requires programming proficiency is challenged by the emergence of automated plagiarism generators. These generators enable effortless obfuscation attacks, exploiting vulnerabilities in existing detectors by inserting statements to disrupt the matching of related programs. Thus, we present a novel, language-independent defense mechanism that leverages program dependence graphs, rendering such attacks infeasible. We evaluate our approach with multiple real-world datasets and show that it defeats plagiarism generators by offering resilience against automated obfuscation while maintaining a low rate of false positives.

T. Sağlam, M. Brödel, L. Schmid & S. Hahner (2024): **Detecting Automatic Software Plagiarism via Token Sequence Normalization.** – ICSE '24: Proceedings of the IEEE/ACM 46th International Conference on Software Engineering, art. no. 113: 1–13.

Student Visitors from Brazil

A group of 16 students from the Brazilian *Universidade Federal de Campina Grande* (UFCG) visited KASTEL Security Research Labs (SRL) from April 22 to 25, 2024. The visit was funded by the German Academic Exchange Service (DAAD) via the "Study Visits and Study Seminars for Groups of Foreign Students to Germany 2024". Central aspects of the visit were the scientific exchange between our guests from UFCG and our researchers at KASTEL SRL, especially from the Research Group for Privacy and Security, as well as the promotion of intercultural understanding and cooperation. Besides the scientific aspects, the students had the opportunity to learn more about KIT in general including study and PhD opportunities.

Better Together: The Interplay Between a Phishing Awareness Video and a Link-centric Phishing Support Tool

(Abstract) Two popular approaches for helping consumers avoid phishing threats are phishing awareness videos and tools supporting users in identifying phishing emails. Awareness videos and tools have each been shown on their own to increase people's phishing detection rate. Videos have been shown to be a particularly effective awareness measure; link-centric warnings have been shown to provide effective tool support. However, it is unclear how these two approaches compare to each other. We conducted a between-subjects online experiment (n = 409) in which we compared the effectiveness of the NoPhish video and the TORPEDO tool and their combination. Our main findings suggest that the TORPEDO tool outperformed the NoPhish video and that the combination of both performs significantly better than just the tool. We discuss the implications of our findings for the design and deployment of phishing awareness measures and support tools.

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, art. no. 826: 1–60.

SoK: Explainable Machine Learning in Adversarial Environments

(Abstract) Modern deep learning methods have long been considered black boxes due to the lack of insights into their decision-making process. However, recent advances in explainable machine learning have turned the tables. Post-hoc explanation methods enable precise relevance attribution of input features for otherwise opaque models such as deep neural networks. This progression has raised expectations that these techniques can uncover attacks against learning-based systems such as adversarial examples or neural backdoors. Unfortunately, current methods are not robust against manipulations themselves. In this paper, we set out to systematize attacks against post-hoc explanation methods to lay the groundwork for developing more robust explainable machine learning. If explanation methods cannot be misled by an adversary, they can serve as an effective tool against attacks, marking a turning point in adversarial machine learning. We present a hierarchy of explanation-aware robustness notions and relate existing defenses to it. In doing so, we uncover synergies, research gaps, and future directions toward more reliable explanations robust against manipulations.

M. Noppel & C. Wressnegger (2024): **SoK: Explainable Machine Learning in Adversarial Environments.** – 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, California, USA: 19 pp.

PolySphinx: Extending the Sphinx Mix Format with Better Multicast Support

(Abstract) With the advent of consumer wearables that capture brain activity, the use of brainwaves to verify a user's identity has been proposed as a convenient alternative to passwords. While recent work on brain biometrics shows feasible performance, it falls short in considering practical applicability. We propose a new solution, BrainNet, which trains a Siamese Network to measure the similarity of two electroencephalogram (EEG) inputs, and uses time-locked brain reactions instead of continuous mental activity to improve accuracy. This approach removes the need for retraining the brainwave recognition system, a common pitfall in current solutions, facilitating practical deployment. Furthermore, BrainNet achieves Equal Error Rates (EERs) of 0.14% in verification mode and 0.34% in identification mode, outperforming the state of the art even when evaluated under unseen attacker scenarios.

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), San Francisco, California, USA: 48.

Explanation-driven Self-adaptation using Model-agnostic Interpretable Machine Learning

(Abstract) Self-adaptive systems increasingly rely on machine learning techniques such as Neural Networks as black-box models to make decisions and steer adaptations. The lack of transparency of these predictive models makes it hard to explain adaptation decisions and their possible effects on the surrounding environment. Furthermore, adaptation decisions in this context are typically the outcome of expensive optimization processes. The complexity arises from the inability to directly observe or comprehend the internal mechanisms of the black-box predictive models, which requires employing iterative methods to explore a possibly large search space and optimize according to many goals. Here, balancing the trade-off between effectiveness and cost becomes a crucial challenge. In this paper, we propose explanation-driven self-adaptation, a novel approach that embeds model-agnostic interpretable machine learning techniques into the feedback loop to enhance the transparency of the predictive models and gain insights that help drive adaptation decisions effectively by significantly reducing the cost of planning them. Our empirical evaluation demonstrates the cost-effectiveness of our approach using two evaluation subjects in the robotics domain.

F.R. Negri, N. Nicolosi, M. Camilli & R. Mirandola (2024): **Explanation-driven Self-adaptation using Model-agnostic Interpretable Machine Learning.** – SEAMS '24: Proceedings of the 19th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, 2024: 189–199.

Requirements Classification for Traceability Link Recovery

(Abstract) Being aware of and understanding the relations between the requirements of a software system to its other artifacts is crucial for their successful development, maintenance, and evolution. There are approaches to automatically recover this traceability information, but they fail to identify the actual relevant parts of the requirements. Recent large language model-based requirements classification approaches have shown to be able to identify aspects and concerns of requirements with promising accuracy. Therefore, we investigate the potential of those classification approaches for identifying irrelevant requirement parts for traceability link recovery between requirements and code. We train the large language model-based requirements classification approach NoRBERT on a new dataset of requirements and their entailed aspects and concerns. We use the results of the classification to filter irrelevant parts of the requirements before recovering trace links with the fine-grained word embedding-based FTLR approach. Two empirical studies show promising results regarding the quality of classification and the impact on traceability link recovery. NoRBERT can identify functional and user-related aspects in the requirements with an F1-score of 84%. With the classification and requirements filtering, the performance of FTLR could be improved significantly and FTLR performs better than state-of-the-art unsupervised traceability link recovery approaches.

T. Hey, J. Keim & S. Corallo (2024): **Requirements Classification for Traceability Link Recovery.** –
32nd IEEE International Requirements Engineering 2024 Conference (RE'24), Reykjavik, Iceland: 13 pp.

Provable Security for the Onion Routing and Mix Network Packet Format Sphinx

(Abstract) Onion routing and mix networks are fundamental concepts to provide users with anonymous access to the Internet. Various corresponding solutions rely on the Sphinx packet format. However, flaws in Sphinx's underlying proof strategy were found recently. It is thus currently unclear which guarantees Sphinx actually provides, and, even worse, there is no suitable proof strategy available. In this paper, we restore the security foundation for all these works by building an analytical framework for Sphinx. We discover that the previously-used Decisional Diffie-Hellman (DDH) assumption is insufficient for a security proof and show that the Gap Diffie-Hellman (GDH) assumption is required instead. We apply it to prove that a slightly adapted version of the Sphinx packet format is secure under the GDH assumption. We are thus, to the best of our knowledge, the first to provide a detailed, in-depth security proof for Sphinx that holds. Our adaptations to Sphinx are necessary, as we demonstrate with an attack on sender privacy that would otherwise be possible in Sphinx's adversary model.

P. Scherer, C. Weis & T. Strufe (2024): **Provable Security for the Onion Routing and Mix Network Packet Format Sphinx.** – Proceedings on Privacy Enhancing Technologies Symposium, 2024 (4): 755–783.

Fantômas: Understanding Face Anonymization Reversibility

(Abstract) Face images are a rich source of information that can be used to identify individuals and infer private information about them. To mitigate this privacy risk, anonymizations employ transformations on clear images to obfuscate sensitive information, all while retaining some utility. Albeit published with impressive claims, they sometimes are not evaluated with convincing methodology. Reversing anonymized images to resemble their real input – and even be identified by face recognition approaches – represents the strongest indicator for flawed anonymization. Some recent results indeed indicate that this is possible for some approaches. It is, however, not well understood, which approaches are reversible, and why. In this paper, we provide an exhaustive investigation in the phenomenon of face anonymization reversibility. Among other things, we find that 11 out of 15 tested face anonymizations are at least partially reversible and highlight how both reconstruction and inversion are the underlying processes that make reversal possible.

J. Todt, S. Hanisch & T. Strufe (2024): **Fantômas: Understanding Face Anonymization Reversibility.** – Proceedings on Privacy Enhancing Technologies Symposium, 2024 (4): 24–43.

Project DIRECTIONS (Data Protection Certification for Educational Information Systems): KIT Researchers Present a List of Criteria for Data Protection-Compliant School Information Systems

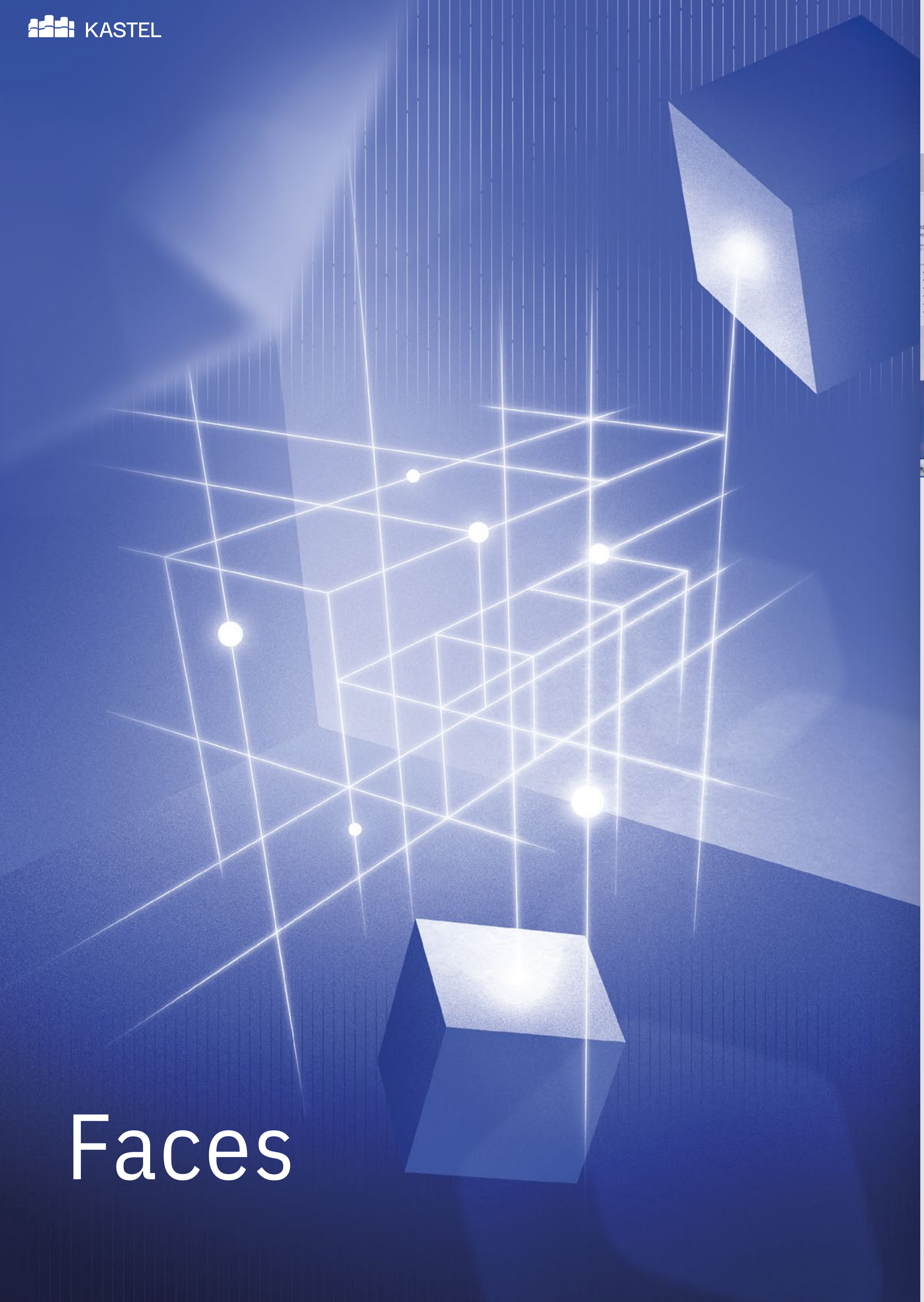
Information systems such as learning apps, content platforms, or video tools are playing an increasingly important role in everyday digital school life. However, there are often concerns about protecting the data of students. In the DIRECTIONS project, researchers from the Karlsruhe Institute of Technology (KIT) and the University of Kassel want to remedy this situation with a data protection certification and ensure greater security for information systems in schools. The participants have now published a list of criteria that serves as the basis for the first official data protection certification in the education sector. The BMBF-funded project started in 2021 and ends in 2027. The aim is to be able to use the DIRECTIONS certification as a reliable instrument for the use of school applications in the future.

K. Brecker, P. Danylak, J.T. Helmke, G. Hornung, M. Kohpeiß, H. Link, S. Lins, H.-H. Schild, S. Schindler, E. Späthe & A. Sunyaev (2024): **DIRECTIONS-Kriterienkatalog – Fassung 0.7.** – 166 pp., online available: <www.directions-cert.de>.

On the Influence of Conventional and Automated Market Makers on Market Quality in Cryptoeconomic Systems

(Abstract) Decentralized exchanges (DEXs) have become an alternative to centralized exchanges (CEXs) for trading assets in the form of tokens in cryptoeconomic system markets. The emergence of DEXs is strongly driven by their potential to tackle challenges for market quality originating from CEXs by design, such as opaque market-making strategies and centralization of power. A core reason for this is the lack of an analysis concept for investigating influences of market makers, including automated market makers (AMMs) used in DEXs and conventional market makers used in CEXs, on market quality in cryptoeconomic systems. To better understand influences of market makers on market quality in cryptoeconomic systems, we developed an analysis concept based on our formal price model grounded in established concepts of market microstructure. We demonstrate the usefulness of the analysis concept by examining conventional market makers on CEXs (i.e., Binance and Coinbase) and automated market makers (AMMs) on DEXs (i.e., Uniswap v2 and Uniswap v3). The main purpose of this work is to support the analysis of influences of different market makers on market quality in cryptoeconomic systems. This is useful to better understand how cryptoeconomic systems can ensure high market quality and safeguard market participants when issuing tokens.

D. Kirste, A. Poddey, N. Kannengießer & A. Sunyaev (2024): **On the Influence of Conventional and Automated Market Makers on Market Quality in Cryptoeconomic Systems.** – Electronic Markets, accepted paper.



Faces

Interdisciplinarity

Interdisciplinarity is one of the main pillars of **KASTEL Security Research Labs**! We explore the topic of security and safety from the perspective of different disciplines. Only with this broader view is it possible to address the pressing issues in such a way that applicable and user-friendly solutions can be derived.

25

Fellows

1

Young Investigator Group

Our team of consists of specialists from the disciplines:

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

We live our professional networking through:

- Joint discussions,
- Joint seminars,
- Joint projects,
- Joint publications.

Two new Fellows and a Young Investigator Group are now part of **KASTEL Security Research Labs**. We welcome to our team:

- Emilia Grass,
- Raffaela Mirandola,
- Friederike Zufall

NEW YOUNG INVESTIGATOR GROUP (2024)

“I AM AT KASTEL BECAUSE ...

... IT PROVIDES AN IDEAL ENVIRONMENT FOR INTERDISCIPLINARY COLLABORATION AND ADVANCED RESEARCH ON CRITICAL INFRASTRUCTURE RESILIENCE.”

Jun.-Prof. Dr. Emilia Grass

Research Group Building Healthcare Resilience against Cyber-Attacks at KIT

Personal

Emilia Grass leads a Helmholtz research group “Building Network Resilience in Healthcare against Cyber-Attacks” at KASTEL Security Research Labs (SRL). 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.

Research Interest

Dr. Emilia Grass’ research is focused on enhancing cyber resilience in healthcare, integrated within KASTEL SRL. Her work leverages quantitative and data-driven methods to fortify critical healthcare infrastructures against cyber attacks. In collaboration with the University of Mannheim and Imperial College London, the aim of her projects at KASTEL SRL is to integrate risk quantification, simulation, and optimization to ensure patient safety and business continuity in the case of disruptions. Grass’ research addresses the growing risks posed by digitalization in healthcare, developing novel methods to predict, mitigate, and recover from cyber incidents. Her interdisciplinary approach combines operations research, machine learning, and cybersecurity, thereby striving to create resilient, adaptive systems capable of withstanding and swiftly recovering from disruptions.

Selected Publications

S. Ghafur, E. Grass, N. Jennings & A. Darzi (2019): *The Challenges of Cybersecurity in Health Care: the UK National Health Service as a Case Study.* – The Lancet Digital Health, 1 (1): e10–e12.

N. O’Brien, E. Grass, G. Martin, M. Durkin, A. Darzi & S. Ghafur (2021): *Developing a Globally Applicable Cybersecurity Framework for Healthcare: a Delphi Consensus Study.* – BMJ Innovations, 2021 (7): 199–207.

NEW FELLOW (2023)

“I AM AT KASTEL BECAUSE ...

... RESEARCH ON SOFTWARE QUALITY ASSESSMENT FOCUSING ON DEPENDABILITY AND SECURITY REQUIRES INTERDISCIPLINARY RESEARCH AND COLLABORATION.”

Prof. Dr. Raffaela Mirandola

Research Group Self-Adaptive Software-Intensive Systems at KIT

Personal

Raffaela Mirandola has held from September 2023 the Otto Lehmann’s professorship in Software Engineering for Self-adaptive Systems. She is part of the Steering Committee of leading international conferences, like *IEEE ICSA* for software architecture, and *IEEE/ACM SEAMS* for self-adaptive systems. She is part of the Editorial Board of the *ACM Transactions on Autonomous and Adaptive Systems*, and Special Issue co-editor for the *Journal of Systems and Software, Elsevier.*

Research Interest

My research focuses on developing techniques and tools for engineering complex autonomous software-intensive systems that can meet quality requirements, even in the presence of unforeseen events like malicious attacks. Emphasis is placed on resilience and antifragility. Resilience denotes a system’s ability to absorb and recover from changes, while antifragility involves not only withstanding change but also improving as a result. Antifragile systems thrive and evolve when facing adverse events. Designing and validating such systems requires new approaches surpassing current architectures, frameworks, and tools in adaptive systems design. This entails a principled definition of antifragility, along with suitable metrics and analysis approaches to guide decisions during design and demonstrate trustworthiness.

Selected Publications

M. Camilli, R. Mirandola & P. Scandurra (2023): *Enforcing Resilience in Cyber-physical Systems via Equilibrium Verification at Runtime.* – ACM Transactions on Autonomous and Adaptive Systems, 18 (3): 12:1-12:32.

F.R. Negri, N. Nicolosi, M. Camilli & R. Mirandola (2024): *Explanation-driven Self-adaptation using Model-agnostic Interpretable – Machine Learning.* – SEAMS ’24: Proceedings of the 19th International Symposium on Software Engineering for Adaptive and Self-Managing Systems, 2024: 189-199.

NEW FELLOW (2023)

“I AM AT KASTEL BECAUSE …

… COMPUTATIONAL LAW MAY FUNDAMENTALLY TRANSFORM OUR LEGAL SYSTEMS AND THE WAY WE THINK ABOUT ‘LAW’.”

TT-Prof. Dr. Frederike Zufall

Chair for Public Law and Computer Science at the Center for Applied Legal Studies (ZAR), KIT

Personal

Frederike Zufall studied law (first state examination 2010 with honours) at Humboldt University of Berlin and the Université Panthéon-Sorbonne (Paris I). This was followed by a doctorate at the Humboldt University with a comparative law thesis on Japanese law. She completed her legal clerkship and the Second State Examination in Law at the Higher Regional Court of Frankfurt am Main. In 2016, she was appointed to an assistant professorship at the Waseda Institute for Advanced Study at Waseda University in Tokyo, where she conducted interdisciplinary research until 2019. After another year at the Free University of Brussels (Law Science Technology Society Research Group), she started her habilitation project at the Max Planck Institute for Research on Collective Goods in Bonn. Since June 2023, she has held the Chair of Public Law and Computer Science at KIT.

Research Interest

We conduct interdisciplinary research on “computational law” at the interface between law and computer science. Computational law is an approach to automated legal reasoning and targets the operationalization of law through computational methods. We investigate the extent to which the law itself and legal decision-making may be subject to approaches on AI. The focus here is on methods of machine learning and natural language processing (NLP). The alleged shift towards AI and automated legal decision-making would not only fundamentally affect legal systems, but also requires us to rethink existing concepts on (legal) “security” once the law itself becomes technology.

Findings from this applied research also form the basis of legal dogmatic research on the regulation of AI and data law at the EU level, also from the perspective of comparative law.

Prof. Dr. Patricia Arias Cabarcos

Research Group IT Security at University of Paderborn

My research interests lie at the intersection of security, privacy, and human-computer interaction. My vision is that people should not be cognitively stressed, or need to have deep technical knowledge to be able to live a secure digital life. I am convinced that only achieving this vision will unlock true cybersecurity.

Within my group, we seek to understand how users behave, think, and handle technology and how technology impacts users’ behavior. We then develop new solutions that are easy to use, inclusive, and privacy-friendly. Our current main areas to which we contribute are password security and usability, novel behavioral biometrics, behavioral data privacy, privacy awareness, and transparency-enhancing technologies.

Selected Publications

P. Arias-Cabarcos, S. Khalili & T. Strufe (2023): *‘Surprised, Shocked, Worried’: User Reactions to Facebook Data Collection from Third Parties.* – Proceedings on Privacy Enhancing Technologies, 2023 (1): 384–399.

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.

PD Dr.-Ing. Ingmar Baumgart

Competence Center for IT Security at FZI Research Center for Information Technology

With the increasing digitization of all industries, the topics of IT security and data protection are becoming increasingly important. In particular the trend of connecting embedded systems to the internet (“Internet of Things”, IoT) significantly increases their attack surface.

Therefore, our research group focuses on new concepts and methods to secure such IoT products. This includes, in particular, procedures and tools for identifying IT security vulnerabilities in networked systems.

In addition to preventive protection mechanisms, approaches to detecting attacks are also being investigated. The research in these areas is strongly application-oriented in the domains of mobility, production, and energy.

Selected Publications

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.

M. Wehmer & I. Baumgart (2023): *The Fast Rise of Cautious Vehicle-to-X: Towards Evaluating Misbehavior Detection in the Field.* – 2023 IEEE 26th International Conference on Intelligent Transportation Systems (ITSC): 3930–3936.

Prof. Dr. Bernhard Beckert

Research Group Application-oriented Formal Verification at KIT

Our research area is the application of formal, logic-based methods for the specification and verification of software – from models to source code. Our research extends from the theoretical foundations to the development of new tools.

To allow for scalable verification of object-oriented software, we are developing approaches with which different tools can be combined and the correctness of a program can be measured probabilistically. We are analyzing smart contracts and their security as a new application field for formal verification. To this end, we are developing a model-driven, verification-based approach for developing secure and correct smart contract applications.

Selected Publications

J. Schiffl, A. Weigl & B. Beckert (2023): *Static Capability-based Security for Smart Contracts.* – IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), 2023: 110–117.

F. Lanzinger, Ch. 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.

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

The Vision and Fusion Lab and Fraunhofer IOSB jointly operate the laboratory for the Subtopic "Engineering Security for Production Systems" and coordinate its research activities on industrial cybersecurity.

The cross-institutional team conducts cybersecurity research for mixed production, from fully automated production to human-machine collaboration in manufacturing. It covers topics for designing and operating secure production infrastructures, i.e., industrial network security, black- and grey-box testing for industrial devices, industrial cyber risk assessment, as well as attack detection and mitigation strategies. To also enable trustworthy interactive manufacturing assistance systems that protect individuals' privacy, trusted computing technologies and remote attestation protocols are leveraged to safeguard distributed usage control mechanisms and multi-party encryption schemes. The related research is aimed at increasing the transparency of personal data processing by means of data provenance tracking and eXplainable AI methods.

Selected Publications

P.G. Wagner & J. Beyerer (2022): *Quantifying Trustworthiness in Decentralized Trusted Applications.* – Proceedings, 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems (Sat-CPS '22): 67–76.

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

Prof. Dr. Veit Hagenmeyer

Director of the Institute for Automation and Applied Informatics (IAI) at KIT

Energy systems, being critical infrastructures, can be the target of attacks. To address Generic Object Oriented Substation Event (GOOSE) poisoning, which can result in Denial-of-Service (DoS) attacks, a new method called *EDA4GNeT* [1] was created. This utilizes mathematical modeling to analyze network traffic behavior in substations, thereby enabling anomaly detection.

This Intrusion Detection System (IDS) is tested through simulations of a DoS attack on a substation. To further enhance the robustness of IDS, adversarial attacks are investigated. In fact, learning-based components are integral to energy systems. Testing ML-based IDS against Modbus TCP attacks helps understand malicious capabilities and allow us to share datasets from the KASTEL Security Lab Energy with the community. This research sets the stage for further exploration of adversarial attacks and IDS in the context of energy systems [2].

Selected Publications

[1] 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.

[2] 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.

Prof. Dr. Hannes Hartenstein

Research Group Decentralized Systems and Network Services (DSN) at KIT

The research group "Decentralized Systems and Network Services" currently focuses on blockchains and distributed ledger technologies, broadcast and consensus processes, secure smart contracts, peer-to-peer networks and their monitoring, decentralized messaging using the example of Matrix, identity management and access control, as well as secure and privacy-compliant data processing in partially trustworthy environments.

As part of the Helmholtz Topic "Engineering Secure Systems" the security and privacy of decentralized systems are being researched, especially for "mobility-as-a-service". Systems are designed and analyzed that enable independent mobility service providers to quickly reach a consensus without having to reveal secrets, as well as systems with which payments can be made and billed very efficiently and securely.

Selected Publications

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, Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

M. Grundmann, M. Baumstark & H. Hartenstein (2022): *On the Peer Degree Distribution of the Bitcoin P2P Network.* – 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Shanghai, China, 2022: 1–5.

Prof. Dr.-Ing. Anne Koziolek

Research Group Modelling for Continuous Software Engineering (MCSE) at KIT

Our research group is concerned with the early phases and activities in the development of dependable software, or more generally, dependable software-intensive technical systems. We are interested in providing systematic yet low-cost model-based design space exploration to support making good design decisions, which are a major success factor for mission-critical software-intensive technical systems and fundamental for a security-by-design approach.

One strand of research is to recover traces from security-related requirements to models and implementation to automate model-based security analyses such as dataflow analyses. With this research, our group wants to conciliate model-based software engineering with development processes that have fast and agile feedback cycles and thus combine the benefits of both approaches.

Selected Publications

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 Research Group Artificial Intelligence, Cybersecurity and Programming Languages at University of Southern Denmark

I research the design and evaluation of end-user viable information security and privacy. My focus is to understand human perceptions and behaviors to ensure end-users' security and privacy when they interact with technology. Thereby, independently of whether the end-user of a security solution is a layperson, an administrator, or a developer, the focus always lies on making security & privacy solutions viable for the target audience, i.e., taking into consideration their specific needs and skill sets.

While my research encompases a broad range of topics in the cybersecurity and privacy fields, I focus on the user authentication, awareness & education, notifications, e-mail communication, and factors influencing individuals' and organizations' security posture.

Selected Publications

P. Mayer, Y. Zou, B.M. Lowens, H.A. Dyer, K. Le, F. Schaub & A.J. Aviv (2023): *Awareness, Intention, (In) Action: Individuals' Reactions to Data Breaches.* – ACM Transactions on Computer-Human Interaction, 30 (5): 77:1–77:53.

C.W. Munyendo, P. Mayer & A.J. Aviv (2023): *"I just stopped using one and started using the other": Motivations, Techniques, and Challenges when Switching Password Managers.* – CCS '23: Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security: 3123–3137.

Prof. Dr. Jörn Müller-Quade

Research Group Cryptography and Security at KIT

Simply protecting against known attacks on IT systems only leads to short-term security until new attacks are found. In cryptography and IT security, we therefore follow the paradigm of provable security: In a model of reality, clearly defined security goals cannot be violated under explicitly given assumptions. If attacks are nevertheless detected, the underlying model or the assumptions used were not sufficiently realistic. With this knowledge, the model can be improved or assumptions can be discarded. One goal of our research is to develop protocols for distributed computation on secret data.

Methods for secure multi-party computation make it possible, e.g., to compute statistics on sensitive data without learning the individual data. Security gaps can also result from the interaction of components in a system. The "universal compatibility" framework is a security model that was specifically developed to enable a modular approach: If individual components are proven to be secure, then the security is also maintained when the components interact.

Selected Publications

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.

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.

Prof. Dr. André Platzer

Research Group Logic of Autonomous Dynamic Systems at KIT

We develop the logical foundations of cyber-physical systems to answer the question of how to trust computers to control physical processes. Solving this challenge is the key to computer support in vital areas such as automobiles, aircraft and train systems, as well as robotics.

We are designing programming languages with logics that provide proofs as guarantees of correctness. One of the most fundamental discoveries behind our "Differential Dynamic Logic" is that properties of global behavior of the underlying dynamic systems can be analyzed purely from the logic of local changes without having to solve the dynamics. We pursue the corresponding theory, practice, and application.

Selected Publications

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.

Prof. Dr. iur. Oliver Raabe

Research Group Legal Informatics and IT Security Law (ITR) at the Center for Applied Legal Studies (ZAR), KIT

As a legal information scientist, I have been dealing with legal issues at the interface of technology regulation and compliant technology design since 2000.

In this context, data protection and IT security law regularly serve as references for the monitoring and derivation of legal options for action. On this basis, our research group at KASTEL Security Research Labs deals with the normative framework of end-to-end IT security in future intelligent transport systems. Due to the multilateral character of the relevant regulatory regimes, the consistency of the regulatory structure is particularly challenging in this case.

The work on legal informatics aims to support software architects in the implementation of the substantive investigations on IT security in mobility law as patterns for legally compliant system design.

Selected Publications

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

Our research group works on the interplay of software architecture and predictable software quality as well as view-based design methods for software-intensive technical systems.

This work consists of, on the one hand, research on software architecture quality analysis, which includes architecture-based simulators for performance and reliability and architecture-based analyses of confidentiality, vulnerability, and maintainability. And, on the other hand, research on the extension of software engineering-based approaches to handle complexity to make them applicable to non-software domains, such as meta-modeling, model and view-based development, and view, version, and variant consistency management. Both research lines are specialized for automotive and mobility applications as well as for Industry 4.0 domain.

Selected Publications

M. Walter, S. Hahner, T. Bureš, P. Hnětynka, R. Heinrich & R. Reussner (2023): *Architecture-based Attack Propagation and Variation Analysis for Identifying Confidentiality Issues in Industry 4.0.* – at–Automatisierungstechnik, 71 (6): 443–452.

S. Seifermann, R. Heinrich, D. Werle & R. Reussner (2022): *Detecting Violations of Access Control and Information Flow Policies in Data Flow Diagrams.* – Journal of Systems and Software, 184: 111138.

Dr. Andy Rupp

Research Group Cryptographic Protocols at KIT and University of Luxemburg

Our team tackles the tension between the need for privacy protection and the conflicting practical requirements of important application domains such as mobility, payments, and communication. We do not only aim for efficiency and scalability but particularly for compliance with domain-specific laws and regulations, business models, value-added services, user requirements, amongst others, thereby enabling a practical deployment in the first place.

This work includes combining requirements such as the need for surveillance under certain well-defined conditions, anti-money laundering, data analytics, etc., with privacy protection by technical means. Our team at KASTEL Security Research Labs is working on dedicated security models as well as provably secure cryptographic primitives and protocols for privacy, accountability, and transparency.

Selected Publications

V. Fetzer, M. Klooß, J. Müller-Quade, M. Raiber & A. Rupp (2023): *Universally Composable Auditable Surveillance.* – In: J. Guo & R. Steinfeld (eds.): Advances in Cryptology. ASIA-CRYPT 2023. Lecture Notes in Computer Science, vol. 14439: 453–487.

A. Jolfaei, A. Rupp, S. Schiffner & T. Engel (2024): *Why Privacy-Preserving Protocols are Sometimes not Enough: A Case Study of the Brisbane Toll Collection Infrastructure.* – Proceedings on Privacy Enhancing Technologies, 2024 (1): 232–257.

Prof. Dr.-Ing. Ina Schaefer

Research Group Test, Validation and Analysis of Software-Intensive Systems (TVA) at KIT

Security-by-Design and By-Construction Engineering: Our working group develops concepts and tools to ensure functional properties and security properties by construction.

Post-hoc Quality Assurance: Complementary to this, a special focus of the research work is on efficient and effective testing methods, especially for multi-variant and evolving software systems. This also includes validation procedures for intelligent systems in which parts of the functionality are implemented using trained AI components.

Software Diversity (Variability & Adaptability): Modern software systems are highly configurable in order to adapt to different requirements and environmental contexts. The working group researches how the robustness and resilience of software systems can be increased through diversity.

Selected Publications

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. Proceedings, 20th International Conference (SEFM 2022): 209–226.

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): 35 pp.

Dr.-Ing. Gunther Schiefer

Research Group Digital Privacy at KIT

We are concerned with the question of how digital information (personal or company) can remain private or confidential as far as possible and still allow the development of its respective benefits. For this purpose, business processes and information systems have been designed in such a way that information is available when and where it is absolutely needed, but not beyond that (need-to-know principle).

To achieve this, we use, e.g., methods of cryptography, intelligent data distribution (fog- and edge-computing), etc., in diverse domains and environments (mobile, cloud, Internet of Things (IoT), etc.) Furthermore, the business process design is considered in order to identify and exploit solution potential. In addition, compliance requirements (e.g., GDPR, ISO 27.001) are always considered from the very beginning

Selected Publications

Y. Wuwang & G. Schiefer (2022): *Consumer-friendly Methods for Privacy Protection Against Cleaning Robots.* – In: W. Li, S. Furnell & W. Meng (eds.): Attacks and Defenses for the Internet-of-Things. ADIoT 2022. Lecture Notes in Computer Science, vol. 13745: 102–121.

F. Sharevski, M. Mossano, M. Veit, G. Schiefer & M. Volkamer (2024): *Exploring Phishing Threats through QR Codes in Naturalistic Settings.* – Symposium on Usable Security and Privacy (USEC) 2024, San Diego, California, USA: 17 pp.

Prof. Dr. Indra Spiecker gen. Döhmann

Chair for Law of Digitization at University of Cologne

Our working group conducts research within the "Human and Societal Factors" Research Group and in the Energy Lab.

Our research focuses on legal and interdisciplinary challenges in data protection law and IT security law, as well as information technology in various scenarios. In this context, our working group analyzes the technical and legal foundations, as well as concrete requirements arising from legal acts such as the European General Data Protection Regulation (GDPR) or IT security norms and develops possible technology based procedures and measures for their implementation and enforcement. The working group also deals with all privacy and security related aspects of digitization and its regulation in various scenarios and specifications, such as artificial intelligence, service robotics, critical infrastructures like energy, or e-voting.

Selected Publications

I. Spiecker gen. Döhmann, V. Papakonstantinou, P. de Hert & G. Hornung (eds., 2023): *General Data Protection Regulation. Article-by-Article Commentary.* – 1211 pp., Beck, Nomos, Hart.

I. Spiecker genannt Döhmann (2023): *§ 20: Digitalisierung, Informationsgesellschaft, Massendaten, Künstliche Intelligenz.* – In: U. Kischel & H. Kube (eds.): Handbuch des Staatsrechts. 4th ed.: 899–934, C.F. Müller.

Prof. Dr. Thorsten Strufe

Research Group Practical IT Security (PS) at KIT

As a "Privacy and Security Lab", the research interests of our group lie in privacy protection and the resilience of networked systems. We address three research fields: behavioral privacy, anonymous communication, network security.

In the first field, we investigate the identifiability of individuals based on their behavior – and which private properties can be learned about them. This relates, for example, to activities in the metaverse and on video ("CeTI", KASTEL Security Research Labs), activities on the web (BMBF "Synthiclick"), or actual mobility, e.g., in smart cities (BMBF "Propolis"). Of course, we are simultaneously developing protective mechanisms to enable smart city applications, for example, without compromising user privacy. In our DFG projects "Resilient Network Embeddings" and "Anonymous Group Communication", we deal with questions of privacy protection for communication on the Internet, as well as the provision of communication possibilities even in light of censorship or network failures. Additionally, we investigate attacks and possible protection mechanisms on 5G/6G mobile communication, for instance also by means of quantum physics.

Selected Publications

P. Arias-Cabarcos, M. Matin, 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.

À. Miranda-Pascual, P. Guerra-Balboa, J. Parra-Arnau, T. Strufe & J. Forné (2023): *SoK: Differentially Private Publication of Trajectory Data.* – 3rd Privacy Enhancing Technologies Symposium (PETS), 2023 (2): 496–516.

Prof. Dr. Ali Sunyaev

Research Group Critical Information Infrastructures (cii) at KIT

Within KASTEL Security Research Labs, the cii research group is concerned with sociotechnical research on IT security, especially with respect to the (de)centralization of information systems in the context of mobility systems and the prevention of malicious user behavior. Specifically, our group investigates how the decentralization of socio-technical systems impacts security properties and how different degrees of decentralization of information systems influence consumers (e.g., in terms of fairness).

Using theory-driven design and development methods, computational tools, and empirical research, our work offers a new and interesting perspective to gain insights into the complex processes of future digital systems and their reliable application in the real world.

Selected Publications

T. Dehling & A. Sunyaev (2023): *A Design Theory for Transparency of Information Privacy Practices.* – Information Systems Research, accepted manuscript: 22 pp.

M. Greulich, S. Lins, D. Pienta, J.B. Thatcher & A. Sunyaev (2024): *Exploring Contrasting Effects of Trust in Organizational Security Practices and Protective Structures on Employees' Security-related Precaution Taking.* – Information Systems Reseach, accepted manuscript: 23 pp.

Prof. Dr. Melanie Volkamer

Research Group SECUSO (Security · Usability · Society) at KIT

We research security and privacy. Our focus is on humans and our society. We use the so-called "human-centered security and privacy by design" approach. We research methods for the development and evaluation of (1) user-friendly security and privacy protection measures as well as (2) awareness, education, and training measures especially for companies. Our research group has to be very interdisciplinary in order to be successful. Among others, the group comprises scientists in computer science, mathematics, and psychology. The group is also well known for its research on usable verifiable electronic voting systems. Our research results have been published in a classical way. The following list is a selection of measures developed in the course of our research that are publicly available for citizens:

- Secure communication, incl. phishing email detection and message encryption: e.g., awareness posters, *NoPhish* videos, *TORPEDO*, *PassSec+*, security training, and awareness robot *START*,
- Protection of user accounts, e.g., *ACCESS*, awareness tools, awareness posters,
- Privacy protection: e.g., *Privacy Friendly Apps*.

Selected Publications

M. Volkamer, O. Kulyk, J. Ludwig & N. Fuhrberg (2022): *Increasing Security without Decreasing Usability: A Comparison of Various Verifiable Voting Systems.* – Proceedings of the 18th Symposium on Usable Privacy and Security (SOUPS 2022): 233–252.

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.

Prof. Dr. Marcus Wiens

Chair of General Business Administration, in particular Innovation and Risk Management at TU Bergakademie Freiberg

Our research focuses on economic and systemic risk and innovation management, critical infrastructure protection (esp. cybersecurity), and cooperative & behavioral approaches to risk management. Methodologically, we work primarily with approaches from operations research, game theory, experimental research (behavioral economics), and empirical surveys.

In the area of cyber risks, our team applies approaches to attacker modeling (incl. cyber threat intelligence, CTI), risk quantification, economic assessments of cyber risks via damage simulations for companies (e.g., process value analysis), and supply chains. On the user level, we investigate risk attitudes and beliefs (esp. trust) as well as optimal behavioral incentives. I am involved in several research projects that focus on approaches to foster coordination and cooperation and strengthen the systemic resilience of systems with innovative approaches.

Selected Publications

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, 32 pp.

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.

TT-Prof. Dr. Christian Wressnegger

Research Group Intelligent System Security (IntelliSec) at KIT

My research revolves around combining machine learning (or AI in the broader scope) and computer security. My team and I develop methods in the area of system security and application security, for instance, approaches for attack detection or vulnerability discovery in software. Moreover, we research the robustness of machine learning against attacks striving for "secure AI". In this context, I am particularly interested in the security of explainable AI (XAI).

In the scope of KASTEL Security Research Labs, we contribute to all three areas application domains (energy, production, and mobility) in various projects. We publish our work in highly prestigious journals and proceedings of conferences (e.g., *IEEE S&P, USENIX Security, ACM CCS*, and *ISOC NDSS*). We even won the "Distinguished Paper Award" of the *USENIX Security Symposium* 2022.

Selected Publications

M. Noppel & C. Wressnegger (2024): *SoK: Explainable Machine Learning in Adversarial Environments.* – 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, California, USA: 19 pp.

Q. Zhao & C. Wressnegger (2023): *Holistic Adversarially Robust Pruning.* – Proceedings of the 11th International Conference on Learning Representations (ICLR): 22 pp.

Prof. Dr. Martina Zitterbart

Research Group at Institute of Telematics (TM) at KIT

The research group headed by Martina Zitterbart is dedicated to protocols, algorithms, and architectures for high-performance communications. An important topic addressed is network security, whether concerning the Internet or the industrial Internet. Research on network security is carried out in the context of KASTEL Security Research Labs. Protection methods for critical infrastructures such as the emerging smart grid are designed, analyzed, and prototypically implemented.

By applying machine learning, new ways to detect and mitigate network attacks are explored. Machine learning is also applied in the context of traffic engineering and congestion control. For better robustness and security in critical infrastructures, lightweight redundancy mechanisms are researched. Further focal points of our research include software-based networks as well as autonomous self-driving networks.

Selected Publications

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, 2023: 159–167

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

Prof. Dr. J. Marius Zöllner

Research Group Applied Technical Cognitive Systems at KIT

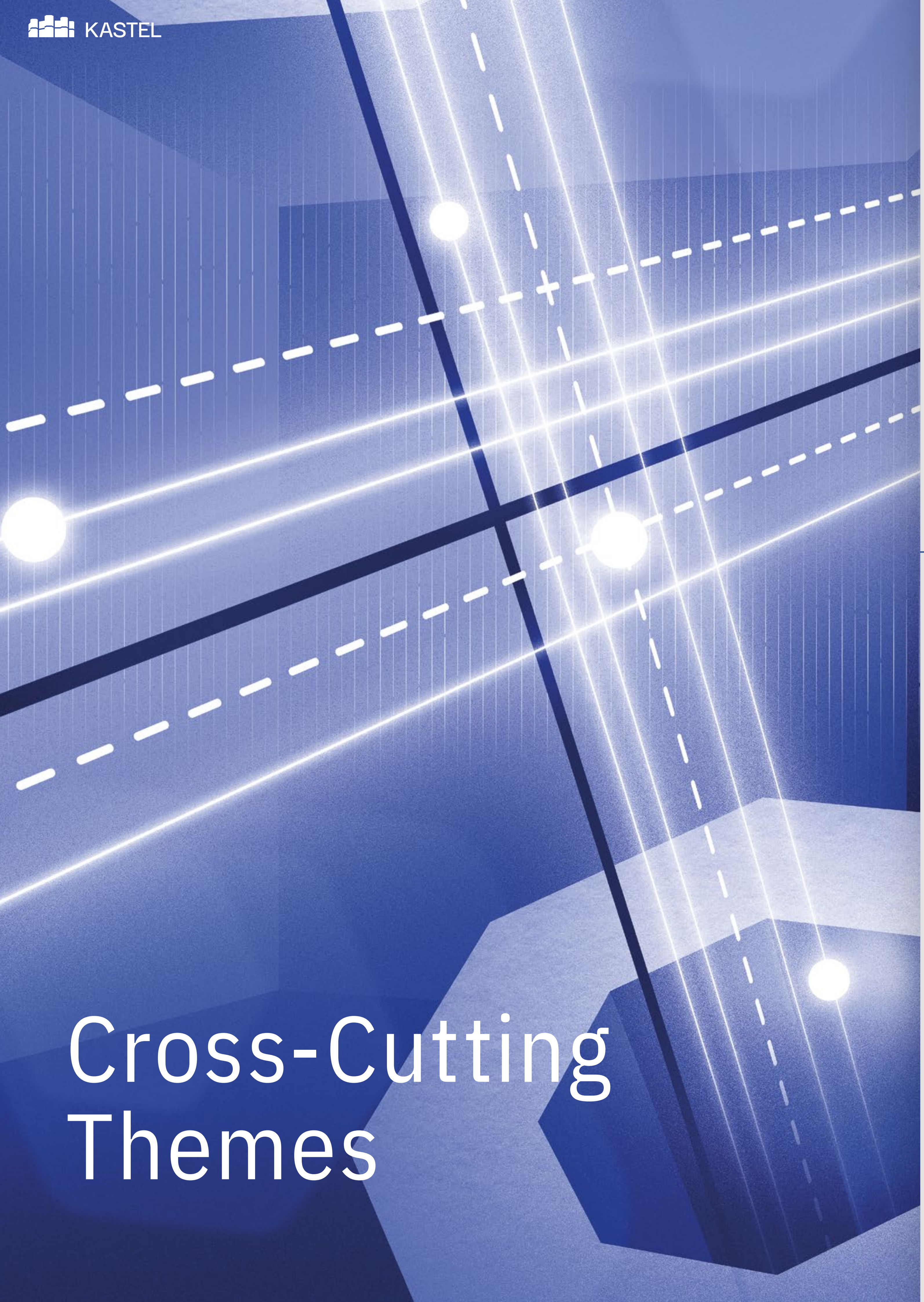
Our research focus is on making perception in automated vehicles safe, secure, and interpretable. We study realistic adversarial attacks on camera-based perception modules, including traffic light detection, and evaluate them in the *Testfeld Autonomes Fahren Baden-Württemberg.*

We work on dynamic and sparse deep learning model architectures, like mixtures of experts, which combine efficient inference with an increased model capacity to withstand attacks. Additionally, we analyze the effect of robustness enhancement measures on model interpretability to understand the decision-making process of neural networks.

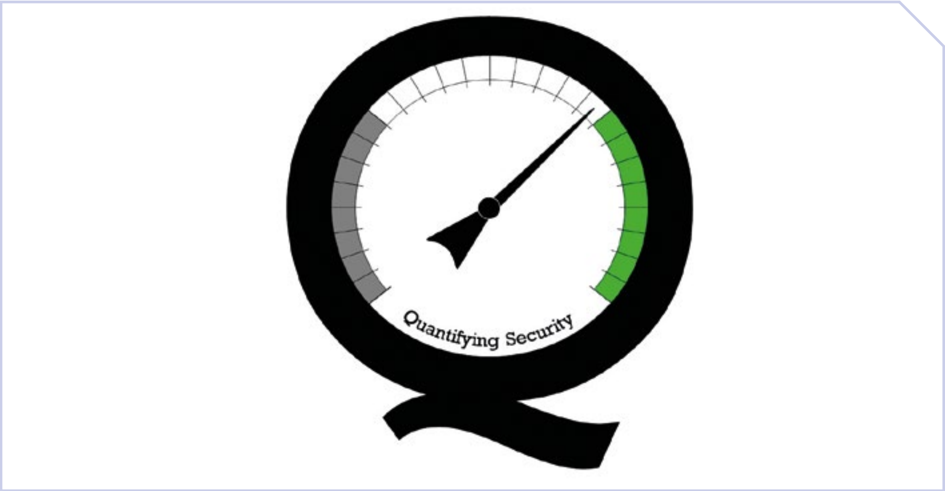
Selected Publications

S. Pavlitska, N. Lambing & J.M. Zöllner (2023): *Adversarial Attacks on Traffic Sign Recognition: A Survey.* – 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Tenerife, Spain: 6 pp.

S. Pavlitska, C. Hubschneider, L. Struppek & J.M. Zöllner (2023): *Sparsely-gated Mixture-of-Expert Layers for CNN Interpretability.* – 2023 International Joint Conference on Neural Networks (IJCNN), Gold Coast, Australia: 10 pp.



Cross-Cutting Themes



"Quantifying Security"

Methods for Engineering Secure Systems

Involved Fellows

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

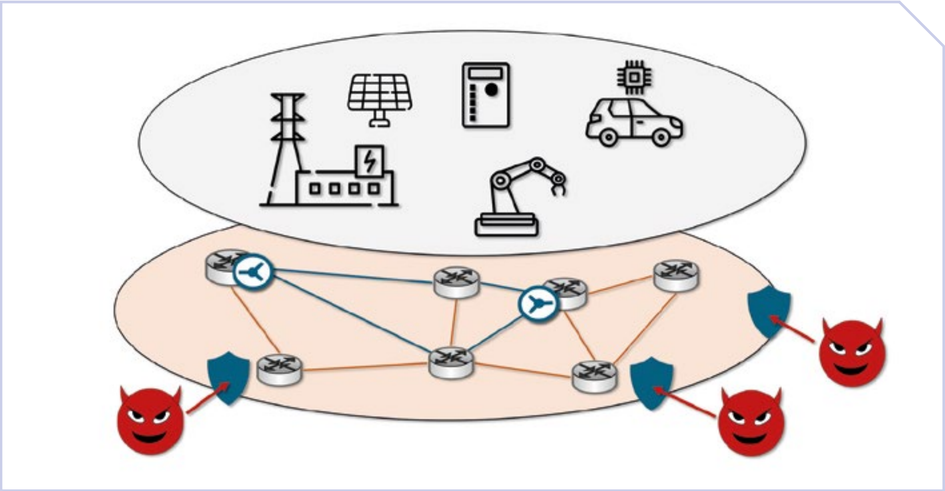
Quantifying Cyber Risk: Enabling Decisions in a World of Multiple Crises

In a world of multiple crises and hybrid warfare, the number of cyber attacks rapidly grows. Given that critical and non-critical infrastructures are increasingly connected and software-defined, cyber attacks may have devastating effects and pose a critical threat to society.

As of today, it is a huge and unsolved challenge to quantify cybersecurity risks in an accurate and scientifically sound way. Thus, it is difficult to decide whether it is adequate to deploy a system or, given a fixed budget, how to obtain the best return on security investment.

The interdisciplinary KASTEL research group "Quantifying Security", comprised of researchers with backgrounds in cryptography, privacy, practical IT security, formal methods, software engineering, business economics, and operations research, contributes towards solving this problem. Key contributions are the research of disciplinary quantitative security indicators that cover meaningful aspects of a system, for example the correctness of code or the cost of invalidating assumptions made in a security proof. By combining these disciplinary indicators that have a rigorous theoretical foundation with less formal security analyses, a quantitative statement of a system's security can be made, which is a first and context-agnostic prerequisite towards quantifying context-dependent risk. The research is performed in close collaboration with the three KASTEL labs for mobility, energy, and production.

Jeremias Mechler



“Secure Computation and Communication”

Methods for Engineering Secure Systems

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

Critical Infrastructures in a World of Conflicts

In a world increasingly entangled in geopolitical conflicts, the security and availability of critical infrastructures is of prime importance. Bad actors threaten these infrastructures in order to destabilize societies and economies. The research group “Secure Computation and Communication” (C&C) strives to combat this by developing novel methods for securing these critical computation and communication infrastructures. Examples of such critical communication infrastructures are control networks for production and energy systems, but also the Internet as the backbone of our modern social and political life.

One class of attacks that threatens the availability of such infrastructures are Distributed Denial of Service (DDoS) attacks. We developed *eMinD* [1], a micro-flow-independent DDoS detector that scales well to high data rates and large numbers of flows. *eMinD* employs Machine Learning (ML) models that detect and identify attack patterns. Other Denial of Service attacks target specific protocols, such as those used to add redundancy for low latency control applications. We identified this attack surface and developed *TRUST* [2], a novel redundancy mechanism that is impervious to such attacks, while simultaneously introducing only minimal additional overhead.

In conclusion, C&C works to identify and combat threats to protect the critical infrastructures we all depend on.

Felix Neumeister & Samuel Kopmann

References

[1] 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, 2023: 159-167.

[2] F. Neumeister, M. Göckel & M. Zitterbart (2023): *TRUST: Transparent Redundancy for UDP Streams.* – 2023 IEEE 21st International Conference on Industrial Informatics (INDIN), Lemgo, 2023: 7 pp.

Look for the 'who-area'

Tip 2

Look for fake 'who-areas'

“Human and Societal Factors”

Methods for Engineering Secure Systems

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

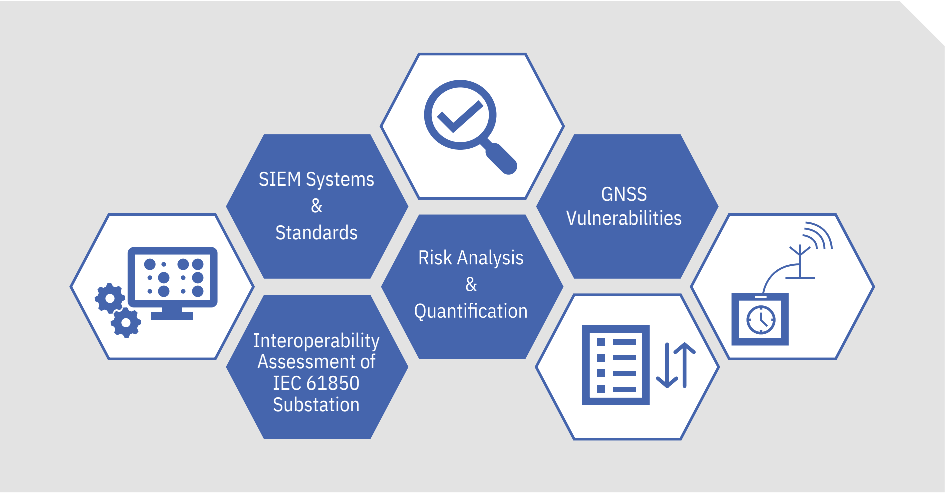
Effective Strategies to Counter Phishing Attacks in Crisis Situations

One of the key aspects in the research of the Human and Societal Factors research group are the direct benefits for society as a whole resulting from our research. For instance, the cybersecurity awareness materials developed in our research can help mitigate the impact of cyber threat actors in diverse situations of crises.

Humanitarian crises, such as floodings or war, often lead to public calls for donations to support relief efforts. Unfortunately, cybercriminals are known to exploit these calls by launching phishing campaigns. These campaigns impersonate legitimate organizations, aiming to steal sensitive information or funds from well-intentioned donors. Our awareness materials and our *TORPEDO* Thunderbird add-on which are both based on the validated and effective *NoPhish* anti-phishing concept help users to protect themselves against malicious campaigns.

Similarly, organizations operating critical infrastructure can easily be affected by crises, even when this is not immediately apparent. For instance, the Russian cyber attacks on the KA-Sat satellite network on the day of the invasion of Ukraine also saw German wind parks go offline as collateral damage, since they depend on the same satellite network for communcation. German organizations can be collateral in phishing-based attacks as well; our awareness materials offer them an effective way to protect themselves.

Peter Mayer & Benjamin Berens



“KASTEL Security Lab Energy”

Engineering Security for Energy Systems

Involved Fellows

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

Safeguarding Digital Substations Through Risk Assessment

Smart Grids (SGs), essential to future energy systems, feature a heterogeneous structure with extensive integration between physical and IT systems. The related interdisciplinary studies at the KASTEL Security Lab Energy aim to enhance cyber-physical security and resilience in future energy systems by raising awareness and implementing countermeasures against global crises, such as disturbances or outages in electric grids. Our research emphasizes the necessity of rigorous interoperability testing of multi-vendor digital substations, recommending a two-phase configuration method to address communication issues [1]. Furthermore, our developed hybrid risk assessment method provides precise risk evaluations [2]. Using a GNSS simulator, we have successfully demonstrated various attacks in the lab and assessed their difficulty within a qualitative risk assessment in our research. Furthermore, our ongoing research to implement a tailored Security Information and Event and Management (SIEM) system for energy infrastructure is expected to enhance risk analysis by correlating security events from multiple sources. By adopting standards such as IEC 62443 and IEC 62351-7, we plan to not only strengthen defenses but also ensure compatibility across the sector. Ultimately, building on our existing knowledge and future efforts, our ongoing research aims to ensure a secure and resilient future by strengthening grids and fostering innovation.

Sine Canbolat

References

[1] G. Keppler, A. Bonetti, S. Canbolat, A. Mumrez, V. Hagenmeyer & G. Elbez (2024): *Interoperability Assessment of IEC 61850 Devices in a Multivendor Digital Substation.* – In: 6th Global Power, Energy and Communication Conference (GPECOM2024), Budapest, Hungary (in press).

[2] S. Canbolat, G. Elbez & V. Hagenmeyer (2023): *A New Hybrid Risk Assessment Process for Cyber Security Design of Smart Grids using Fuzzy Analytic Hierarchy Processes.* – at-Automatisierungstechnik, 71 (9): 779–788.

“KASTEL Security Lab Mobility”

Engineering Security for Mobility Systems

Involved Fellows

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

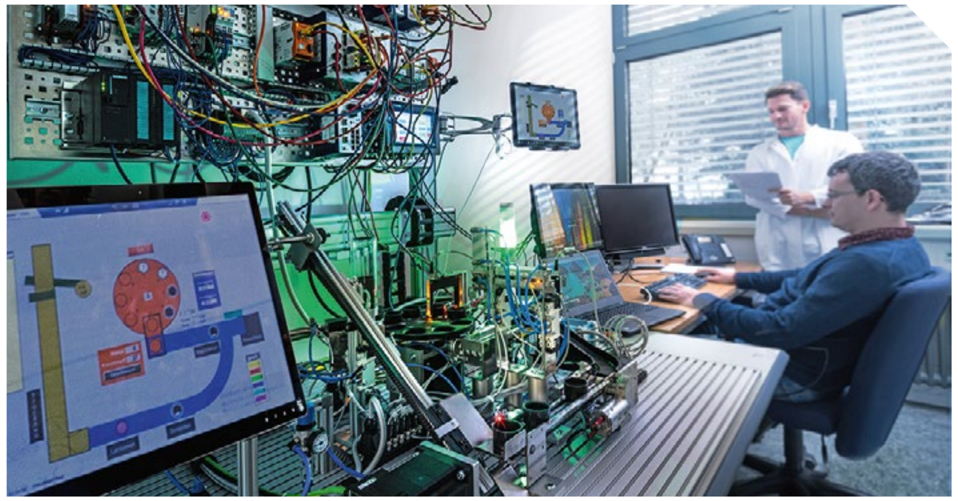
Counteracting the Mobility Crisis by Securing the Shared Mobility of the Future

Our society is threatened by a mobility crisis: The inherent conflict between sustainability and transport requires not only low-emission vehicles, but also new mobility concepts. One concept is shared mobility, in which vehicles are shared between different travelers – not only through time sharing (as with taxis or carsharing) or by sharing predefined itineraries (as with buses and trains), but also through concepts such as “mobility on demand”. Here, autonomous robotaxis are shared between travelers with similar itineraries by means of smart resource and route planning. Another concept is the provision of various mobility services as part of “mobility as a service”, thereby sharing mobility systems between different service providers. However, sharing poses inherent risks to security and privacy. Shared mobility can compromise protection goals like the confidentiality of travelers’ personal data, the integrity of the distribution of transport fees between service providers, or the availability of robotaxis and their underlying transport infrastructure. The mission for our security research is to anticipate and counteract such risks, as vulnerabilities will limit the acceptance of new mobility concepts. Securing shared mobility systems is therefore a prerequisite for sustainable mobility of the future.

References

S. Pavlitska, N. Lambing & J.M. Zöllner (2023): *Adversarial Attacks on Traffic Sign Recognition: A Survey.* – 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Tenerife, Spain: 6 pp.

M. Leinweber, N. Kannengießer, H. Hartenstein & A. Sunyaev (2023): *Leveraging Distributed Ledger Technology for Decentralized Mobility-as-a-Service Ticket Systems.* – In: H. Proff (ed.): Towards the New Normal in Mobility. 547-567, Springer.



“KASTEL Security Lab Production”

Engineering Security for Production Systems

Involved Fellows

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

Industrial Security in a World of Crisis

The 21st-century world is interconnected through evolving digital infrastructure. Healthcare, manufacturing, and education now share data for better governance, services, and compliance. This connectivity is targeted by malicious actors, causing socio-economic impact. The COVID-19 pandemic, geopolitical tensions, climate change, and economic instability have intensified these threats, thereby exposing digital vulnerabilities. In a world facing multiple crises, cybersecurity research on attack detection and security testing is indispensable. It ensures the integrity, availability, and confidentiality of information systems, safeguarding societal functions and maintaining public trust. Advanced cybersecurity measures are critical for protecting our interconnected world's digital lifelines. Critical infrastructures like manufacturing, power grids are frequent targets. Advances in threat detection and security testing are crucial for cybersecurity. At KASTEL Security Research Labs, self-learning methods have been developed to detect industrial process-targeted attacks [1]. At the same time, a cross-domain dataset [2] has been created to enhance cybersecurity threat detection research.

Security testing is essential for uncovering vulnerabilities in devices and preparing for real-world attacks. By simulating attacks [3], organizations can proactively strengthen their defenses. This continuous improvement cycle is vital for adapting to new threats.

Ankush Meshram

References

[1] A. Meshram, M. Karch, C. Haas & J. Beyerer (2023): *Towards Self-learning Industrial Process Behaviour from Payload Bytes for Anomaly Detection.* – 2023 IEEE 28th International Conference on Emerging Technologies and Factory Automation (ETFA): 8 pp.

[2] M. Karch, D. Rösch, A. Kummerow, A. Meshram, C. Haas & S. Nicolai (2022): *CrossTest: A Cross-domain Physical Testbed Environment for Cybersecurity Performance Evaluations.* – 2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA): 8 pp.

[3] A. Borcherding, N. Penkov, M. Giraud & J. Beyerer (2023): *SWaTEval: An Evaluation Framework for Stateful Web Application Testing.* – Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023): 430–441.

“Digital Democracy”

Involved Fellows at KASTEL SRL

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

Securing Democracy with Usable Secure End-to-End Verifiable Voting Systems

Recent years have seen a constant increase in digitization, further boosted by the COVID-19 pandemic. Many processes have been made easier, more accessible, and more efficient. In the same way many governmental processes are also being digitized in the hope of making them more efficient.

As a way to bolster digital participation and accessibility elections have also been digitized – what type of elections depends on the country in which the elections are conducted: from university and social elections in Germany, local parliamentary elections in Switzerland, to parliamentary elections in Estonia.

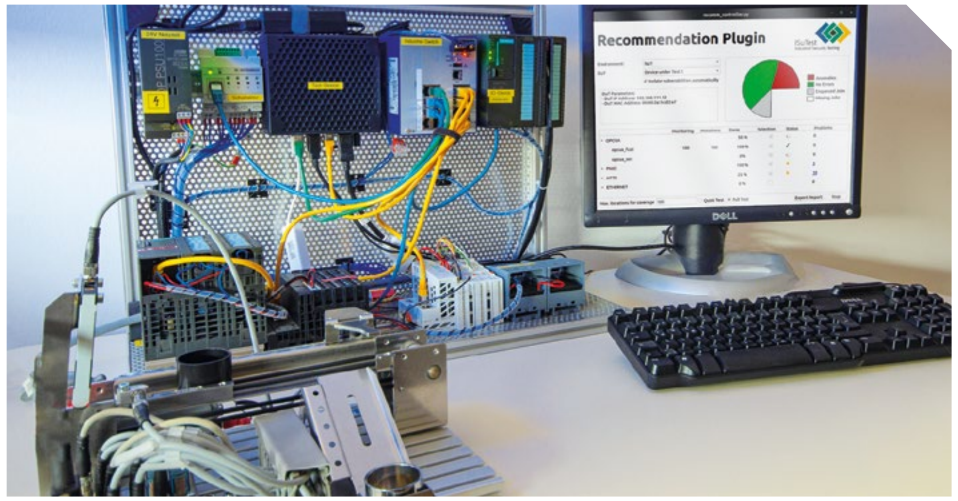
However, most systems in place rely on very strong trust assumption, e.g., one needs to fully trust them regarding vote secrecy and vote/election integrity while it is not reliably possible to detect manipulations – not even by the vendor of the system. Consequently, potential manipulations or negligence of vote secrecy cannot be independently (dis)proven. At the same time, the system – like any other Internet application – can be attacked from all over the world. Thus, there is the question of whether voters can and should still have trust in the electoral process and, by extension, in democracy itself, as voters receive no assurance that their votes are accurately recorded and counted, and that their choices remain secret. Moreover, unsatisfied voters or malicious actors might claim electoral fraud, and neither the election organizers nor the system provider would be able to conclusively disprove such allegations.

The goal of the research in the Topic “Engineering Secure Systems” is to reduce the trust assumptions by investigating on usable end-to-end verifiable voting systems – ideally providing some level of coercion-resistance.

Reference

M. Volkamer, O. Kulyk, J. Ludwig & N. Fuhrberg (2022): *Increasing Security without Decreasing Usability: A Comparison of Various Verifiable Voting Systems.* – Proceedings of the 18th Symposium on Usable Privacy and Security (SOUPS 2022): 233–252.

Contributions from our Partners



"ISuTest® – Automated Vulnerability Assessment for Industrial Automation Components"

Portrait

More and more machines and systems in the manufacturing industry are networked. This opens up opportunities, for example to improve processes with generated data. At the same time, however, there are also risks, as industrial automation components become more susceptible to faults and attacks via the network. The Industrial Security Testing Framework "ISuTest" is a tool for finding vulnerabilities in networked automation components. Discovered vulnerabilities can be fixed by the manufacturer, thus reducing the component's attack surface. In the future, robustness to attacks will be a quality criterion that manufacturers can use to set themselves apart from others.

"ISuTest" is designed as an open, extensible framework and thus sets itself apart from commercial competitors with closed-source software. The direct target group of "ISuTest" are manufacturers and integrators of automation components. It supports its users from the setup of a vulnerability test to its execution to the isolation of vulnerabilities to the post-processing of the bug to the developer, who can subsequently fix it.

"ISuTest" is deployed at different security testing labs and is actively used to search for vulnerabilities by several industrial partners. Research results from KASTEL Security Research Labs are integrated into "ISuTest" on a regular basis.

Steffen Pfrang & Christian Haas

Highlight

In 2022, "ISuTest" was nominated for the NEO Innovation Award, which is presented by the Karlsruhe Technology Region.

Cybersecurity Training Lab

Portrait

Professionally trained IT security specialists are a rare commodity in Germany. So as not to fall behind in the arms race with cyber criminals, IT teams and managers must constantly hone their skills and improve their expertise in order to stay at least one step ahead. Several Fraunhofer Institutes and universities of applied sciences are now offering a modular, part-time continuing education program to alleviate the unmet demand for training opportunities.

Training and development in the field of IT security is an issue of national interest, given that cyber attacks on critical infrastructures or industrial complexes can result in significant financial losses, the disruption of vital supply networks, or the breakdown of public order. The growing trend toward connectivity and digitalization only accentuates the threat.

Fraunhofer IOSB leads the consortium cybersecurity for industrial production and regularly offers related training sessions for industrial customers in the Security Lab for Production Systems. The training lab is also used within KASTEL Security Research Labs as an additional lab infrastructure.

Collaborative Research Center 1608 Convide

Involved Fellows at KASTEL SRL

- Bernhard Beckert
- Anne Koziolek
- André Platzer
- Ralf Reussner (Spokesperson)
- Ina Schaefer

Portrait

At the Collaborative Research Center (CRC) 1608 "Consistency in the View-Based Development of Cyber-Physical Systems", more than fifty researchers from Karlsruhe Institute of Technology, the University of Mannheim, Technical University Munich, and Technical University Dresden explore new methods for the development of cyber-physical systems (CPS).

A cyber-physical system is characterized by the integration of computational and physical processes. Influencing many sectors of our daily lives, today's CPS range from electric vehicles over modern production plants to smart home systems. The fact that CPS comprise of many electronic, mechanical, and software-controlled components poses difficult challenges for their design. First, there is a need for modern CPS to be highly dependable and secure, as well as configurable and flexible. Second, these systems can only function reliably if all parts interact seamlessly.

As a result of these requirements, developers find it difficult to control the complexity of modern CPS. Notably, abstraction alone is of little help because it leads to fewer analyzable models. To deal with this ever-increasing complexity, so-called views of the system – sub-models specific to the developer's task – are used during development. Since there exist manifold dependencies between these views, there is an urgent need for novel consistency-maintaining methods that enable shorter development and faster update cycles. By defining a new role for Software Engineering in Advanced Systems Engineering, the CRC will provide solutions that will make CPS development more agile and efficient.

sfb1608.kit.edu

Highlight

The DFG has granted the funding for a supplementary proposal by Jun.-Prof. Dr. Maike Schwammberger, creating an additional project in research area A that involves the investigation of consistency challenges for autonomous traffic agents.

HELMHOLTZ KERNINFORMATIK at KIT

KiKIT – The Helmholtz Pilot Program Core-Informatics at KIT

Involved Fellows at KASTEL SRL

- Bernhard Beckert
- Hannes Hartenstein
- Anne Koziolek
- André Platzer
- Raffaela Mirandola
- Ralf Reussner
- Ina Schaefer
- Martina Zitterbart

Portrait

In the information age, computers are a key driver in all areas of research, technology, business, and society. Therefore, high-quality software, hardware, and AI models are necessary to maintain digital sovereignty and need provisional research. Currently, research on core informatics, i.e., research on fundamental methods of informatics that can be applied in various applications and domains, is a blind spot in the Helmholtz Association, which has informatics research but mainly weaved into their specific classical research area.

Through the Pilot Program Kerninformatik am KIT (KiKIT), research on core informatics is to become a focus of the Helmholtz Association. KiKIT focuses on the research of novel general methods in the fields of

- algorithm and software engineering,
- data analysis and machine learning, as well as
- hardware and network systems.

Moreover, KiKIT pursues the goal of providing stable research tools (research software, AI models, etc.) to accelerate other research activities within the Helmholtz Association as well as to support innovation in industry.

Currently, there are 26 PIs and 40 researchers in 36 projects working on topics like Sustainability, Correctness, Explainability, and Performance of Software and Hardware. They each follow the goal of strengthening Germany's sovereignty in informatics.

kikit.kit.edu

CYBER SEC ***|__
KIT GRADUATE SCHOOL

KIT Graduate School Cyber Security

Portrait

The KIT Graduate School Cyber Security has become an established presence at KASTEL Security Research Labs. In November 2023, Ulrike Zimmermann took over as the coordinator. The Graduate School has gained new members from different research fields and maintains a regular networking schedule, forming a close-knit interdisciplinary community of early career researchers. Regular, tailor-made workshops provide the members with additional qualifications and allow them to hone their presentation, visualization, and project management skills. A photography project conducted with Innovation and Relations Management (IRM) at KIT had participants visualize their dissertation topics in an abstract way. The beautiful results now adorn the first floor of the Informatics building and were on loan as exhibits at the 2024 Community Congress by StartUpSecure KASTEL. The latest workshops included voice training, with practical exercises for speaking in public; one of them was specifically tailored for women researchers.

cybersec.kcist.kit.edu

Milestones

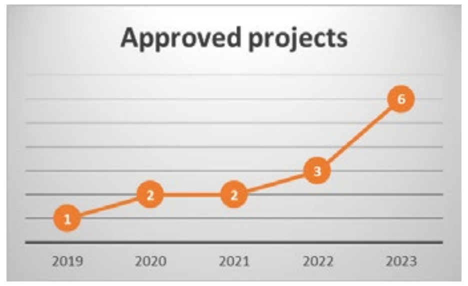
The "CyberSec Seminar" series and the "Security & Privacy Lunch" have gained significant traction. Following suggestions by the members, these two regular events now take place on separate dates instead of on the same day, providing even more opportunities to meet in an informal context. In 2023/24, members of the KIT Graduate School published six core A papers, including four at PETS (the most prestigious privacy venue) and four core A* papers, including two at IEEE S&P (the most competitive Security and Privacy conference).

startup secure
KASTEL

StartUpSecure KASTEL

Portrait

StartUpSecure KASTEL is the KIT incubator for start-ups in the field of IT security. The goal of the program is to provide continuous support for IT security start-up projects from all over Germany throughout their entire lifecycle. In particular, we focus on financial support, qualification measures, and raising awareness of cybersecurity issues in line with the needs of our network partners, potential pilot customers, and investors. In addition, we regularly organize events to strengthen the networking of our community and provide a stage for relevant topics and dedicated speakers.



Thanks to the extensive quality checks of the KASTEL Security Research Labs, almost all of our submitted projects have been approved by the German Federal Ministry of Education and Research (BMBF). Through a continuous series of consultations over the past three years and the successful cooperation with the KIT Graduate School Cyber Security, the project quality has improved significantly and the community is now stronger. The results can be seen in the number of funded projects.

The most notable annual event is the "Community Congress", held in 2024 on March 24, which centered on the intersection of AI and cybersecurity. With over 80 attendees, it stands out as one of the region's key gatherings. Mark your calendars for the next edition on April 10, 2025, focusing on "Mobility and Cyber Security".

www.startupsecure-kastel.de

Consultations per year	2019	2020	2021	2022	2023	1st half 2024
Initial consultation	10	14	11	22	14	4
Funding advice	1	6	13	4	5	3
Follow-up consultation		10	32	26	37	17

Milestones

In September 2023, a CyberSec Get-together took place in K26 at Kronenplatz, Karlsruhe, as a pre-program of the popular "116th Founders' Barbecue" of the KIT Founders Forge. With representatives of the incubators CISPA in Saarbrücken and ATHENE in Darmstadt, as well as many start-ups from the community and those interested in founding a company, the afternoon was all about elevator pitches, networking, and exchanging ideas. The event was such a success that it will now be held annually.

More about KASTEL Security Research Labs ...

... in our corporate video..

kastel-labs.de/about-kastel/

KASTEL Security Research Labs

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

KASTEL

Part I: Research &
Researchers