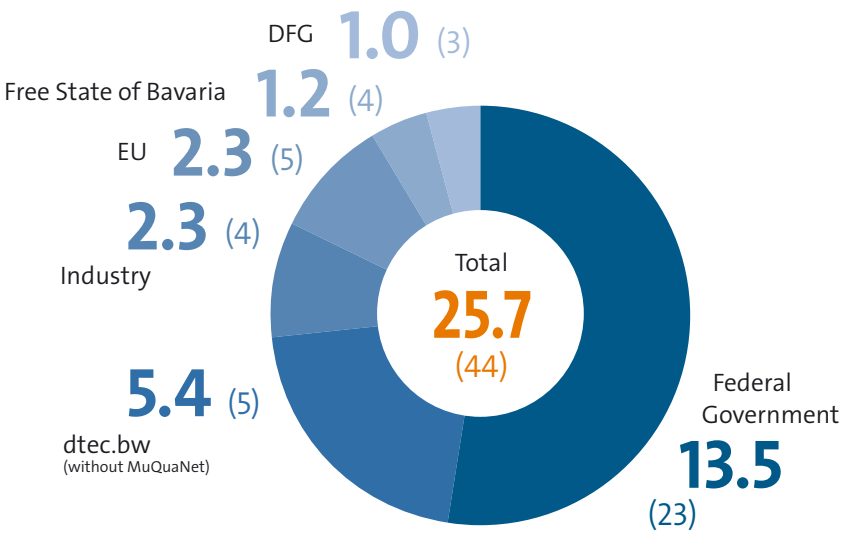

der Bundeswehr
Universität München
CODE
ANNUAL REPORT
2022
CODE RI
Research Institute
Cyber Defence
Universität der Bundeswehr München

Project Funding

In 2022, a total of 44 projects financed by third-party funds were either processed or acquired. dtec.bw projects receive funding from the budget of the BMVg division.

Third-party Funds*



* Numbers (rounded) in millions of euros, quantity of projects in parentheses.

dtec.bw Project**

MuQuaNet – The Munich Quantum Network

MuQuaNet
The Munich Quantum Network

Participating Professorships

Hon.-Prof. Dr. Udo Helmbrecht
Prof. Dr. Michaela Geierhos
Prof. Dr. Florian Alt
Prof. Dr. Arno Wacker

** With participation of RI CODE and project start in 2020; not included in the third-party funds overview (left).

Internationality

RI CODE maintains a large international network.

Employees***

In 2022, CODE employees came from 17 countries.

Cooperation Partners***

In 2022, RI CODE cooperated with 80 partners in 25 countries.

Legend

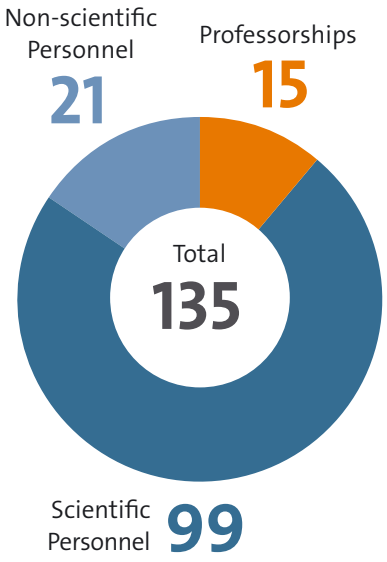
- Location of RI CODE
- 1 — Number of CODE employees from the Country of origin
- 1 — Number of international cooperation partners in the respective country
- Countries with cooperation partners and employees

*** More information about contacts and cooperation partners can be found from p. 82 onwards.

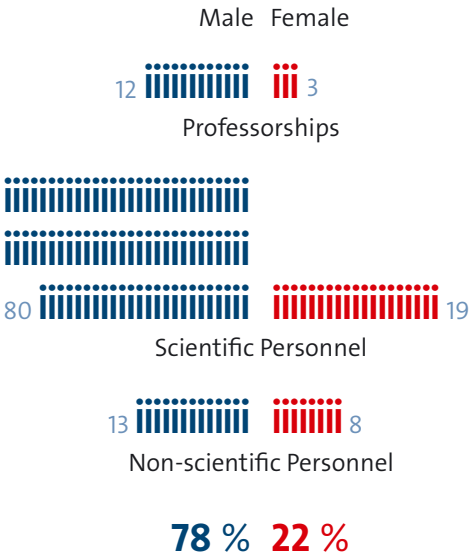
Staff Structure

**RI CODE had a total of 135 employees in 2022.
22 % percent of staff were women.**

Employees



Gender Share

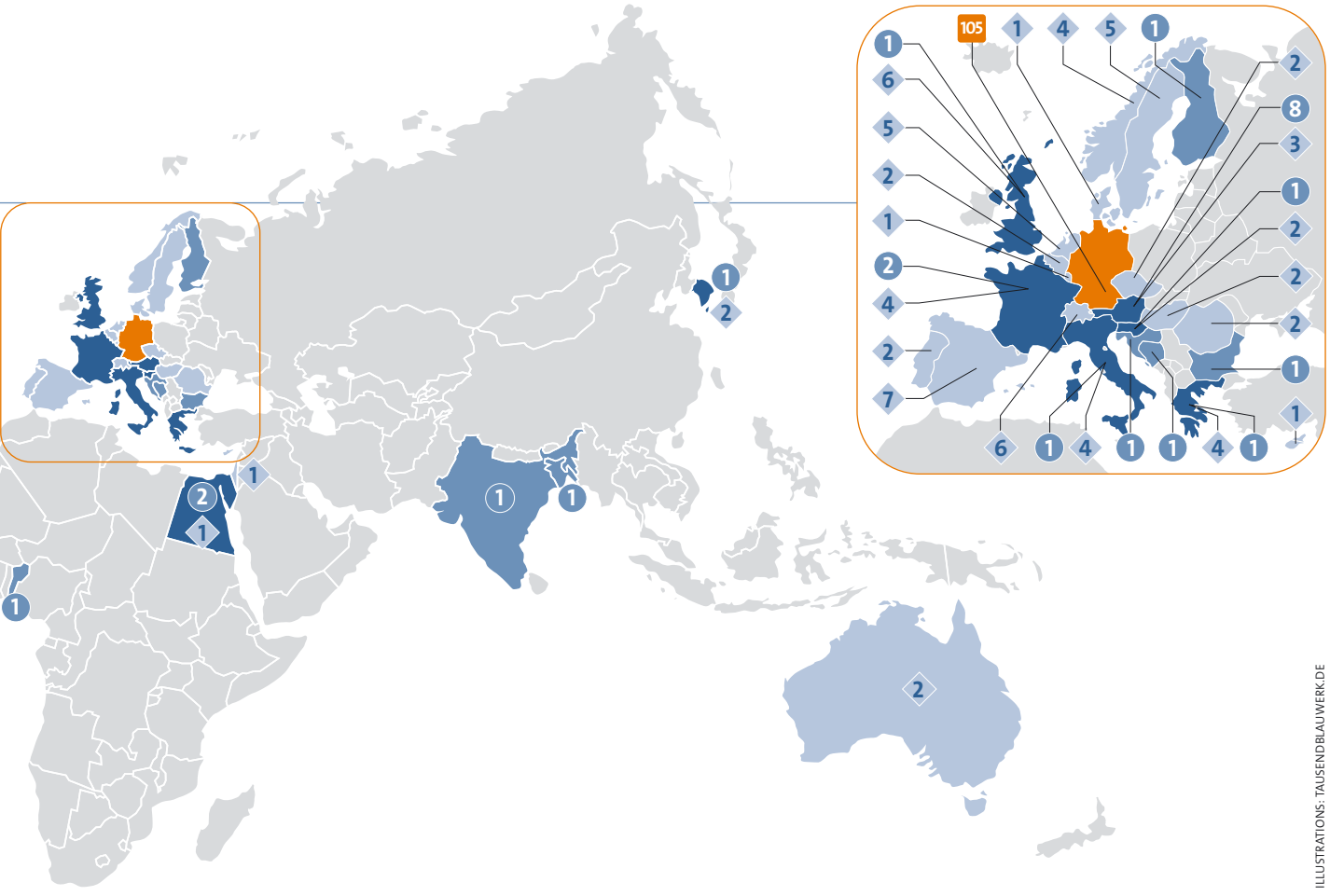


Research Work

Overview of doctorates and publications at RI CODE 2022

Doctorates

Publications



ILLUSTRATIONS: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
ANNUAL REPORT
2022

RI CODE
Research Institute
Cyber Defence
Universität der Bundeswehr München

Preface by the President

Given the major challenges posed by the global crises we face, protecting our critical infrastructures and IT systems is also becoming increasingly important. Business, politics, society, and the Bundeswehr (German Armed Forces) all depend on comprehensive, appropriate protective measures to avoid a breakdown of public life in the event of an emergency. We can be proud that science is making a decisive contribution here, as this Annual Report 2022 from our Research Institute Cyber Defence and Smart Data (RI CODE) shows.

The University of the Bundeswehr Munich recognized the hybrid threat scenario much earlier than other universities and developed a tailored profile with "Security and Sustainability in Technology and Society" to successfully address it.

It is important for me to emphasize that RI CODE has been doing valuable pioneering work and finding innovative solutions in this field since its foundation as a Research Center in 2013. On the occasion of the 10th anniversary of its foundation, I would like to warmly congratulate the institute's directors around Wolfgang Hommel and Michaela Geierhos as well as the entire team and wish them continued success! Ad multos annos! I am particularly happy that the CODE anniversary coincides with the 50th birthday of our university, founded in 1973, which we will celebrate with numerous exciting events.

Looking at the promising projects and highlights of RI CODE in the past year shows that the institute is excellently positioned. For example, the prestigious Google Faculty Award went to a CODE professorship for the first time. A new CODE chair (Prof. Ntoutsi) is involved in two Horizon Europe projects: STELAR and MAMMOth, both started in fall 2022. In addition, collaboration with the Bundeswehr has been intensified: Prof. Alt started a research project with WIWeB for the first time to explore military XR technologies from different perspectives. Civil security research was also expanded with a new joint project on artificial intelligence. In addition, CODE is participating in the BMBF lighthouse project 6G-Life (6G infrastructure in succession to 5G networks).

The importance of RI CODE is also reflected in the public perception by high-ranking visits from politics and the Bundeswehr. In December 2022, for example, the German Chief of Defence personally informed himself about the institute's work. As part of the "Locked Shields" exercise, the Bundeswehr's Deputy Chief of the Cyber and Information Domain Service and Chief Information Security Officer and a member of the German Bundestag visited RI CODE.

Also of importance is the expansion of international cooperation with our friendly partner countries, such as France and the USA. A delegation of the École de l'Air et de l'Espace, the academic cadre of the French Air Force, visited our university and RI CODE to further deepen the exchange in teaching and research.

I hope this brief insight into the diverse and exciting activities of RI CODE has piqued your interest in reading the current annual report. Enjoy it!

With best regards,

Prof. Dr. mont. Dr.-Ing. habil. Eva-Maria Kern, MBA
President University of the Bundeswehr Munich


Wolfgang Hommel, Marcus Knüpfer, Michaela Geierhos

Dear Readers,

Research, education, and training as well as active networking in the areas of Cyber Defence, Smart Data, and Quantum Technology are the three main areas of activity of RI CODE. In 2022, there were numerous activities in all three areas, into which this annual report provides exciting insights.

As a central scientific institution of the UniBw M and a departmental university research institute, we live from the teamwork of our research groups. We are therefore particularly pleased about the recruitment of Prof. Dr.-Ing. Mark Manulis in March and Prof. Dr. Eirini Ntoutsi in August 2022, who joined us as professors for Privacy and Open Source Intelligence, respectively, and have been actively building up their research groups ever since. A major part of this report, the chapter "Research", is accordingly dedicated to introducing our research groups and a selection of current research projects.

Besides the research-oriented content of our degree programs at the university, such as the Master Cyber Security (MCYB) and the specialization Cyber Defence in the Master of Intelligence and Security Studies (MISS), the Cyber Range of the RI CODE is also becoming an important instrument for the advanced training of IT security specialists and executives of the Bundeswehr. Thus, in 2022, the German contribution to the international cyber defence exercise Locked Shields and, for the first time, the exercise Cyber Phoenix for participants of the German and Dutch Cyber Reserve were conducted at RI CODE. Our annual Capture the Flag event, this year themed "The Spanning Tree – Catching B8tes", also achieved significant growth with 80 teams qualifying. See the "Highlights" section for more details.

The year 2022 also offered the opportunity to exchange ideas in person again after several years dominated by video conferences. In particular, the CODE Annual Conference 2022, under the motto "Data-Driven Innovation – Impulses for Secure Digitization", and the Cyber/IT Innovation Conference, hosted together with the BMVg CIT, could again be held in presence on the university campus. A summary can be found in this report, video recordings of numerous presentations are linked on our website.

The variety and multiplicity of our activities, however, would not be possible without comprehensive support from inside and outside the organization. The staff members in the CODE office and all research groups therefore deserve our thanks for their dedicated and tireless efforts. For their not only generous, but also especially active support, we would like to thank the Head of Department CIT, Lieutenant General Vetter, the Inspector CIDS, Vice Admiral Dr. Daum, all our direct contacts at the Federal Ministry of Defence and Command Center of CIDS, as well as the management of our university.

We hope you enjoy reading and look forward to celebrate CODE's 10th anniversary with you in 2023!

Prof. Dr. Wolfgang Hommel

Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Management of the Research Institute CODE

FIG.: XXXXXXXXXXXXXXX

Contents

ABB.: ADOBE STOCK / FERNANDO CORTÉS

Highlights
From the Institute

Research
Portraits and Projects

Further Projects

Cooperations
Germany and the World

Young Science
Offers and Opportunities

Addendum
Publications and Activities

Organizational Structure

Categories

OUR MISSION STATEMENT

FIG.: ADOBE STOCK / STNAZKUL

The Research Institute CODE is a central scientific institution of the University of the Bundeswehr Munich. We use our expertise for the benefit of society and the Bundeswehr and contribute to making Germany a bit safer through innovations in the field of cyber/IT.

Three key areas are the focus of our activities:

- **Research and technology development**
- **Knowledge transfer and consulting for decision-makers**
- **Education and training**

We conduct both basic and applied research as well as technology development in the fields of cyber defence, smart data, and quantum technology. Our work focuses on the concrete and perspective benefits for society and the Bundeswehr. Due to our close ties with the Bundeswehr's CIDS (Cyber and Information Domain Service) organizational unit, we are in a unique position to develop solutions for current and future challenges in the CIDS domain through research in a secure environment.

Our goal is to research technical innovations and concepts for the protection of data, software, and systems in a holistic and interdisciplinary manner. In particular, we emphasize the development of application-oriented technologies and the acceptance of secure technologies by society. To this end, we work closely with the Bundeswehr, government agencies, research institutions, and industry so that our partners can transfer new research findings and technologies into practice in a way that adds value.

We are open to scientific discourse and pursue long-term cooperations. With the broad competencies of our professorships and research groups, we provide advice to decision-makers from the Bundeswehr and politics and promote knowledge transfer. Our scientific advisory board actively supports RI CODE in its strategic development with its technical expertise.

We offer an optimal framework for education and training. Our IT infrastructure allows research and training at the highest level. In teaching, we prepare students at the University of the Bundeswehr Munich for the challenges of their professional lives and provide practical training for members of the Bundeswehr and Cyber Reserve in our modern Cyber Range. Direct access to quantum computers enables us today to find innovative solutions for the challenges of tomorrow.

We stand by our responsibility and role model function to work together with our partners and, above all, the Bundeswehr to protect a free democratic society. Every day, we are working to make a significant contribution to protecting against the dangers in cyber and information space, and we are prepared to be measured against this. ■

Highlights

From the Institute

FIG.: ADOBE STOCK / WETTE

Reservists from Germany and the Netherlands were training together during the Cyber Phoenix exercise.

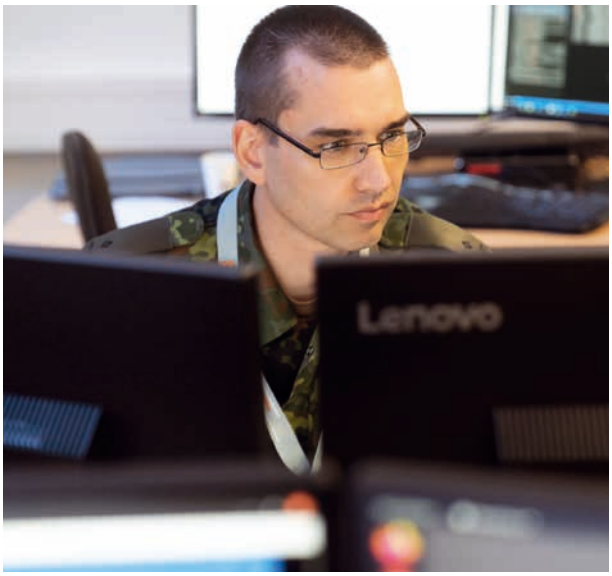
Cyber Phoenix Reserve Exercise at RI CODE

Defensive Training Against Cyber Attacks

From August 29 to September 2, 2022, the Cyber Phoenix exercise of the Cyber and Information Domain Service (CIDS) of the Bundeswehr took place at the Research Institute CODE. A total of 22 reservists from the Netherlands and Germany trained together to defend against hostile cyber attacks. During a visit, Major General Setzer and the Dutch Brigadier General van den Berg experienced the successful cooperation between their teams firsthand.

Refreshing, Building, and Exchanging Knowledge

The training rooms of RI CODE's Cyber Range ICE & T were bustling with activity. Almost all workstations were occupied and 22 uniformed reservists sat concentrated in front of two screens each. Refreshing and building knowledge, sharing ideas, and succeeding together was the goal of the collaborative cyber exercise such as Cyber Phoenix. In three individual exercises and two elaborate scenarios lasting several hours, the participants from the Netherlands and Germany had the opportunity over five days to put their skills to the test in order to be able to support the armed forces of the two countries quickly and reliably in an emergency. The multinationally mixed teams consisted of up to six members each, who attempted to protect network environments against cyber attacks within a mission in a fictitious scenario.



Besides IT forensics topics, complex cyber defence scenarios were also part of the exercise.

Individual Exercise Content and Direct Supervision

The content of the Cyber Phoenix exercise was created by the staff of the Cyber Range of RI CODE. During the first two days of the exercise, the main focus was on IT forensics in the areas of Windows, Linux, and Network. On Wednesday and Thursday, complex scenarios with extensive storylines were trained: For example, a fictional hospital had to be defended against a cyber attack or data theft via a smartphone had to be prevented. The CODE training team worked out most of the tasks from scratch for this exercise and adapted them to the needs of the reservists: "Our Cyber Range is fully

Major General Jürgen Setzer and exercise instructor August F. greeted additional reservists on Distinguished Visitors Day to inspect the exercise.

ALL FIG.: UNIBW M./ SIEBOLD

virtualized and flexible, which allows us to tailor our training very individually," said Marcus Knüpfer, acting managing director of RI CODE. The continuous and direct support provided by the trainers at the range also ensures a good learning effect for all participants.

High-ranking Military Representatives visit CODE

On the second to last day, Major General Setzer, Deputy Inspector in the Cyber and Information Domain Service, and his Dutch colleague Brigadier General van den Berg were also convinced of the well thought-out structure and up-to-date content of the exercise: During the "Distinguished Visitors Day", they took the opportunity to find out more about Cyber Phoenix and the RI CODE. During an exercise tour, the two generals, together with other guests – cyber reservists from all over Germany as well as military representatives from Peru - got to talk to the participants and were able to ask them about the trained content.

Feedback Round at the End

The exercise ended on Friday with a joint final round: What could the reservists take away from the intensive training week? What went well and, on the other hand, where is still room for improvement? A positive overall impression emerged from the various comments, in which the contribution of the RI CODE's trainer team was also praised in particular: "Thank you for the excellent mentoring and the well-designed content with up-to-date security gaps! Keep your passion for developing," said one of the participants. We definitely plan to do so: RI CODE intends to continue to expand its training program for Bundeswehr professionals and leaders and the Cyber Reserve. ■

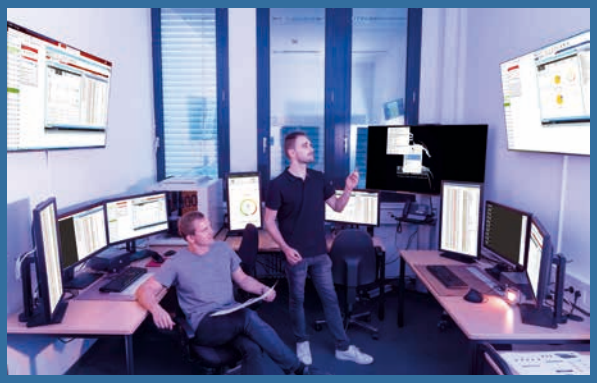
More about Cyber Phoenix

https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/aktuelles/cyber-phoenix-2022-5494904

Brigadier General René van den Berg (left, Commander of the Dutch Defensie Cyber Commando) and Major General Jürgen Setzer (Deputy Inspector CIDS).

ICE & T's classrooms are made for team training.

ICE & T Cyber Range at RI CODE



Our trainers monitor the team progress, manage scenarios, and enable a unique learning experience.

The Cyber Range IT Competence Education & Training (ICE & T) at the Research Institute CODE is a comprehensive and flexible solution for real-world cyber security training. It provides a platform for learning and deepening competencies in Cyber Network Operations with a strong focus on teamwork. ICE & T also enables the evaluation of new cyber security products and approaches.

During training, cyber security scenarios are processed in a virtualized environment. The scenarios currently available at ICE & T are grouped in the categories Cyber Incident & Response Management (CIRM) Level 0–2, Supervisory Control and Data Acquisition (SCADA), and Penetration Testing (PT). Participants learn to analyze and defend against various attack patterns or apply PT methods in real system networks.

ICE & T is fully virtualized on a server cluster using a VMware ESXi hypervisor. More than 400 virtual machines are used to enable multi-level scenarios as well as over 80 individual exercises and back-office services. The modular architecture also enables the integration of hardware components such as IoT and SCADA devices.

ICE T
IT Competence
Education & Training

Further Information

code@unibw.de

Information flyer
"Cyber Range":
https://go.unibw.de/84

ALL FIG.: UNIBW M / SIEBOLD

433-qubit Osprey processor with 3D architecture.

Quantum Technologies

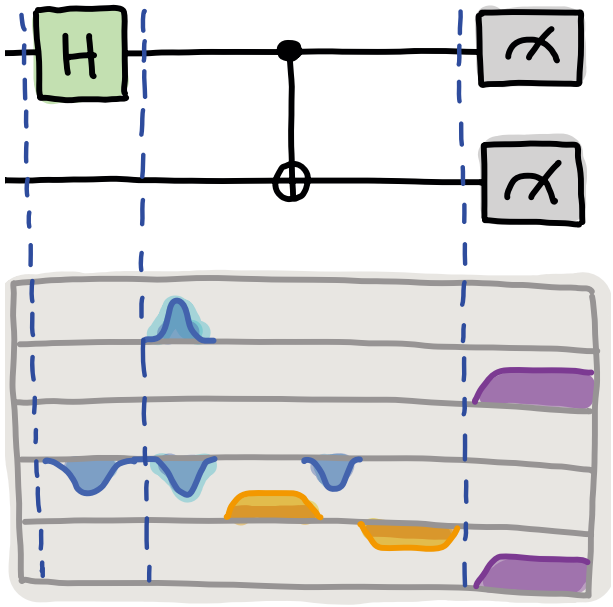
Quantum Information Processing with Quantum Computers

Experimental control of quantum systems enables the processing of quantum information, in particular by exploiting the quantum properties of superposition, interference, and entanglement. Applications of quantum technologies are expected in navigation, sensing, data transmission, and data processing. Because of the resulting potential impact on defence and security, NATO has designated quantum technology as one of its most important new breakthrough technologies.

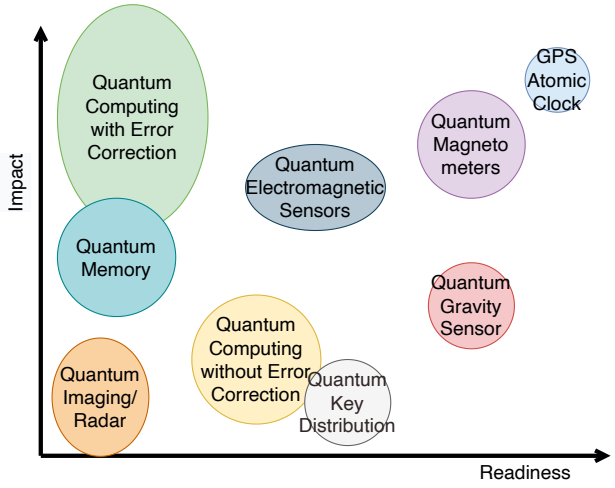
QUANTUM information processing forms the backbone of quantum technologies: Quantum data from quantum sensors can be processed and briefly cached in quantum memories. Quantum computers can be interconnected via quantum networks in distributed systems and linked to classical computers. Some of the quantum technologies are still at a very early stage and have a different readiness and impact.

As an IBM Quantum Hub, RI CODE at the University of the Bundeswehr Munich has had exclusive access to the IBM quantum computing infrastructure since 2018. The current availability of small noise quantum computers (up to 433 qubits) enables researchers to test quantum algorithms, heuristics, error correction, and error mitigation schemes, as well as perform experiments to explore and apply quantum information processing.

Research at RI CODE is concerned with algorithm development, application in quantum optimization, quantum machine learning, quantum simulation, and quantum walks, and implementation on the IBM quantum computers using circuit optimization and error mitigation techniques to be developed. The quantum computers are programmed using the software development kit Qiskit at the circuit, pulse, and algorithm levels, and corresponding experiments are performed.



Quantum information processing can be studied at the circuit level and pulse level on the IBM quantum computer.



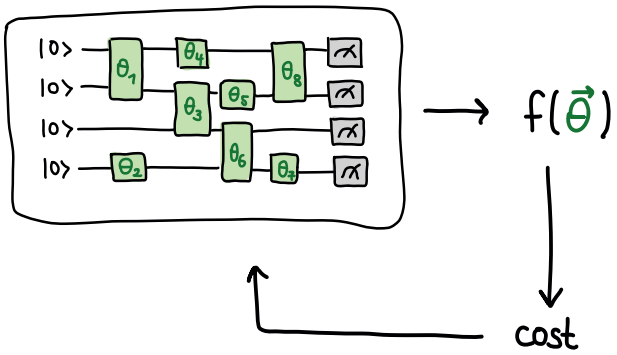
Quantum technologies.

FIG.: CONNIE ZHOU FOR IBM; RI CODE (2)

In parallel, the teaching program will be further expanded and lectures, lab courses, and workshops on quantum information processing are offered.

Quantum optimization

Many problems from logistics, supply chain management, or cryptanalysis can be transformed into an optimization task whose result is a state, a bit sequence or a distribution. For many of these problems, only



Visualization of a quantum variation algorithm circuit.

approximate solutions can be found using supercomputers.

Quantum variation algorithms enable a learning-based approach. The parameters of the circuit (gate or pulse parameters) are found by optimizing a cost function. Quantum variational algorithms are continuously improved in theory and experimental implementation. For example, it has been shown that quantum computers can approximate combinatorial optimization problems efficiently and with higher accuracy than classical computers. [1]

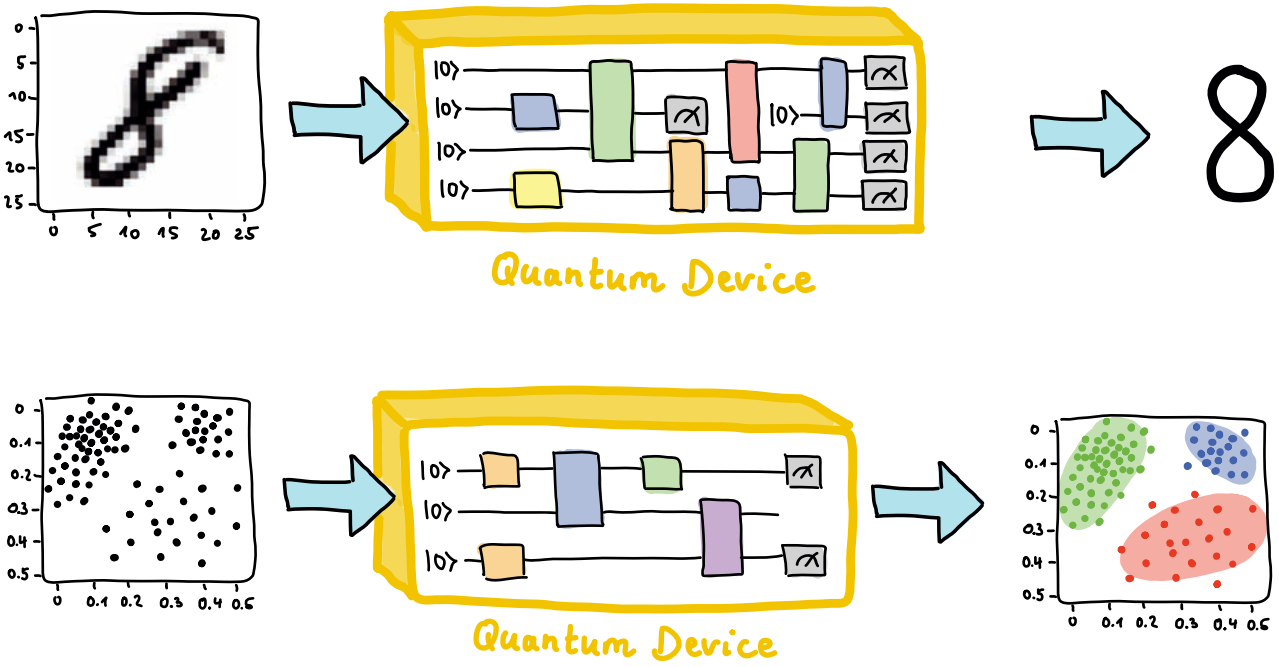
Quantum machine learning

Using quantum variational algorithms, quantum machine learning applications can be realized, both for classical data and quantum data from quantum sensors, for example.

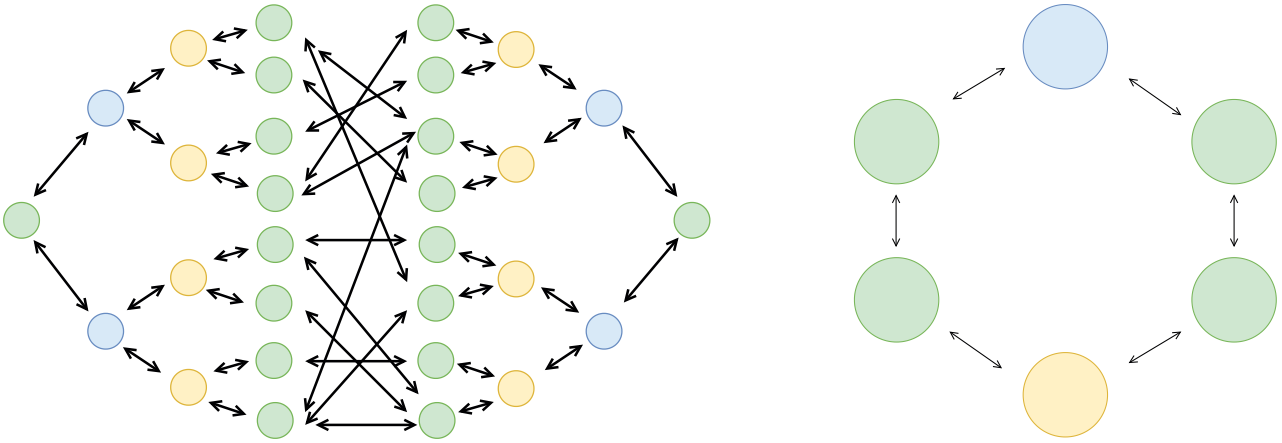
Specifically, these include quantum clustering, quantum Boltzmann machines, kernel methods, quantum convolutional neural networks, quantum support vector machines, quantum autoencoders, or generative adversarial quantum networks. Kernel machine learning methods are ubiquitous in pattern recognition, with "support vector machines" being the best-known method for classification problems, and can also be used as quantum algorithms.

The encoding of classical data into quantum states (quantum circuit) is called a quantum feature map. This feature map opens the possibility of integrating the advantages of quantum information processing into machine learning algorithms. It is expected that we can obtain a quantum advantage by choosing a quantum feature map, which is not easy to simulate with a classical computer. We investigate the predictive power of different combinations of quantum circuit architectures for the quantum feature maps. Finding a quantum advantage for real-world data classification is challenging, especially when dealing with heterogeneous data or large datasets that require more qubits than are available on current quantum computers. In our research, we are investigating quantum circuit architectures for data from multiple sources (data fusion), and the possibility of combining quantum chips to process larger data sets. [2]

Recently, an "exponential" advantage has been demonstrated in the field of quantum machine learning with quantum data. Instead of processing quantum data with a classical computer, one can transfer it to quan-



Visualization of supervised and unsupervised quantum machine learning.



Quantum walk on different geometries.

tum memory and have a quantum computer analyze it. One then needs exponentially less data to characterize the quantum state of the sensor compared to conventional processing. [3]

Quantum random walk

Quantum walks are a powerful technique for developing quantum algorithms and simulating complex quantum systems. They have become a universal computational model over the last decade and were originally developed as a quantum version of classical random walks, where the direction of the next step is determined by flipping a coin.

Random walks have applications in many fields, from biology to computer science to finance, and the same is true for quantum walks. The laws of quantum information state that the evolution of an isolated quantum system is deterministic. Randomness appears when the system is measured, and classical information is obtained. We investigate possible application to search and combinatorial optimization problems when quantum walks in different geometries, are affected by repeated stroboscopic measurements. [4]

Quantum simulation

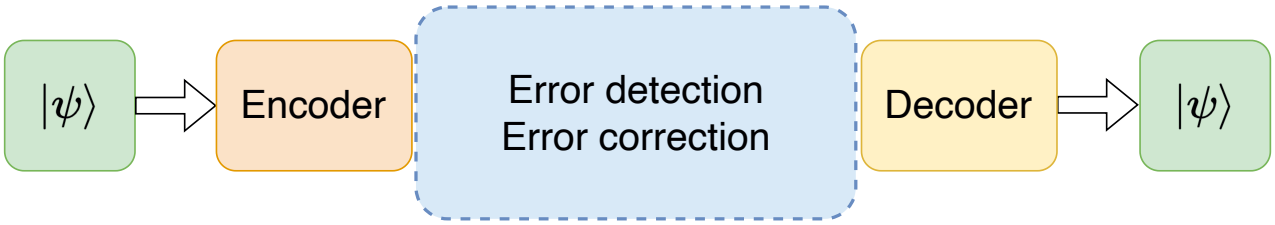
A universal quantum computer can emulate a quantum system by simulating its natural dynamics. Simulating these systems with classical computers is very difficult because the resources required grow exponentially with system size. However, quantum computers could overcome this hurdle and provide solutions in much shorter time.

Research at RI CODE has simulated quantum materials and open quantum systems on IBM quantum computers. This can be important for the development of energy storage materials, for example. [5]

Quantum natural language processing

Quantum computing methods can also be applied in computational linguistics, where they help to determine word embeddings. Here, words are represented by a vector in a real vector space, where words with similar meaning are mapped to vectors with a small distance.

Now pure quantum states correspond to rays in a complex Hilbert space whose scalar product leads naturally to such a distance function. Word embeddings can eventually be represented by parameterized quantum circuits whose parameters can be optimized using quantum machine learning. One application of this approach enables prediction of a word in a given context. These techniques are equally adaptable to NISQ devices. [6]



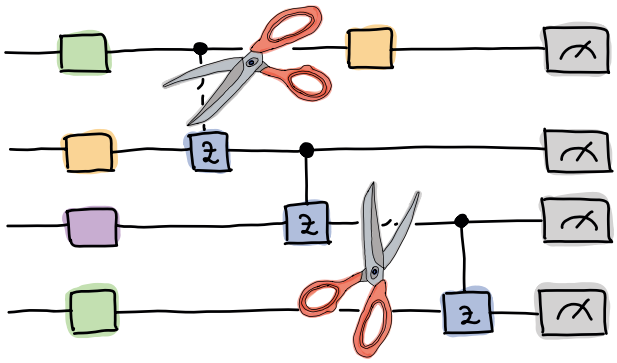
Quantum error correction.

ALL FIG.: RI CODE

Hardware implementation

To explore quantum information processing, various experiments are performed on a superconducting quantum computer, such as Entanglement Measurement, Tomography, Quantum Optimal Control, Calibration or Pulse-level Programming, Learning from Experiments, or Quantum Algorithmic Measurement. In addition, error mitigation techniques can be tested to reduce the hardware errors that occur when running quantum computing algorithms. Quantum error mitigation is related to quantum error correction and optimal quantum control – two research areas that also aim to reduce the impact of quantum information processing errors in quantum computers.

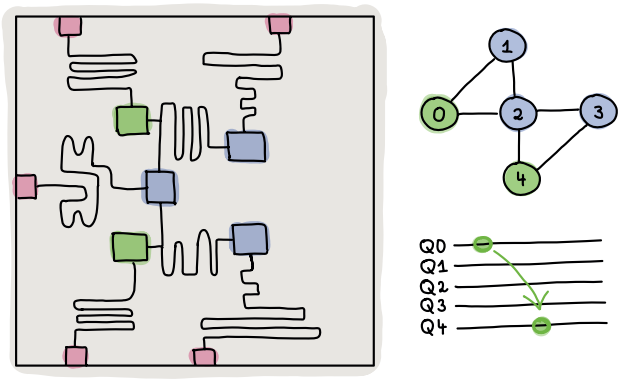
The quantum circuit model is an abstraction that hides the underlying physical implementation of gates and measurements on a quantum computer. Precise control of real quantum hardware requires the ability to execute instructions at the level of pulses and readouts. Qiskit Pulse can be used to explore advanced control schemes, such as optimal control theory and error



Quantum circuits are decomposed into smaller units by wire cutting and gate virtualization.

mitigation, which are not available in the circuit model by programming a quantum computer directly at the pulse level. Yet, the depth of quantum circuits that can be reliably executed on current quantum computers is limited by their noisy operations (i.e., perturbed by interaction with the environment) and the small number of qubits. Thus, scaling remains a current problem to be overcome. An intermediate solution is a scalable hybrid computational approach that combines classical computers and various quantum computers through distributed quantum computing. Quantum circuits are decomposed into smaller units so that they can be executed on smaller quantum chips.

Classical post-processing and controlled approximations can then be used to reconstruct the output of the original circuit. With this quantum classical approach,



Quantum teleportation experiment.

small quantum computers can run an algorithm that requires more qubits than available, and runtime and accuracy can be optimized until it is possible to apply quantum error correction.

Quantum computers in teaching

The topics from applied research were passed on to students and employees of service providers close to the Bundeswehr with the help of practice-oriented courses at Munich universities and through supervision of final theses. For example, students were able to perform experiments on quantum teleportation on the quantum computers. ■

1) CEREZO, M., ARRASMITH, A., BABBUSH, R. et al.: Variational quantum algorithms. Nat Rev Phys 3, pp. 625–644, 2021. https://doi.org/10.1038/s42254-021-00348-9.

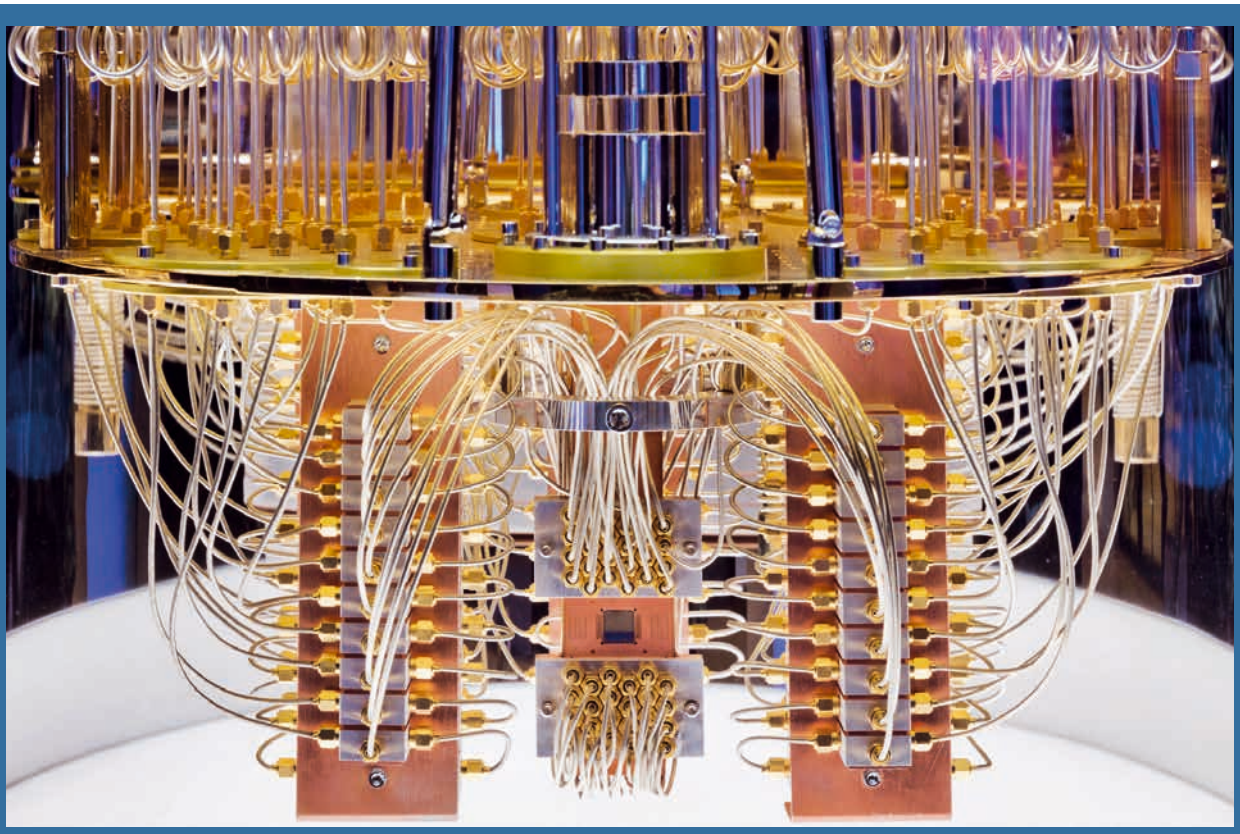
2) KUNCZIK, L., TORNOW, S.: Quantum Kernel Based Data Fusion. 2022 25th International Conference on Information Fusion (FUSION), pp. 1–7, 2022. doi: 10.23919/FUSION49751.2022.9841330.

3) CEREZO, M., VERDON, G., HUANG, HY. et al.: Challenges and opportunities in quantum machine learning. Nat Comput Sci 2, pp. 567–576, 2022. https://doi.org/10.1038/s43588-022-00311-3.

4) TORNOW, S., ZIEGLER, K.: Measurement induced quantum walks on an IBM Quantum Computer. arXiv preprint arXiv:2210.09941, 2022.

5) TORNOW, S., GEHRKE, W., HELMBRECHT, U.: Non-equilibrium dynamics of a dissipative two-site Hubbard model simulated on IBM quantum computers. Journal of Physics A: Mathematical and Theoretical 55 (24), 245302, 2022.

6) COECKE, B.: The Mathematics of Text Structure. arXiv:1904.03478.



Quantum Computing

QUANTUM COMPUTING is a new paradigm that enables exponential speed increases over classical computing for certain computational problems. The computing operations are performed with qubits. A qubit is the smallest unit of information in a quantum computer. It is a quantum mechanical two-state system that can be in a superposition state of 0 and 1. Superposition enables interference effects that are central to quantum algorithms.

Only when a measurement is made does the qubit enter one of the two states (0, 1). The measurement result can then be stored in a classical bit. With each additional qubit, the size of the state space available for a quantum algorithm doubles. This exponential scaling is the basis for the performance of quantum computers. Theoretical work has shown that – compared to the best known classical algorithms – certain structured problems can be computed exponentially faster with quantum algorithms.

Quantum computers promise enormous potential for efficiently solving some of the most difficult problems in the natural, economic, and computer sciences, such as factorization, optimization, and modeling of complex systems. These problems are intractable for any current or future classical computer.

Today, many practical computational problems employ heuristic algorithms whose effectiveness has been empirically demonstrated. Analogously, heuristic quantum algorithms have also been proposed. However, empirical testing is not possible until the appropriate quantum hardware is available.

With recent remarkable technological advances, it is now possible to test quantum algorithms and quantum heuristics on small quantum computers.

Contacts related to quantum computing at RI CODE

Dr. Sabine Tornow
sabine.tornow@unibw.de
+ 49 89 6004 7315

Dr. Wolfgang Gehrke
wolfgang.gehrke@unibw.de
+49 89 6004 7314

FIG.: RI CODE (2); IBM CORPORATION

Report on the CODE Annual Conference 2022

Digitization? Sure thing, but secure!

Security for a world that is increasingly becoming digital: On July 12 and 13, under the motto "Data-driven innovation – Impulses for secure digitization," the annual conference of the Research Institute Cyber Defence and Smart Data (RI CODE) at the University of the Bundeswehr Munich focused on the challenges of the future.

THE FACT THAT digitization is no longer just a buzzword can be seen by the developments of recent years: Since the pandemic, digital solutions have become part of the everyday (working) lives of billions of people around the world. Video conferences, virtual courses with connected devices, and voice-based assistance systems have become normal within a short period of time. But how secure are these services, which are having an increasingly large impact on our lives and work? And what should be considered in light of the rapid future developments?

Between Opportunities and Risks

The CODE Annual Conference 2022, held July 12–13 on the campus of the University of the Bundeswehr Munich, was dedicated to the major issues of digitization, focusing in particular on cyber security, artificial intelligence, and innovation.

The first day of the event started in the morning with a welcome speech by the President of the University of the Bundeswehr Munich, Prof. Dr. Merith Niehuss. Then a video message from the Federal Minister of Defence, Christine Lambrecht, followed. In her speech, the minister emphasized, among other things, the relevance of research in the field of cyber security. The "Zeitenwende" (changing times) in security policy as a result of the Ukraine war poses new challenges for society and increases the pressure on digital progress, she said. In particular, capabilities in the field of cyber defence play a key role in this

Discussing the topic "Regulation of AI and Cyber Security – Digital Boom or Missed Opportunity?" (f. l. t. r.): Lina Rusch (moderation), Lt. Gen. Michael Vetter, Wilfried Karl, Benjamin Brake, Prof. Patrick Glauner, and Dr. Arndt von Twickel.

BOTH FIG.: RI CODE / A. WAGENER FOTOGRAFIE

context. Lambrecht emphasized: "Cyber defence extends far beyond the Bundeswehr and deep into our society. Therefore, it is even more important that the Research Institute CODE has for years been dealing with the pressing issues of digital change and now also the 'Zeitenwende'."

After a presentation of current developments at the Research Institute CODE by Executive Director Prof. Dr. Wolfgang Hommel, a number of high-level representatives from various federal ministries and departments gave keynote speeches on the first day of the event – including Lieutenant General Michael Vetter (BMVg), Benjamin Brake (BMDV), and Wilfried Karl (ZITiS). Two controversial panel discussions facilitated lively debates in the area of tension between the potential and risks of digitization. The first panel, moderated by Lina Rusch (Editorial Director Tagesspiegel, Background Digitization and AI), dealt with the topic "Regulation of AI and Cyber Security – Digital Boom or Missed Opportunity?". The second panel discussion in the afternoon, titled "Data Protection vs. Data Treasure," raised the question of who can and may benefit from big data and for which issues. Marc Akkermann (Infodas GmbH) led the panel.

Transfer of Research Results into Practice

In addition, CODE professors Florian Alt and Johannes Kinder presented their current work, thus paving the way for the transfer of current research results into practice. In his presentation on "Usable Security for Smart Environments," Prof. Alt pointed out the problem that in many cases human behavior is the cause of damages due to cybercrime. In the approach he presented, sensors are used to capture human behavior and physiological states in real time and develop better security mechanisms based on this. Afterwards, Prof. Kinder addressed the topic of "Security for Modern Software Systems" in his presentation. Although overall security awareness among software and system manufacturers has increased significantly in recent years, the continuously increasing complexity of modern software systems continues to offer new types of vulnerabilities for attackers, said the professor for Computer Systems Hardening. His research group at RI CODE therefore investigates both software and malware at all levels – from JavaScript to machine code and CPU architecture effects – using techniques of formal program analysis as well as machine learning, among others.

In addition to the exchange between science, industry, politics, authorities and the Bundeswehr, the CODE annual conference also focuses on knowledge transfer.

Lieutenant General Michael Vetter (Head of the Cyber- and Information Technology Department (CIT) and Chief Information Officer (CIO) at the Federal Ministry of Defence (BMVg) and Major General Jürgen Setzer (Deputy Inspector CIDS, and CISO of the Bundeswehr) during the session.

The first day of the event ended with a social event in the UniCasino. Enjoying the perfect weather and cool drinks, the participants of the annual conference took the opportunity for further exchange and networking.

The second day of the event on July 13 began with a welcome speech by RI CODE's Technical Director, Prof. Dr. Michaela Geierhos, and a keynote by Prof. Dr. Christian Hummert, Research Director of the Agentur für Innovation in der Cybersicherheit (Agency for Innovation in Cyber Security). In his presentation, Prof. Hummert pointed out the need for consistent trend monitoring: "If a topic is at the market research provider Gartner, it's too late for us." The rest of the morning was also devoted to a more in-depth look at important topics of the future: A total of six highly versatile workshops focused on topics such as quantum technologies, Europe's role in cybersecurity research, and digitization in healthcare.

Workshop: Development of Quantum Technologies

The "Quantum Technologies" workshop addressed the current state of the art of various quantum technologies. The development of quantum technology, such as quantum sensors, quantum imaging, quantum memories, or quantum computers, is progressing at a fast pace and is massively funded by both national initiatives and industry. During the pandemic, national funding efforts, e.g., for the construction of quantum computers, were even further enhanced. Applications have also been discussed extensively from both industrial and academic perspectives. These include, for example, earth observation, medical diagnostics, communications technology, materials development, quantum optimization, and machine learning.

Workshop: Opportunities for Cybersecurity Research

The workshop "Opportunities for Cybersecurity Research Within the Framework of the EU Funding Programs 'Horizon Europe' and 'Digital Europe'"presented the National Coordination Center for Cybersecurity in Industry, Technology and Research (NCC) with its plans for establishing a national cybersecurity community as well as the EU funding opportunities in the field of cyber security and the application processes required for this. Especially with regard to the presented EU fund-

FIG.: RI CODE / A. WAGENER FOTOGRAFIE (2)

ing opportunities, the current trends in cybersecurity research were discussed by the participants. Among other things, the focus was on questions regarding current challenges and future risks.

Workshop: Digitization in the Healthcare Sector

Stress prevention is a significant factor in ensuring the operational capability of military and civilian forces. The goal of the Smart Health Lab is to implement stress prevention and performance enhancement in the context of mission preparation and prevention with the help of an interdisciplinary project (computer science, psychology, sports science) and the use of Extended Reality (XR) technologies.

In addition to basic research, application-oriented research will also be conducted and all relevant influencing factors of the infrastructure, as well as physiological and psychological parameters will be researched both individually and in terms of a system of interacting conditions. For this purpose, Data Science and Artificial Intelligence techniques are used to process the physiological data collected by means of various sensor systems. Findings from the project provide important information and implementation recommendations for digitized, individualized stress training to prepare soldiers for deployment. The workshop used practical examples to introduce the topic and presented current challenges, research questions, and approaches to solutions.

Innovation Conference

The workshops were followed in the afternoon by the Cyber and Information Technology Innovation Conference hosted by the Bundeswehr. With the help of the Cyber and Information Technology Innovation Conference, the Bundeswehr intends to take a holistic approach to the cyber/IT innovation dialog and to the demand-driven identification and introduction of IT innovations in the business area of the Federal Ministry of Defence.

From the numerous submissions on the relevant topics of cyber security, communications, geoinformation, and information processing, a jury had selected six innovative ideas in advance, each of which was presented to the expert audience in a seven-minute short

First Lieutenant Marc A. Wietfeld and his team (ARX Landsysteme & Hensoldt Venture/Sensors GmbH) were delighted to win first place at the 2022 Innovation Conference.

Numerous visitors attended the social event at the UniCasino on Tuesday evening for further networking and exchanging ideas.

presentation. The prizes for which participants from universities, start-ups, companies, and associations competed, had a total value of €39,000.

After the six creative pitch presentations, the conference guests had the opportunity to discuss with the presenters. Afterwards, Lieutenant General Michael Vetter awarded the winners: First place went to First Lieutenant Marc A. Wietfeld and his team (ARX Landsysteme & Hensoldt Venture/Sensors GmbH), who developed "Bird's Nest," an AI-supported system for fire support of the Bundeswehr on the battlefield. Second place (João Schneider, University of Würzburg, and Lennard Rose, University of Applied Sciences Würzburg-Schweinfurt) and third place (Kai Rehnelt, SECLOUS GmbH) were also aimed at concrete application possibilities in the Bundeswehr. For example, a machine learning model for the classification of water vehicles based on acoustic signals and a highly secure infrastructure for the efficient collaboration of alliance partners were awarded prizes.

Aim of the CODE Annual Conference: Exchange and transfer of knowledge

The Annual Conference of RI CODE is intended to promote interdisciplinary networking and exchange between science, industry, politics, authorities and the Bundeswehr – a claim that was once again met by the program and guests this year. Speakers and panelists from industry, government agencies, and organizations provided a variety of perspectives on issues related to digitization. The newly established area of quantum technologies at RI CODE and the cooperation with IBM also found their place in the program. The accompanying trade fair offered additional opportunities for exchange, information, and networking. ■

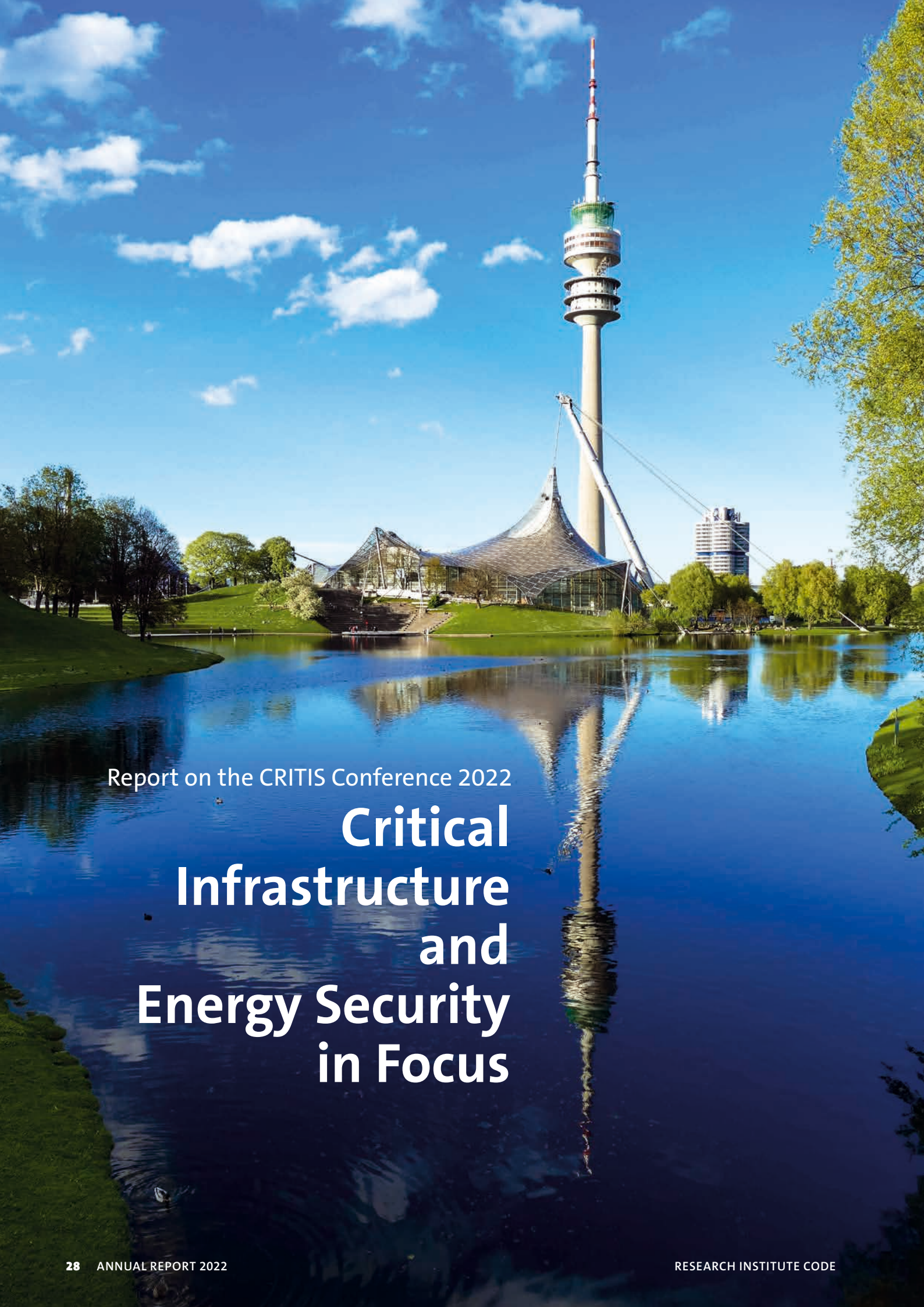
More information about the CODE Annual Conference

www.unibw.de/code/events/jahrestagungen

www.youtube.com/c/FzcodeDeubw

code@unibw.de

FIG.: RI CODE / D. PÖHN; RI CODE / A. WAGENER FOTOGRAFIE



Report on the CRITIS Conference 2022

Critical Infrastructure and Energy Security in Focus

The 2022 International Conference on Critical Information Infrastructures Security (CRITIS) was held at the campus of the University of the Bundeswehr Munich (UniBw M). The three-day event was organized by the research group COMTESSA (Core Competence Center for Operations Research, Management Intelligence Tenacity Excellence, Safety & Security ALLIANCE) under the direction of Prof. Dr. Stefan Pickl (Professorship of Operations Research) and in close cooperation with the Research Institute CODE (Cyber Defence and Smart Data).

MORE THAN 100 PARTICIPANTS from science, industry, politics, authorities and, especially operators of critical infrastructures were welcomed by Prof. Stefan Pickl and the chairman of the CRITIS steering committee, Prof. Bernhard Hämmerli (Lucerne University of Applied Sciences and Arts) in mid-September. The conference addressed the three central scientific domains of information, infrastructures, and security specifically in the context of Operations Research (OR)-based analyses and complex data-based optimization methods. Prof. Bernhard Hämmerli thanked the Honorary Chair, Prof. Dr. Udo Helmbrecht, and RI CODE in particular for the excellent cooperation in this important field.

Major General (ret.) Dr. Dr. Dieter Budde, Prof. Bernhard Hämmerli, Dr. Päivi Mattila, Christian Després, Prof. Stefan Pickl (f. l. t. r.).

FIG.: PIXABAY / H.HUMMEL; UNIBW M

Christian Després (l.) and Stefan Pickl presented the SANCTUM project and the international consortium: SANCTUM is a future crisis center that also integrates reachback services.

In the context of the conference, the central topics were examined from different sides, both scientifically and practically, under the aspect of criticality. The conference was led by the competence center COMTESSA, which was developed by the Professorship of Operations Research at UniBw M. It deals with the analysis and simulation of complex systems as well as the development of optimization methods for IT-based decision support.

Hybrid Threats – International Cooperation in the EU-HYBNET

Moderated by Major General (ret.) Dr. Dr. Dieter Budde (COMTESSA), the event opened with two impressive keynotes. Dr. Päivi Mattila, coordinator of the EU-HYBNET project, addressed the current political situation in her presentation on hybrid threats in the area of critical infrastructure.

This situation is currently strongly influenced by Russia's war against the Ukraine and the resulting energy crisis in Europe. Mattila emphasized the importance of energy scenarios, strategic autonomy, OR-based procedures for pipeline protection, and special data analyses (indicator-based ad hoc analyses). Some of these scenarios are being developed in close cooperation with the Research Institute CODE as well, she said.

SANCTUM – Intelligent Crisis Management

In his keynote, Christian Després from the French Ministry of Equipment, Transport, Ecology, and Housing explained the complex issues of IT-based decision support. Christian Després coordinates the international SANCTUM project, which specifically aims to improve the effectiveness of crisis management at the government level. He demonstrated how SANCTUM's pioneering methodology can optimize strategic decision-making in particular.

Plenary Lectures

In the plenary lectures, representatives from the USA, Australia, and Asia presented current scenarios and forward-looking real-time analysis platforms. In view of the current crisis, the platforms are highly important in areas such as maritime security, to mention just one example. Monica Cardarilli from the Joint Research Center (JRC) of the EU presented a "Water Security Plan" for the protection of drinking water systems. Katharina Ross (Fraunhofer Institute EMI) presented the EU project Safety4Rail in her plenary lecture.

Munich's Chief Economic Advisor and Oktoberfest CEO Clemens Baumgärtner (l.) welcomed the guests at the reception in the Munich's City Hall.

The plenary lectures by Bernhard Tellenbach (Cyberdefence Campus EPFL) and Maximilian Moll covered the topics "Complex Cyber Defence" and "Prescriptive An-

Virtual Reality demonstration during the Bits & Pretzels session.

alytics" for better protection of critical infrastructures. Horia Nicolai Teodorescu gave an overview lecture on so-called power-side channel attacks.

In addition, a NATO workshop on energy security and a hybrid meeting of the EU expert group "Hybrid Threats" took place embedded in the conference.

Festive Highlight at BMW Welt

The social highlight of the event was the conference dinner at BMW Welt Munich, located across the street from the Olympic site. In his dinner speech, Major General (ret.) Dr. Dr. Dieter Budde, who as a young officer was responsible for special protective measures at the site during the 1972 Olympic assassination, reflected on the importance and handling of critical infrastructures: "After five days of being carefree, the world changed abruptly back then ..."

Clemens Baumgärtner, Officer of the Department of Economic and Labor Affairs of the City of Munich, also referred to the Olympic attack 50 years ago in his speech at the welcoming of the conference participants in the Munich City Hall: "At that time, the attack led to a complete rethinking of security concepts. Perhaps that is why Munich is one of the safest cities in the world today." For him, conferences such as CRITIS help "to keep improving these concepts."

Bits & Pretzels – Young Scientist Awards – Real-time Analysis

On the last of the three conference days, the "Bits & Pretzels" session took place – a technical forum in which three Young Scientist Awards were also presented. Prof. Pickl concluded by thanking all participants as well as the sponsors and, last but not least, the University of the Bundeswehr Munich. ■

More information on CRITIS

https://critis2022.comtessa.org/welcome

stefan.pickl@unibw.de

ALL FIG.: UNIBW M

FIG.: ADOBE STOCK / YOUR123

Research

Portraits and Projects

Research at RI CODE

Currently, there are 44 third-party funded projects being carried out in various research groups at the Research Institute CODE. A selection of these projects is described on the following pages. CODE conducts research in three overarching business areas: Cyber Defence, Smart Data, and Quantum Technology.

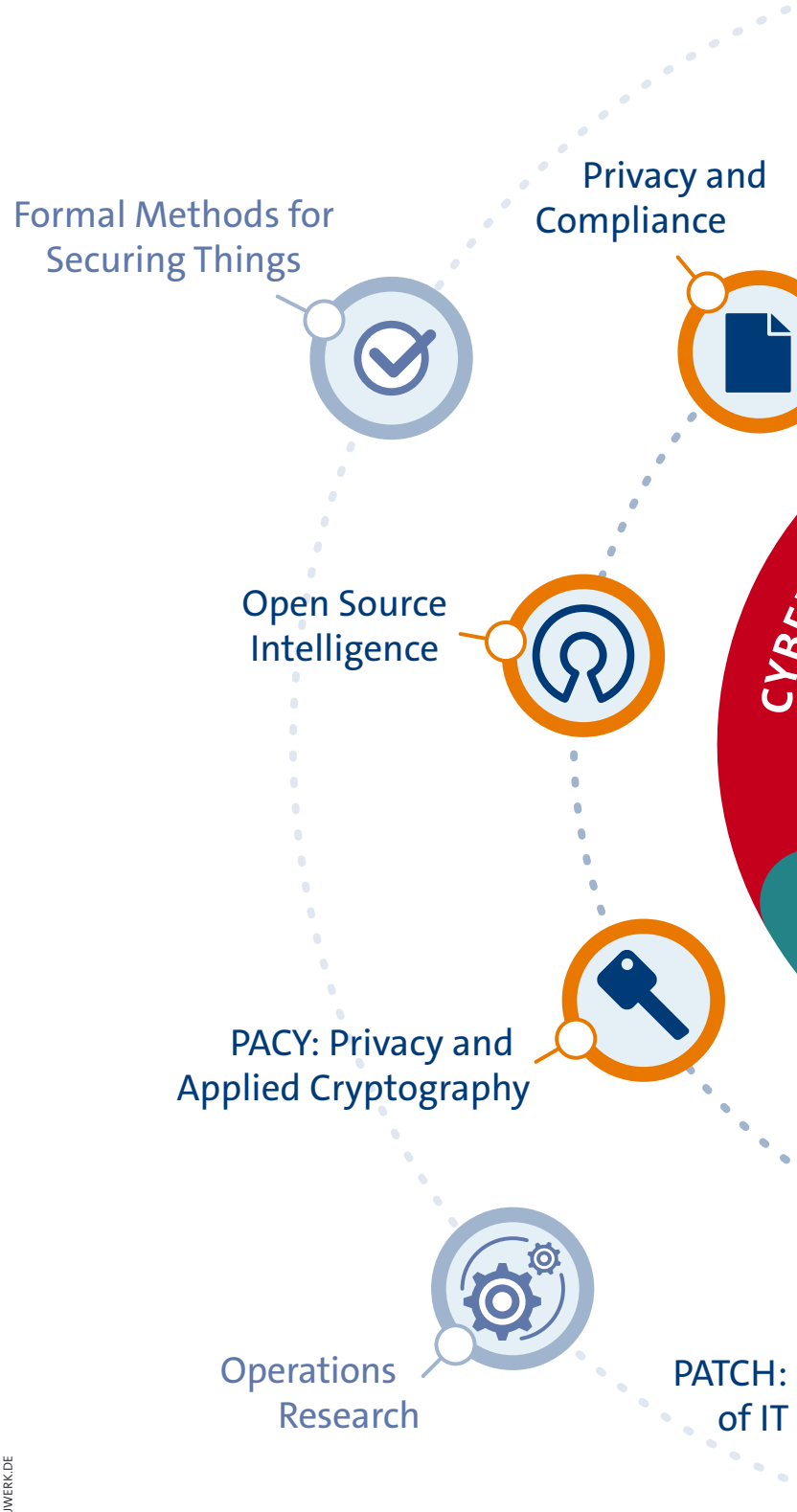
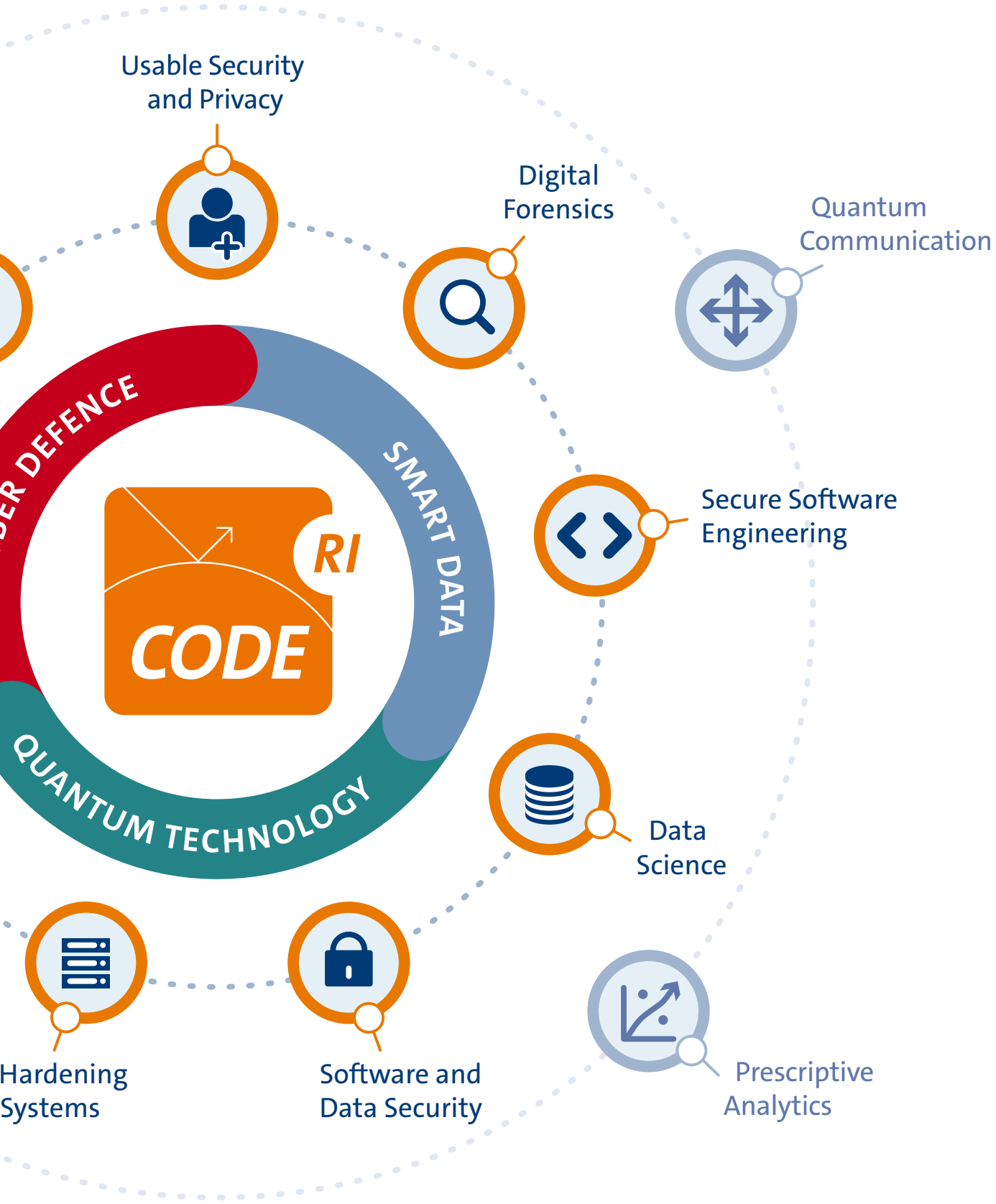


FIG.: TAUSENDBLAUWERK.DE


Usable Security and Privacy
Digital Forensics
Quantum Communication
ER DEFENCE
SMART DATA
RI
CODE
QUANTUM TECHNOLOGY
Secure Software Engineering
Data Science
Hardening Systems
Software and Data Security
Prescriptive Analytics

Prof. Dr. Florian Alt

Research Group Usable Security and Privacy

The Research Group Usable Security and Privacy, headed by Prof. Dr. Florian Alt, explores human behavior in security-related systems. In particular, the group looks into the role of security and privacy in user-centered design processes and investigates how secure systems can be better adapted to the way in which users interact with computing devices.

THE PROFESSORSHIP OF Usable Security and Privacy was founded in 2018 and conducts research at the crossroads of Human-Computer Interaction, IT Security, and Privacy. With his team, Prof. Dr. Florian Alt investigates how researchers and practitioners can be supported in considering security and privacy needs already during user-centered design processes. The ultimate goal is to better blend security and privacy mechanisms with the way in which users interact with technology in everyday life.

Research Areas and Methodology

The research group focuses on a variety of different research topics. These include the study of human behavior and physiological responses in security-critical situations, the development of new as well as the improvement of existing security and privacy mechanisms based on human behavior and physiology (especially gaze), the study of novel threats posed by ubiquitous technologies and the development of appropriate protection mechanisms, and the exploration of approaches to improve the understanding and behavior of users in security-critical situations. Specific application areas include smart home environments, social engineering, social biometrics, and mixed reality.

As part of its research, the group draws on research methods that are commonly known from human-computer interaction and continues to evolve them. These methods include user-centered design and iterative prototyping. The work has a strong human-centered focus, which makes empirical approaches a fundamental part of the group's research. To understand behavior and evaluate new approaches, studies are conducted both in the lab and in the field.

Infrastructure and Publications

The group has access to a human-computer interaction lab, equipped with a state-of-the-art indoor positioning system, stationary and mobile high-end eye trackers as well as other physiological sensors, thermal cameras, and augmented as well as virtual reality devices. In addition, the group is currently setting up a testbed, allowing users' behavior and physiological responses to security incidents to be investigated in the real world.

Together with his team, Prof. Dr. Florian Alt has published over 260 DBLP-listed scientific articles and won more than 15 awards in leading scientific venues of his field. The research of the group received funding from the German Science Foundation (DFG), the Digitalization and Technology Research Center of the Bundeswehr (dtec.bw), the Federal Ministry of Defence (BMVg), the Bavarian State Ministry for Education and Science, the Humboldt Foundation, the DAAD, Google, and the BMW Group.

Development of the Research Group in 2022

The research group Usable Security and Privacy has grown in 2022 and currently includes 16 employees and six research assistants besides Prof. Dr. Florian Alt. Among the research group's scientific staff are nine PhD students and six postdocs, who contributed to more than 35 publications in 2022. Three doctoral students successfully completed their PhD in 2022.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

www.unibw.de/usable-security-and-privacy

The research group for Usable Security and Privacy deals with topics of human-computer interaction, IT security, and privacy. Besides Prof. Dr. Florian Alt, it currently consists of 16 employees and six research assistants.

FIG.: ISTOCK / PHOTOTECHNO; ANGELIKA WAGENER FOTOGRAFIE / RI CODE

Project Gaze-aware Security Mechanisms

Identifying Password Reuse from Gaze and Typing Behavior

Users today must remember too many complex passwords. As a result, they develop strategies, many of which compromise security (e.g., using simple passwords or writing them down). One particularly problematic strategy is password reuse. If such a password is cracked, attackers gain direct access to all accounts protected with that password. In this project, we show how password reuse can be detected by gaze and typing behavior, with the goal of motivating users to use strong, unique passwords.

Using Physiological Data to Detect Password Reuse

Password reuse is a well-known phenomenon. Particularly problematic here is that users do not change their password even when it has been proven to have been cracked (studies show that within three months of a data leak becoming known, only 13 % of users change their password).

Thus, the goal is to prevent users from reusing a password as early as in the password creation stage. In this project, we show that by analyzing gaze data as well as typing data from the keyboard, it is possible to predict the reuse of a password already during registration. Machine learning methods are used to detect a user creating a new password or using an old one - without knowing the actual password.

Gaze is More Informative than Typing

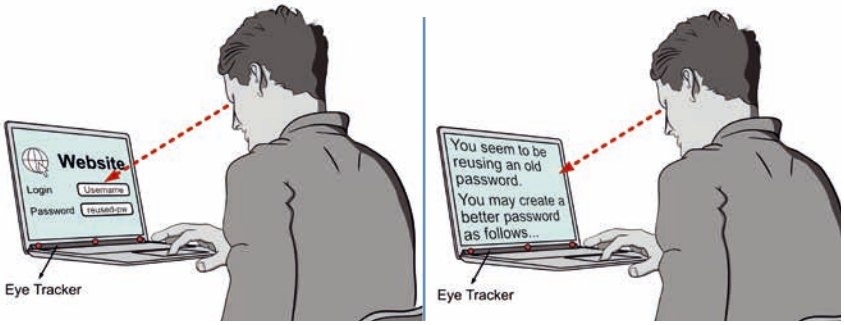
Our results show that typing behavior provides clues to password reuse. In particular, users type significantly faster when reusing. Recognition accuracy can be further increased by gaze data. The reason is that the cognitive load associated with thinking up a new password is reflected in gaze behavior (especially pupil dilation). It is also interesting to note that gaze data allow prediction before the actual input of a password, since the cognitive process already starts when the registration page is opened.

Data Sensitivity Influences Accuracy of Password Reuse Prediction

Our study participants more often reused passwords for a website with less sensitive data (e.g., a user account for a newspaper) than for sensitive data (e.g., email). Thus, the more sensitive the data to be protected, the more effort users put into their passwords and the less frequently they are reused. This also affects prediction accuracy: With sensitive data, more accurate prediction of password reuse is possible.

Nudging Users to Create Unique Passwords

Our system can serve as the basis for interventions that educate or help users create a better, unique password. By using gaze behavior, password reuse can be detected immediately and, in many cases, even before the password is entered. This can increase the likelihood that users will follow recommendations not to reuse passwords, compared to approaches that point out password reuse after the registration process has been completed.



We infer whether a user creates a new password or reuses an old one from behavioral data only, without the need to know the actual password. In particular, we analyze eye movement and keystroke data while a user creates a password.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

https://go.unibw.de/physiological-security-en

Funded by:

dtec.bw

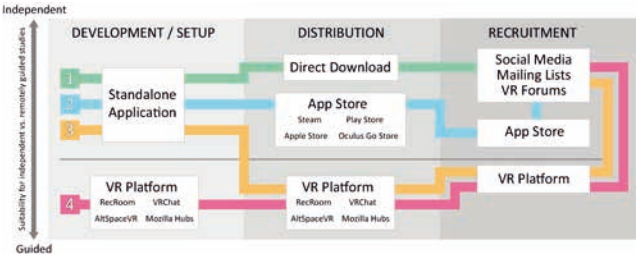
Funded by the European Union
NextGenerationEU

FIG.: CHRISTIAN GESSNER / RI CODE

Project Remote VR Studies

A Framework for Running Virtual Reality Studies Remotely via Participant-owned HMDs

Virtual reality (VR) headsets are increasingly used in research to complement or even replace established methods, especially for use cases that may put users at risk (e.g., automotive user interfaces, military use cases). Moreover, the increasing popularity of VR devices among consumers now offers researchers the opportunity to move VR research from laboratories to users' homes, thus reaching heterogeneous audiences.



Framework for conducting remote VR studies.

VR Research in People's Homes

This project explores challenges and opportunities of research conducted outside of laboratory settings with VR headset owners. The outcome of the project is a framework that sketches different ways in which appropriate studies can be technically implemented, how study applications can be distributed to participants, and through which channels they can be recruited to participate.

Understanding VR Users Through an Online Survey

Based on an online survey, we first studied the target audience to better understand their knowledge, motivations, and VR environments. VR users are often male gamers who, in addition to gaming, use VR as social platforms and for meeting friends and family. A clear majority of participants show interest and willingness to participate in remote VR studies. However, VR environments tend to be heterogeneous in terms of technologies used and spatial setup.

Independent and Remotely Guided Studies

Studies can be conducted asynchronously and reach a large number of participants. However, challenges include potential distractions in home environments (e.g., from other people in the home) and that there is usually no experimenter to monitor proper execution of study instructions and provide assistance with questions and problems. Therefore, providing opportunities for remote study support is advisable, but may require flexibility due to different time zones and the fact that participants may favor participation outside of normal working hours.

Framework for Remote VR Studies

There are several options for development, distribution, and recruiting – from offering a stand-alone VR application for download, to posting the trial application in AppStores, to using a VR platform (e.g., Steam). All options have different advantages and disadvantages and differ in how user data can be collected, how remote support can be implemented, and through which channels recruiting is possible.

Our framework consists of four primary approaches to remote VR studies:

1 Researchers develop a standalone VR application that is distributed directly to participants.
2 Researchers develop a VR application that is distributed through existing vendor platforms (e.g., app stores).
3 Researchers create a VR application that uses an API of an existing social VR platform (e.g., Rec Room, VRChat) and upload it to the appropriate platform.
4 Researchers set up their study environment directly on an existing social VR platform and use the tools provided by these platforms.

Prof. Dr. Florian Alt
florian.alt@unibw.de
+49 89 6004 7320
https://go.unibw.de/xr-security-en

FIG.: VILLE MÄKELÄ / RI CODE

Prof. Dr. Harald Baier

Digital Forensics

Due to increasing digitization and subsequent cybercriminal activities, the need for digital forensics competencies is growing too. The main research areas of the Professorship of Digital Forensics address the handling of bulk data in IT forensic investigations, the generation of synthetic datasets to assess IT forensic tools, anti-forensics, and main memory forensics.

DIGITAL FORENSICS, as the digital equivalent of the classic forensic disciplines, always comes into play when an answer to a question of doubt is sought in connection with an IT system. A case in point would be when a remote-controlled drone is used to transport drugs, but during transport the drone crashes onto the property of a bystander. When called to help, the police take over the drone and are supposed to clarify the questions of doubt as to who was piloting the drone and what routes it was flying. To do this, the supporting IT forensic experts secure the drone's data media, analyze them, and try to provide answers to the questions of doubt.

Seeking Access

An IT forensic investigation is associated with numerous challenges, which the Professorship of Digital Forensics deals with. A first important challenge is the question how data – especially from innovative IT devices such as drones or cars – can be secured and analyzed. The background to this is that these devices often only offer unknown interfaces for access and data storage is dependent on the manufacturer in terms of partitioning, file system, and file format.

Searching for Training Data

A second important challenge is the accuracy of IT forensic tools, meaning that they should work as specified. This requires standardized test data sets. For these, the digital traces to be detected are known a priori and matched against the detected traces by the respective tool. However, such datasets are not sufficiently available to the community.

Throwing Sand in the Gears

A third important task is dealing with anti-forensics, i.e., all measures taken by attackers to cover up or destroy their tracks. Anti-forensics have always been used by criminals – for example, a burglar wears gloves to avoid leaving telltale fingerprints. In digital forensics, it is important to understand and detect anti-forensic methods used by attackers.

Prof. Dr. Harald Baier

harald.baier@unibw.de

+49 89 6004 7345

www.unibw.de/digfor

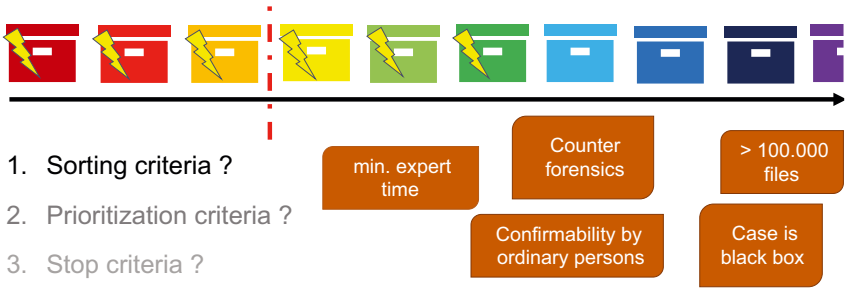
One challenge of IT forensics is to secure and analyze data.

FIG.: ADOBE STOCK / NOPPONPAT; MICROGEN

CSAM: “Just” possession or more?

Investigators face this question every day, and technical assistance is urgently needed.

The number of cases involving child sexual abuse material (CSAM) is increasing dramatically. Our research in the field of digital forensics aims to enable efficient identification of self-produced CSAM among the abusive material acquired from the Internet. In a first step, we automatically group media files based on their metadata using data science algorithms in order to process them in a prioritized manner.



Visualization of the project goal, milestones, and requirements.

EVEN “JUST” POSSESSION of child pornography is provocative. After all, it is a crime that immediately evokes a strong reaction of abomination in most people. Unfortunately, the detection of child sexual abuse material (CSAM) is nothing special anymore for digital forensic experts; it is the norm. Digital forensic experts are faced with the fact that not only the number of cases increased more than sixfold within the last five years, but the general amount of data as well as the number of CSAM detected is increasing, as well.

Most of these cases are the result of automated reports from the USA. Service providers such as Facebook are required by U.S. law to check uploads for known CSAM. In 2021, Germany’s Federal Criminal Police Office (BKA) received 79,701 such reports, which corresponds to just under one report per 1,000 inhabitants. Experience shows that among these suspects there is at least a single-digit percentage of people who have themselves abused children and documented this in the form of images or movies. To prevent further child abuse, identifying these files must be a top priority.

Investigators utilize specific metadata of CSAM for this purpose and look for links to the cameras or smartphones used by the suspect. However, this approach doesn’t work if the suspect has deleted the relevant metadata. The approach is also inefficient when dealing with large amounts of data. Since investigators are now often dealing with more than 100,000 instances of CSAM in a single case, manually identifying these files is a matter of luck.

With our research we want to enable investigators to efficiently and effectively identify self-produced CSAM. In the first step, we automatically cluster media files based on their metadata. In contrast to the usual approach of investigators, we use all available metadata, which makes our approach more resilient to the deletion of certain metadata. To enable the clustering of huge amounts of files, we use the latest data science algorithms. This year we, did a first data analysis of about 4,000 publicly available images and published it at a conference. The results were promising, and we are now scaling our approach. Our next steps are to prioritize the clusters based on their content and define termination criteria that, when reached, an investigator can be confident that it is highly unlikely that evidence of child abuse will be missed.

Samantha Klier, M.Sc.
samantha.klier@unibw.de
+49 89 6004 7346
www.unibw.de/digfor

FIG.: RI CODE / S. KLIER

Synthetic Generation of Datasets

A fundamental problem in Digital Forensics is that, due to data protection and security aspects, the use of real datasets is often difficult or even impossible. However, testing IT forensic evaluation software for education and training in digital forensics as well as for training machine learning methods requires realistic, individual, and dynamically configurable datasets from persistent data carriers, volatile main memory contents, and from the associated network traffic. Datasets from additional IT systems such as smartphones or drones are becoming more important. Such datasets need to contain the forensically relevant traces in each case, so that forensic experts and their tools are prepared for later real-world use. Providing such datasets is extremely time-consuming.

Requirements

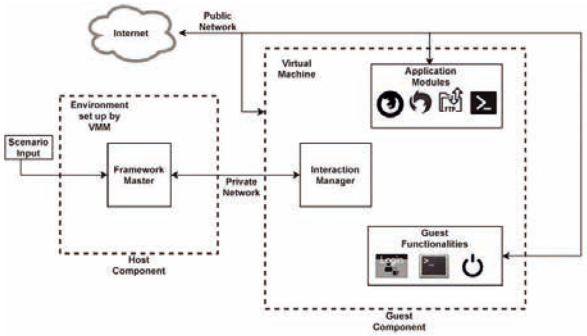
There are numerous requirements for high-quality datasets, such as the coherence – i.e., the respective digital traces must be generated together in the context of the same scenario so that more complex forensic analyses based on multiple data sources are possible in the first place. In addition, the datasets must meet other requirements such as adaptability, availability, traceability, and verifiability. Another essential point for evaluating datasets is to know what the IT forensic software is supposed to find later at all, i.e., the dataset must be "labeled", and the ground truth must be known.

hystck

The team's hystck framework is used to generate synthetic datasets with a realistic ground truth. The framework supports the automatic generation of synthetic network traffic as well as the operating system and application artifacts by simulating human-computer interactions.

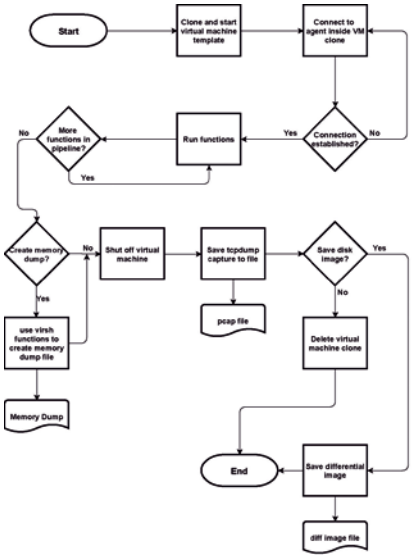
ForTrace

ForTrace is an extension to hystck. With ForTrace, the researchers take a holistic approach to data synthesis, which is the synthesis of persistent, volatile, and network traces. ForTrace is able to recreate various existing, realistic, and complex scenarios relevant to IT forensics, as well as to dynamically configure and extend the data synthesis according to the user's own wishes through its modular framework design. The ForTrace framework is capable of generating not only classic persistent data carriers, but also volatile RAM contents and traces in the network of one and the same IT forensic scenario in consideration. This is what enables a subsequent multi-source analysis in the first place.



The data synthesis framework ForTrace is able to mimic typical user behavior on end systems in order to automatically generate data as realistic as possible for IT forensic evaluation.

FIG.: RI CODE / H. BAIER (2)



ForTrace is able to roll out multiple virtual machines with different software. These are then triggered to mimic user interactions via a separate network interface with a variety of different control commands.

Thomas Göbel, M.Sc.

thomas.goebel@unibw.de

+49 89 6004 7347

www.unibw.de/digfor/forschung/fortrace

Github link "ForTrace":
https://github.com/dasec/ForTrace

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

The research group headed by Stefan Brunthaler focuses on language-based security, an area that investigates the use and applicability of language-based transformations to secure vast amounts of software in a way that is automated, transparent, and effective. A key aspect of these techniques is that it offers unparalleled scalability, as evidenced by the ability to compile enormously complicated software systems, such as web browsers.

THE Munich Computer Systems Research Laboratory (µCSRL) directed by the Chair of Secure Software Engineering conducts world-class research in computer security by coming up with novel defenses that mitigate advanced attacks, primarily focusing on code-reuse attacks. By leveraging our expertise in programming languages, particularly in compiler technology, we tackle challenging and important problems in programming languages, as well as in security and privacy, through our focus on language-based security.

For µCSRL, the past year continued our successful growth and we are also happy to report further milestones in our research efforts.

Our research in software diversity continued and we were able to raise the bar considerably: Not only does our latest research mitigate address-oblivious code reuse (AOCR for short), we also investigated its properties to prevent another advanced and sophisticated code reuse attack, PIROP, which is short for position-independent return-oriented programming. We received great feedback from the research community and expect publication documenting our success in the first half of 2023 in a highly competitive and selective venue. To the best of our knowledge, we are the only research group possessing this technology.

In addition, we were able to find our first bugs using our fuzzing cluster (we found a bug in the "curl" command line tool.) We spent considerable time fine tuning our setup, which provides the foundation for our upcoming research endeavors.

Prof. Dr. Brunthaler was also able to obtain highly competitive international funding from the Austrian Research Promotion Agency (FFG). Together with Prof. Dr. Payer from EPFL, Prof. Dr. Volckaert from KU Leuven, and Prof. Dr. Mayrhofer from the University of Linz, our research group will collaborate with Dr. Thomas Ziebermayr from the Software Competence Center Hagenberg (SCCH) to research novel techniques to protect software and its intellectual property from reverse engineering through competitors. The project, called Dependable Production Systems (DPES, for short), started in 2022 and will last until the end of 2026.

Prof. Dr. Brunthaler and his team have published 37 papers in the area of Systems, with close to half being published at conferences having a CORE ranking of A and A*. For each paper, the effort required to construct research prototypes lies between 15,000 and 20,000 lines of C and C++ code.

In 2022, Prof. Dr. Brunthaler was invited to serve on the program committees of the *Symposium on Network and Distributed System Security* (NDSS 2023 in San Diego), the *ACM Conference on Computer and Communications Security* (ACM CCS 2023 in Copenhagen), and the *IEEE European Symposium on Security and Privacy* (EuroS&P 2023 in Delft). In 2023, Prof. Dr. Brunthaler will also succeed Prof. Dr. Payer as the area chair for System Security at the Journal of Systems Research (JSys).

The µCSRL research group received funding from the German Ministry of Defence, the Austrian Research Promotion Agency, the state of Upper Austria, and Airbus Defence & Space GmbH.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

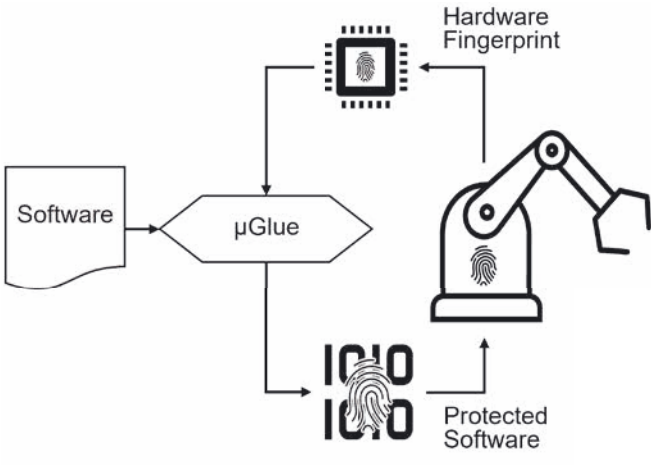
www.unibw.de/ucsrl-en

FIG.: ISTOCK / DE M10

Project µGlue

Efficient and Scalable Software to Hardware Binding using Rowhammer

Industrial espionage and intellectual property theft cause considerable economic damage every year. While the physical manufacturing plants can be secured against theft, existing anti-theft systems for industrial software are incomplete. With µGlue we develop a new kind of copy protection based on software diversity and Rowhammer. µGlue ensures that the protected software only shows the desired behavior when run on genuine hardware.



To counter reverse engineering, µGlue compiles programs such that they expect a hardware fingerprint to operate properly. Without this fingerprint, the program does not exhibit the expected behavior, thereby misleading attackers.

Software Diversity

The idea behind software diversity is to diversify the inner structure of a program without modifying its behavior. Software diversity not only makes diversified programs more resilient against attacks, but also frustrates reverse engineering attempts. In particular, insights gained from analyzing one diversified copy do not translate verbatim to another diversified copy. As a result, software diversity increases the cost of reverse engineering considerably.

Rowhammer

Rowhammer is a technique to exploit a hardware flaw that is present in most commercially available DRAM memory modules. Rowhammer accesses the memory module with a specific access pattern to induce so-called bit flips. A bit flip changes the value of a memory cell from zero to one or one to zero even though the cell itself was not accessed. This phenomenon is caused by the high packing density of modern memory modules. Through proper calibration, single bit flips can be induced systematically.

µGlue

With µGlue we combine the techniques of software diversity and Rowhammer to inseparably link software with underlying genuine hardware. While Rowhammer is typically used in attacks against computer systems, we utilize Rowhammer as a building block for a new type of copy protection. µGlue uses the unique configuration of bit flips in the underlying hardware to guarantee that the software runs correctly on the intended machine. If the same software is run on a copy of the hardware, however, the software no longer exhibits the intended behavior. As a result, the costs of reverse engineering can be increased to a point where theft of intellectual property is no longer economically feasible.

Broader Impact & Social Relevance

µGlue helps to mitigate the theft of intellectual property and, thus, guarantees that expensive investments in the improvement of production lines or the development of new manufacturing plants remains worthwhile.

Prof. Dr. Stefan Brunthaler
brunthaler@unibw.de
+49 89 6004 7330
www.unibw.de/ucsrl

Funded by:
Austrian Research Promotion Agency (FFG)

FIG.: RI CODE / S. BRUNTHALER

Project µOI

C++ Object Integrity

Despite its susceptibility for security vulnerabilities, C++ is still used in many applications. A common type of attack against programs written in C++ are "code-reuse" attacks, which abuse code already present in the attacked program. Among these code-reuse attacks, a notoriously difficult to prevent variant is called counterfeit object-oriented programming (COOP). With µOI, we developed a defence, that combines static and dynamic concepts to mitigate COOP attacks.

Code-Reuse Attacks

For a long time, attackers were able to inject malicious code into programs by exploiting buffer overflows. However, once these code injection attacks were mitigated by defences, such as data execution prevention, attackers improved their attacks to create so-called "code-reuse" attacks. In a code-reuse attack an attacker abuses code that is already present in the attacked program.

Counterfeit Object-oriented Programming

There already exist a lot of effective defenses against code-reuse attacks, such as control-flow integrity or software diversity. However, a new type of code-reuse attack, called COOP, surgically abuses internal structures of C++ programs and, therefore, successfully bypasses existing defenses. In a COOP attack, an attacker injects counterfeit objects into the memory of the victim program to abuse existing code.

COOP Mitigation

With µOI, we implemented a defence that ensures the integrity of C++ objects in memory. A modified compiler hardens compiled programs, by creating and verifying run-time checksums of C++ objects. These checksums prevent attackers from inserting counterfeit objects into memory as well as modifications of existing objects. As a result, µOI successfully prevents COOP attacks.

Broader Impact & Social Relevance

The implemented defence improves the safety of C++ applications running on a broad variety of devices by limiting the attack scope in the area of highly sophisticated code-reuse attacks.

Similar to ransom notes, "code reuse" attacks combine existing program code fragments so that they have different functionality.

FIG.: PICTURE ALLIANCE / DPA

Prof. Dr. Stefan Brunthaler
brunthaler@unibw.de
+49 89 6004 7330
www.unibw.de/ucsrl

Prof. Dr. Michaela Geierhos

Data Science

The interdisciplinary team of the Professorship of Data Science combines expertise from the fields of computer science, computational linguistics, and economics to address current and future-oriented research questions in the areas of Semantic Information Processing and Knowledge & Data Engineering.

Applied Research

Data Science is an applied, interdisciplinary science. Its goal is to generate knowledge from data in order to support decision-making processes, for example. Approaches and knowledge from different fields such as mathematics, statistics, stochastics, computer science, and computational linguistics are used. The Professorship of Data Science investigates methods for extracting information from data and develops data-driven solutions by processing, preparing, analyzing, and inferring large amounts of data (Big Data). It therefore focuses on knowledge-based and computational linguistic approaches. The tasks include developing algorithms for (semantic) text analysis and enabling human-computer interaction via information systems (e.g., information retrieval, question answering). Practical applications include search engines, social media mining, sentiment analysis, and knowledge-based question-answering systems.

Theory-Practice Transfer

In order to link theory and practice in research issues as well, the Data Science team maintains numerous collaborations with partners from the military, corporate and the public sector. In an increasingly fast-changing world, forward-looking and innovative software solutions are the key to long-term success. Even if the future often seems uncertain, the research group members are inspired by Alan Kay's guiding principle from 1970: "The best way to predict the future is to invent it."

Practice-oriented Training

The Data Science courses particularly focus on a concept that combines theory and practice. From the very beginning, students benefit from the opportunity to directly apply the theoretical knowledge gained in the lectures in varied exercises and diverse practical projects. In this way, the Professorship of Data Science contributes to the excellent academic education of students at the University of the Bundeswehr Munich.

Data Science Use Cases

The current areas of application range from the detection of disinformation campaigns and hate speech in social media to the detection of so-called deep fakes and situation-based early crisis detection. The goal of today's research is to detect influence campaigns as early as possible, to warn against them, and to track their development and spread in order to ultimately initiate suitable countermeasures. For this purpose, the identification and modeling of short-term disinformation campaigns in social media such as Twitter, etc. are in focus.

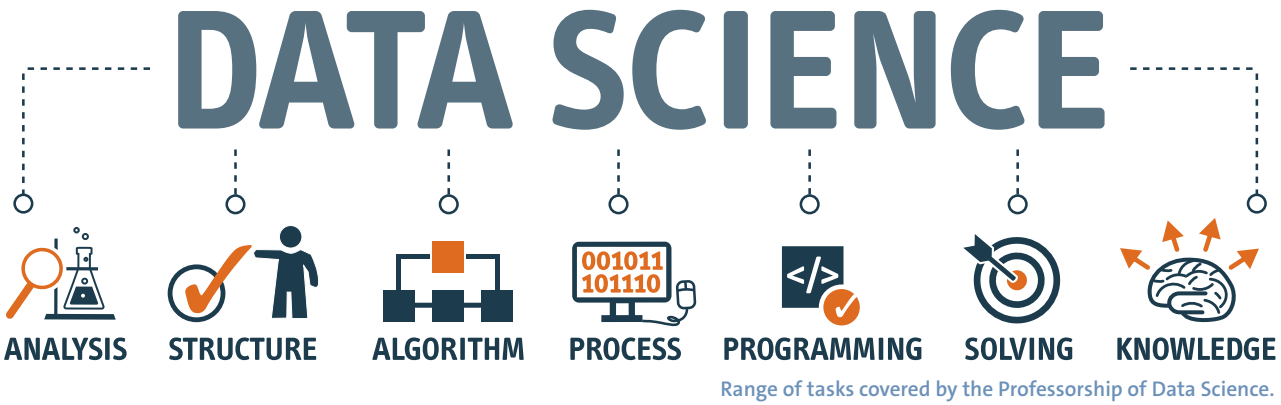
Recent technological advances and developments in the field of Artificial Intelligence (AI) have also given rise to deep fakes. This refers to an audio-visual modification of a video generated by means of AI, in which the face and/or statements of the person depicted in the video have been changed. The research group's aim is to uncover these manipulations.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

www.unibw.de/datascience



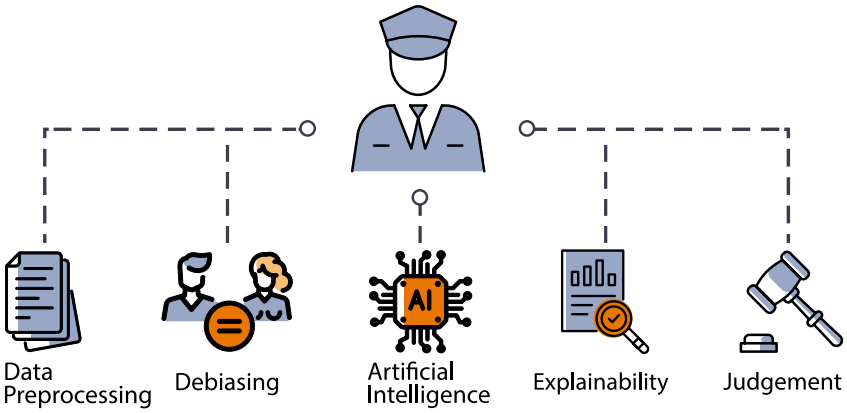
Range of tasks covered by the Professorship of Data Science.

FIG.: SHUTTERSTOCK / RYZHI, TRUEFFELPIX

Project VIKING

Trustworthy Artificial Intelligence for Police Applications

Artificial intelligence (AI) is generally understood as a black box, where it is not comprehensible how a decision has been made, how trustworthy a decision is, whether certain characteristics of affected persons lead to unfair disadvantages, and how or with which data a model's knowledge has been learned. The VIKING project is therefore attempting to overcome these challenges, taking into account technical, legal, and ethical factors.



Factors for using trustworthy artificial intelligence to support police applications.

Police Use Cases

While the Internet offers a wide range of networking opportunities, there are numerous ways in which these possibilities can be abused for criminal purposes. As a result, there is a need for police authorities that are able to monitor specific sources and target reported incidents for investigation. Moreover, investigators are exploring large data sources of text, images, videos, and structured data from a variety of contexts, including social media, companies, or private devices. This variety and volume of data challenges police authorities to answer specific questions and find concrete evidence of wrongdoing. These are tasks that can no longer be solved with manual work. In the VIKING project, therefore, the problems of text analysis, speaker, image, and object detection are to be addressed with the help of AI.

Text Analysis Using Artificial Intelligence

In VIKING, the research institute CODE works on filtering and extracting information of police-relevant texts. The combination of classifying texts into predefined crime types and extracting precise information such as persons, places, times, and dates as well as objects and properties provides the ability to generate structured data models of crime events. This enables filtering of big data sources and matching with existing databases and investigation results. In addition, situation reports can be generated using the extracted information. These can display aggregated information of specific crime types, locations, or time periods while providing the ability to filter specific attributes and visualize annotated maps. All methods used and developed methods must include fair treatment of, for example, ethnic and demographic characteristics. Furthermore, the models and their output must be explainable by using multiple appropriate explainable AI methods. Finally, the project results are integrated into a demonstrator.

Support Rather than Autonomy

The solutions developed in the project are by no means to be understood as a substitute for human decision-making and automation of justice. Rather, the algorithms support the search for relevant data in extensive and heterogenous data repositories. For this purpose, the software then provides suggestions on the detected misconduct or on searched text content, such as persons, location and time information, and relevant objects. The law enforcement authorities then have to check these on the basis of the corresponding explanations and manually integrate them into the further investigation process, whereby no decisions are made by the AI itself, which merely has a supporting function.

Falk Maoro, M.Sc.
falk.maoro@unibw.de
+49 89 6004 7353
https://go.unibw.de/viking

Funded by: BMBF

FIG.: RI CODE / F. MAORO

Collaborative Research Center 901 – On-The-Fly Computing

Parameterized Service Specification for Customized Applications

On-The-Fly (OTF) Computing explores the possibilities of providing people with more customized software services (apps) tailored to their needs. This subproject addresses several types of requirement specifications that enable successful service discovery, composition, and analysis.

Natural Language Specifications

The goal is to enable end-users to participate in their specification process by allowing them to formulate requirements in natural language, without constraints on expressiveness. Similar to using a search engine, they should be able to formulate their requirements in natural language without any special technical background knowledge. For this reason, processing and interpreting natural language queries is an essential requirement for the OTF vision. Since formal specifications are not very intuitive, natural language is usually the only format that comes into question. Developers must therefore accept free-form natural language query descriptions. In doing so, they must contend with the typical difficulties of free-form text. These include a lack of structure and correctness, grammatical and spelling errors, and ambiguity in syntax and semantics. In addition, information is missing that is important for development but that users do not have in mind. Queries are therefore inevitable.

User-centered Dialogue Planning and Design

In terms of agile, participative software development, users will be more involved in the interactive composition process of applications to be created on-the-fly in the future. This dialogue will be carried out by a chatbot, which will be used for targeted queries as well as for the resolution of ambiguities. For this purpose, the subproject investigates iterative clarification processes to specify and complete existing requirement descriptions in natural language. End-users will be individually supported during the specification process by means of targeted queries, suitable examples, or suggestions.

Transparency of Service Configurations

For the final product, the so-called service configuration of an application, it must also be made clear which initial requirements were taken into account and which had to be discarded. In this way, it is not necessary to wait until trial and error to find out whether the initial expectations of the newly configured application have been met. Instead, an understanding of the feasibility of the requirements is created among the users at an early stage.

A before-and-after comparison is used to determine the extent to which the initial requirements have been met in the resulting service. The result is a transparent composition process that includes natural language inaccuracy detection and compensation methods to improve comprehension.

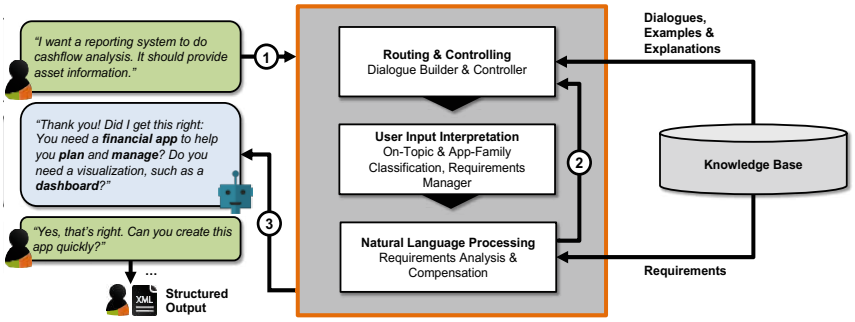


FIG.: RI CODE / M. GEIERHOS

Solving requirement gaps with a chatbot.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

https://sfb901.upb.de/projects/project-area-b/subproject-b1

Funded by: DFG

Prof. Dr. Wolfgang Hommel

Software and Data Security

Wolfgang Hommel's team researches technical and organizational security measures for complex IT infrastructures and communication networks with an increased need for protection as well as their practical application under the motto "Development and operation of secure networked applications."

THE TEAM OF the Professorship of Software and Data Security pursues the goal of developing solutions for real-world-relevant security challenges under the consideration of operational boundary conditions that are typically part of the operation of complex IT infrastructures.

Research and projects with third parties therefore usually begin with a comprehensive empirical analysis, in which, for example, relevant components from the designated application area are either cloned into virtual environments or at least their core characteristics are modeled and simulated to facilitate detailed analysis. This approach allows, among other things, the explorative application of offensive test procedures and thus the qualitative and quantitative analysis of vulnerabilities in complex multi-step attack scenarios. From this, security requirements can be systematically derived, which serve as a basis for the subsequent constructive activities and a later practical evaluation of the results achieved.

The design of new and improved IT security measures follows the security engineering approach: On the one hand, they are designed, modeled, and simulated on a technical level and, on the other hand, they are integrated as seamlessly as possible into the design, implementation, and operational processes of the intended application areas, also from an organizational perspective. An essential requirement is the concrete implementation with subsequent evaluation, which takes place at a minimum in the laboratory but, if possible, also in concrete pilot environments and ideally by individual embedding in scientifically accompanied projects. The role of the human factor in information security, economic, and legal constraints is also taken into account.

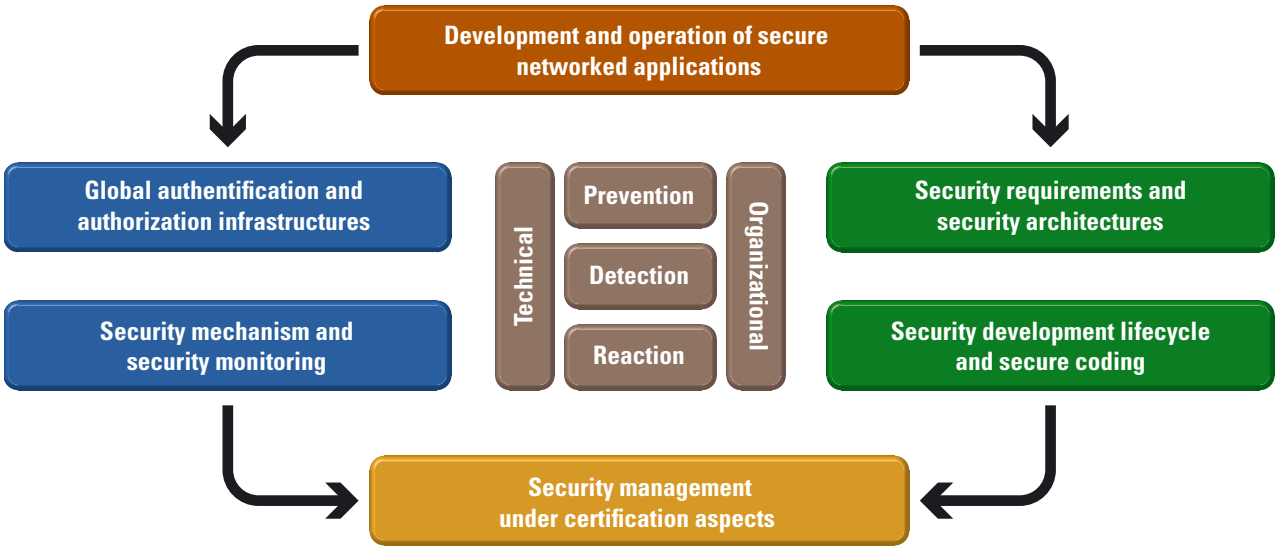
Current research projects and projects are, for example, being done on the implementation of the self-sovereign identity paradigm for use in inter-organizational authentication and authorization infrastructures as a data protection-friendly technological advancement of federated identity management that has proved itself in practice. Ongoing work on security monitoring components and policy-driven management platforms for federated software-defined networks is used, for example, in the establishment and expansion of the 5G telecommunications infrastructure and in the dedicated cross-location networking of industrial control systems. They lay the foundation for securing future 6G technologies and find their application in areas such as securing the remote management infrastructures of future power supply networks. In the area of the Internet of Things, the research focus is on the software-side protection of LoRa- or LoRaWAN-based infrastructures, which are particularly resistant to interference, and have attractive characteristics for industrial as well as governmental and military applications.

Prof. Dr. Wolfgang Hommel

wolfgang.hommel@unibw.de

+49 89 6004 7355

www.unibw.de/software-security



Main research topics of the Professorship of Software and Data Security.

FIG.: ISTOCK / VERTIGO3D; TAUSENDBLAUWERK, QUELLE: W. HOMMEL

Project DISPUT

Digital Identities with Self-sovereign Identity Management: Processes and Technologies

IT security, data protection, and usability are essential aspects, especially for state digital/electronic identities (eID). The DISPUT project supports the Bavarian State Ministry of Digital Affairs (StMD) in setting up and operating the national identity federation FINK and, in the same context, researches self-determined identities (SSI) as a future technology.

Possible future use of eGovernment services via self-sovereign identities.

DIGITAL IDENTITIES accompany us all privately, professionally, and increasingly in eGovernment, where administrative services such as applying for child benefits can be used online. Traditionally, one has to set up a separate account with each online service provider. To keep data consistent and facilitate the use of services, federated identity management (FIM) has been introduced. All users have an individual home organization that is responsible for managing their personal data. With this data, services can be used within a so-called federation.

SSI for Privacy and Data Protection

Since with FIM the home organizations could collect data (when which service was used) and create unwanted tracking profiles, the principle of self-sovereign identities emerged. Here, each person manages their identity data in a kind of digital wallet via smartphone or on a PC. The digital IDs stored in this way can be used flexibly. Even though SSI is often associated with blockchains, it can be implemented with a public key infrastructure (PKI), among other things.

Identity Management for eGovernment

In the context of the DISPUT project, the team of the Professorship of IT Security of Software and Data is dealing with the question of how existing systems in the eGovernment sector should be operated and what possibilities there are to design these systems with SSI in the future. On behalf of the IT Planning Council, the StMD is in charge of implementing the Germany-wide identity federation FINK (Föderiertes Identitätsmanagement interoperabler Nutzerkonten) in the federal and state-wide cooperation. FINK enables citizens to access online administrative services nationwide within the framework of the Online Access Act (OZG) with just one user account.

Holistic Approach for FINK

The basis for FINK is the use of the FIM protocol Security Assertion Markup Language (SAML), which has been tried and tested in the university environment. Due to technological change, more modern protocols are increasingly being used, and these were investigated for use in FINK in the form of demonstration models, among other things. In addition, support was provided for operational processes in the sense of professionalized IT service management. A user study was conducted to consider the user perspective on SSI and possible awareness designs. In addition, activities around SSI are increasing internationally, as can be seen, among other things, in the new version of the eIDAS regulation. Here, the project focuses on cooperation with other projects, including IDunion and the SSI and AARC BPA Expert Group, and on integration into existing IT infrastructures.

Prof. Dr. Wolfgang Hommel
wolfgang.hommel@unibw.de
+49 89 6004 7355
https://go.unibw.de/disput

Funded by: StMD

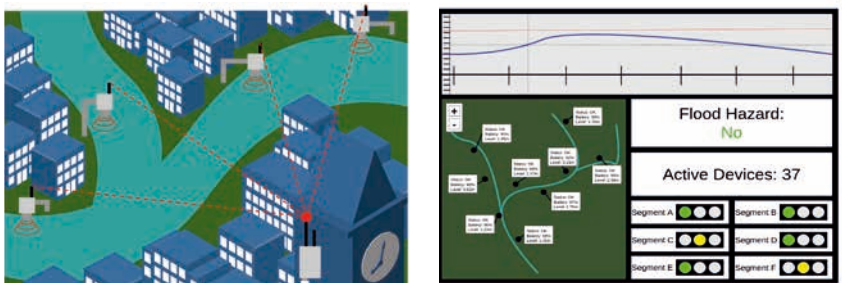
FIG.: RI CODE / M. GRABATIN

Project ROLORAN

Resilient Operation of LoRa Networks

The objective of the ROLORAN project is to investigate and improve the robustness of the IoT protocol LoRaWAN (Long Range Wide Area Network), which is based on the modulation technique LoRa. In addition to measurement series, software analyses, and hardening measures, the practical focus is on prototyping in the context of meshes, jammers, and localization mechanisms as well as testing in various application scenarios.

FOR SEVERAL YEARS now, LoRaWAN has been establishing itself in the IoT sector as a particularly robust low-power WAN protocol. The technical basis for this is the interference-resistant LoRa modulation technology for signal transmission, which uses chirp spread spectrum technology. At the logical level, additional AES128-based methods for integrity assurance and payload encryption complement the robustness of the protocol. Nevertheless, LoRa(WAN) devices can achieve a service life of more than 10 years in battery operation thanks to pronounced energy efficiency and can also easily bridge ranges of several kilometers, depending on the building density. Transmitted data volumes of 256 bytes per packet are particularly suitable for compact data representations and sensor values. Inexpensive end devices send these data packets to (mostly) stationary gateways, which forward the received information to a downstream server infrastructure for evaluation.



Schematic diagram of the deployment of LoRaWAN-based water level sensors with data processing.

Wireless Standard for the Future?

As LoRaWAN is now widely used in IoT applications, the project investigates the current state of the existing LoRaWAN landscape from an IT security perspective. For this purpose, static and dynamic analysis tools are used in the project to check reference implementations for weaknesses and to provide hardened open source software in case of critical errors. Various measurement series in the laboratory as well as in the field complement an assessment by determining the physical limits and behaviors of a LoRaWAN transmission. The investigations also take into account (un)intentional influences by interfering signals and/or transmitters and finally classify the suitability for transmitter localization. Overall, a holistic assessment of the capabilities represents the goal of the analysis.

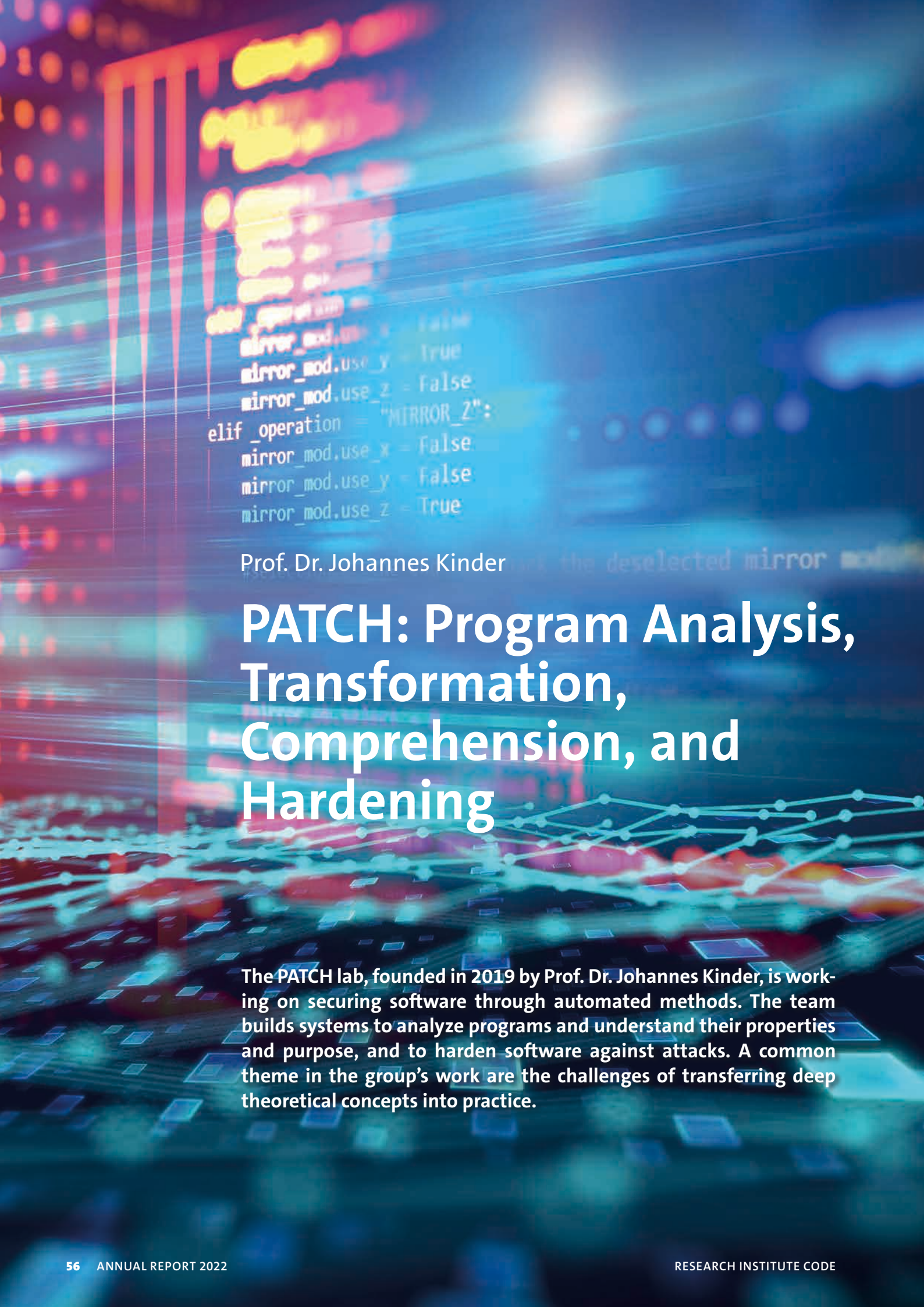
Application Potential in Crisis Scenarios

In addition to the analysis of LoRa(WAN), practical application plays a major role in the project. Here, the project evaluates selected scenarios. At the LoRaWAN level, this primarily concerns large-scale sensor networks. One of the scenarios to be evaluated is a cooperation between the project and the District of Bad Kissingen with the goal of setting up and operating an infrastructure for the realization of a flash flood early warning system. When using LoRa directly without the LoRaWAN architecture, scenarios with point-to-point transmissions are of interest. For this purpose, the project is testing its own prototypes with repeater functionality and their extension to self-organizing meshes, which represent usable alternatives to the failed communication channels in blackout scenarios, for example.

Prof. Dr. Wolfgang Hommel
wolfgang.hommel@unibw.de
+49 89 6004 7355
https://go.unibw.de/roloran

Funded by:
dtec.bw
Funded by the European Union
NextGenerationEU

FIG.: RI CODE / M. SILACI



Prof. Dr. Johannes Kinder

PATCH: Program Analysis, Transformation, Comprehension, and Hardening

The PATCH lab, founded in 2019 by Prof. Dr. Johannes Kinder, is working on securing software through automated methods. The team builds systems to analyze programs and understand their properties and purpose, and to harden software against attacks. A common theme in the group's work are the challenges of transferring deep theoretical concepts into practice.

THE RESEARCH OF the PATCH lab focuses on automatic methods for securing computer systems and software. To design tools for developers and organizations in order to find and neutralize faulty or harmful code is the goal of its work. The approach is based on theoretically well-founded methods: in particular, abstraction, logic, and machine learning.

The name PATCH defines the core areas of the lab headed by Prof. Dr. Kinder: "Program Analysis, Transformation, Comprehension, and Hardening." The programs the researchers are interested in are the applications and systems software that govern our daily lives, from operating systems and device drivers to mobile apps and embedded software for the Internet of Things.

Program Analysis and Bug Finding

Today, automated methods such as static analysis or fuzzing can find many classic software bugs such as overflows in C programs. However, software bugs are still a major cause of security incidents. In its research, the group tackles the problems arising in practice due to complex runtime environments, systems, and hardware. This includes JavaScript ecosystems such as Node.js, newly introduced platforms such as WebAssembly, but also vulnerabilities caused by the speculative execution common in modern processors.

Program Understanding and Reverse Engineering

To check the suitability and security of software, the team develops automated methods to categorize and understand program components. This can allow an organization to discover back doors or malware in third-party software using automated tools or through manual security audits. To this end, the researchers develop both classic, formal methods-based approaches, as well as models based on statistical and deep learning. Each method has its own unique strengths: Static analysis can reason about all possible program behaviors but is often imprecise; dynamic analysis (or testing) is unparalleled in providing actionable reports about deviant program behavior but is limited by what it can observe; and deep learning is capable of capturing human intuition about code, as encoded in function names and source code comments, but requires large amounts of annotated data. Understanding what each method can and cannot do is a prerequisite to finding the solutions that will prevail in practice.

Program Transformation and Hardening

In addition to identifying vulnerabilities, it is important to limit the potential impact of an attack. In complex systems, errors can practically never be ruled out. However, by adding additional controls to the program code, it is possible to prevent an attacker from gaining control over critical components of the system. When designing program transformations, it is critical to not alter the behavior of a program and affect performance as little as possible.

Prof. Dr. Johannes Kinder

johannes.kinder@unibw.de

+49 89 6004 7335

www.unibw.de/patch

The Bavarian Research Association ForDaySec launched in 2022 with a kickoff-event in Passau, in the presence of the Bavarian Minister of Science and Arts Markus Blume. From left to right: Robert Obermaier, Felix Freiling, Harald Kosch, Sabine Toussaint, Thomas Riehm, Henrich Pöhls, Markus Blume, Johannes Kinder, Dominik Herrmann, Joachim Posegga, Stefan Katzenbeisser, and Achim Dilling.

FIG.: ISTOCK / MONSITJ; UNIVERSITY OF PASSAU

Project ForDaySec

Security for Everyday Digitization

The Bavarian research association ForDaySec pursues a holistic approach to addressing the security problems of digitization in private and professional everyday life. The contribution of RI CODE focuses on methods for eliminating vulnerabilities in smart devices, from network printers in the office to robot vacuums at home.

THE DIGITIZATION of everyday devices is a central challenge of IT security. This applies to robot vacuums and temperature controllers in private households as well as to printers, WiFi routers, and industrial control systems in SMEs, municipal water suppliers, and hospitals. Smart components are often deployed with little regard for security, and previously independent systems are being connected without precautions, while the knowledge and human resources to actively manage cyber security are often found lacking.

Interdisciplinary Research

Existing digital infrastructures often cannot be fundamentally redesigned or modified to secure them – security solutions must use existing systems and components. Security and data protection technologies must be easy to administer and implement without specialist knowledge. Here, however, the challenges are not only of a technical nature, but also encounter organizational, procedural, and personnel hurdles. ForDaySec tackles these problems with interdisciplinary research that, together with its members University of Passau, Technical University of Munich, FAU Erlangen-Nuremberg, and University of Bamberg, systematically integrates the challenges of everyday practices from the very beginning.

Firmware Hardening

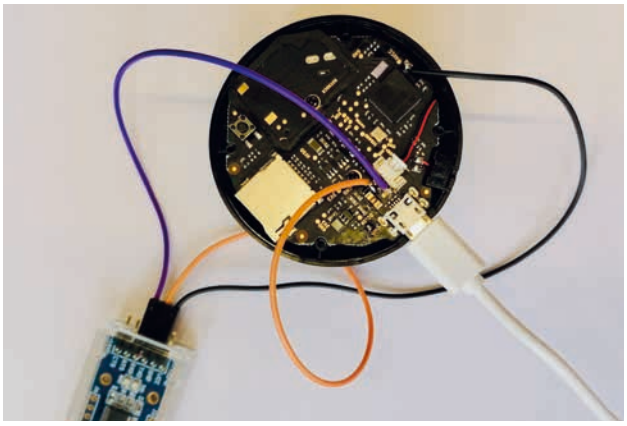
IoT devices run software, often based on open-source products combined with proprietary developments by manufacturers. However, manufacturers often pay little attention to IT security. Especially for products from the low-price segment, security updates are rarely or never made available, and customer support does not exist or is not available on a long-term basis. Thus, known security vulnerabilities in the used open-source libraries remain permanently open and attackers can successfully exploit them, even years later.

Our goal is to close vulnerabilities on the devices themselves and thus harden them. Known vulnerabilities in open-source libraries are to be surveyed and, with the help of patterns, detected directly in the device software and subsequently eliminated, even if a manufacturer does not provide any support for this.

The focus is on the software aspects of such an approach to hardening firmware. Semantic patches are to be created and applied precisely for the vulnerabilities. The integrity and functionality of the firmware must be preserved. Finally, the functionality of the patched firmware will be tested so that it can successfully be deployed.

Sebastian Jänich, M.Sc.
sebastian.jaenich@unibw.de
+49 89 6004 7332
https://go.unibw.de/fordaysec

Funded by: StMWK



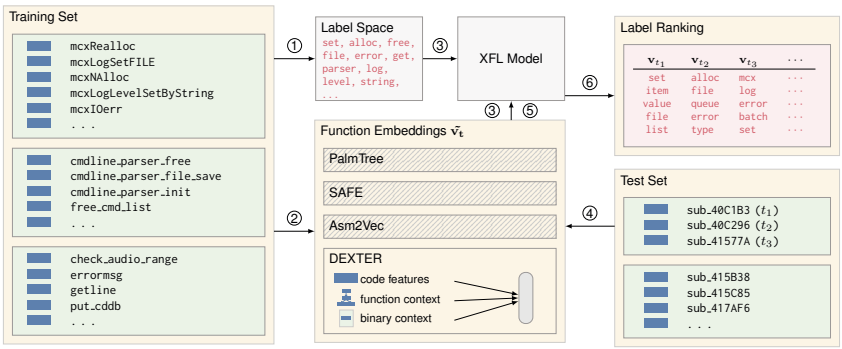
Circuit board of a smart surveillance camera. Vulnerabilities in the firmware of smart home devices can be a point of entry for attackers.

FIG.: RI CODE

Project XFL

Synthesizing Function Names with Multi-label Learning

Function names are extremely useful to a human reverse engineer, but usually unavailable in most security-relevant contexts. XFL learns the relationship between identifiers and code based on thousands of open-source projects and is thus able to suggest plausible names for unknown functions in binaries.



XFL learns the correspondence between the words in a function name and the binary code of the respective function. The resulting model can synthesize plausible names for previously unknown binary functions.

SOFTWARE REVERSE ENGINEERING is the process of understanding the inner workings of a software system. In a computer security context, reverse engineering is typically performed on a binary without access to source code. Binaries typically do not contain function or variable names, which would be valuable signposts for a reverse engineer. Traditionally, reversing tools use patterns of known binary code to label at least some frequently used software components.

Function Names as Labels

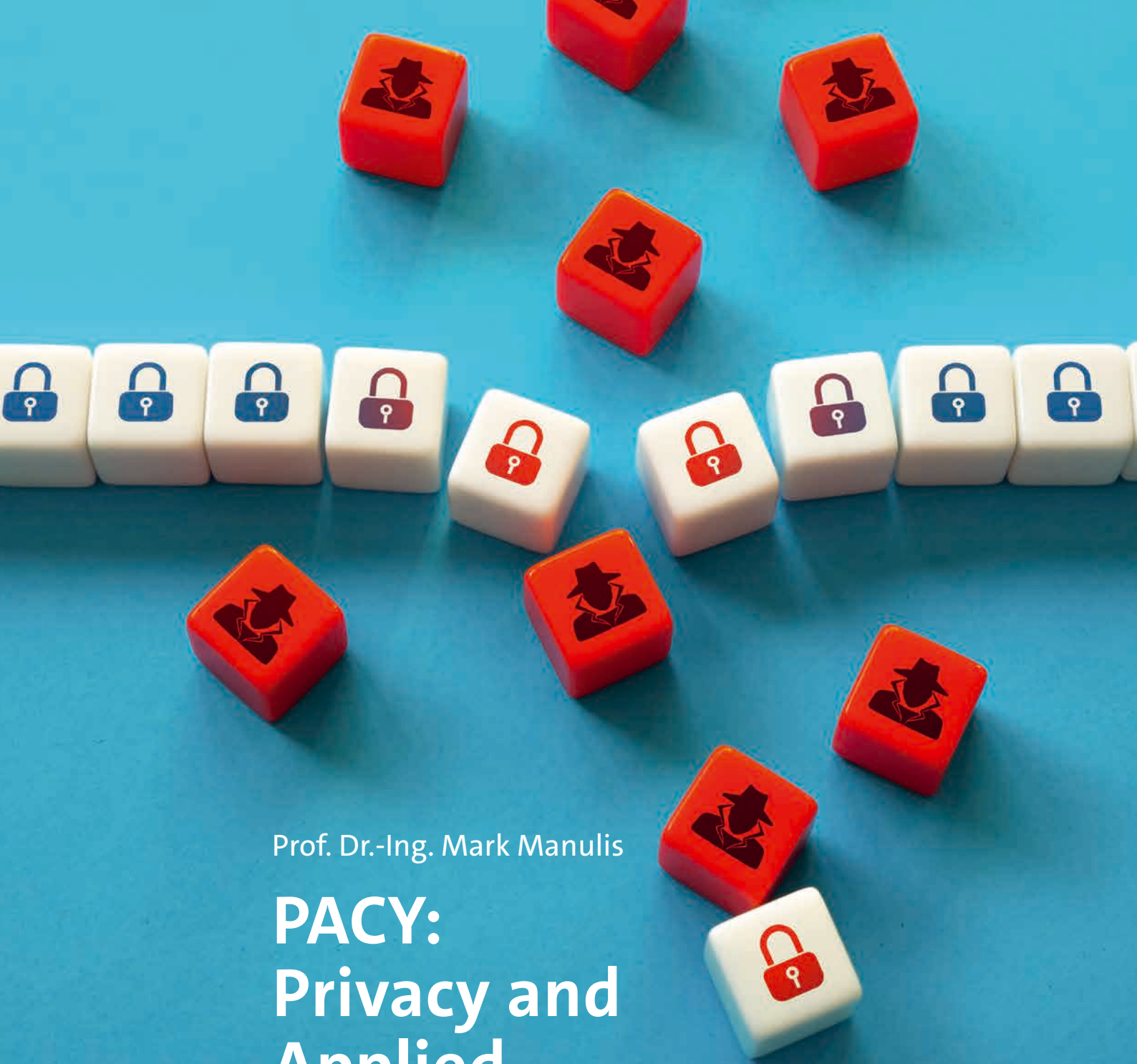
Machine learning promises a new generation of more powerful tools for function identification. Existing approaches face two fundamental problems, however: They can only generate function names that have been seen in the training set; and each such function name represents a separate output class, with the number of possible function names being essentially unbounded. Our solution to this problem is to split function names into meaningful tokens. For instance, a function named make_smooth_colormap would correspond to the set of labels {make, smooth, color, map}. The total number of labels can be controlled such that each function has at least one descriptive label but there are also sufficiently many samples available per label. We therefore arrive at the problem of assigning a set of labels to each function.

Extreme Multi-label Learning

A similar problem is that of tagging text with a set of relevant labels, which motivates multi-label learning and extreme multi-label learning (XML), where the number of labels is very large. We show how to leverage state-of-the-art algorithms from XML for labeling functions in stripped binaries with XFL (eXtreme Function Labeling). XFL is parameterized by a given function embedding, which maps each binary function to a vector representation. While XFL is compatible with state-of-the-art binary code embeddings – such as PalmTree, SAFE, and Asm2Vec – we also designed and implemented DEXTER, a novel function embedding. DEXTER is trained from a vector of per-function features combined with vectors capturing the context of the local call graph and of the whole binary. While this partly manual feature engineering runs counter to current trends in machine learning, we demonstrate that it is highly effective for the XFL task, providing further evidence that semantic preprocessing of code can improve over syntactic language models. In an extensive evaluation on a dataset with 741,724 functions from 10,047 binaries, we demonstrate that our implementation significantly outperforms the state of the art. We describe XFL and its evaluation in an article we will present at the 44th IEEE Symposium on Security and Privacy (S&P), a premier forum for computer security research.

Moritz Dannehl, M.Sc.
moritz.dannehl@unibw.de
+49 89 6004 7333
https://go.unibw.de/bm

FIG.: RI CODE



Prof. Dr.-Ing. Mark Manulis

PACY: Privacy and Applied Cryptography Lab

PACY Lab, led by Prof. Dr.-Ing. Mark Manulis, holder of the Professorship of Privacy, researches technologies for improving privacy based on modern cryptographic methods. The focus is on the design, analysis, and development of cryptographic methods for the protection of users, data, and messages as well as their practical use in web, cloud, IoT, and blockchain applications.

Privacy and Applied Cryptography Lab

PACY Lab, led by Prof. Dr.-Ing. Mark Manulis, holder of the Professorship of Privacy, researches technologies for improving privacy based on modern cryptographic methods. The focus is on the design, analysis, and development of cryptographic methods for the protection of users, data, and messages as well as their practical use in web, cloud, IoT, and blockchain applications.

Research Foci at the PACY Lab

PACY Lab was established in March 2022 and is part of the RI CODE. Its research staff has in-depth knowledge of cryptography, computer science, and mathematics, which they successfully use for foundational and applied research.

The lab explores methods and technologies in the area of Privacy Enhancing Cryptography (PEC), which includes all sorts of cryptographic schemes with extended requirements on confidentiality and privacy.

PACY Lab focuses on the design and practical use of various PEC methods, including advanced encryption and signature schemes and relevant cryptographic protocols. The lab works on modeling and an analysis of their functional properties and protection goals. Dependencies between methods and properties are explored to improve their general understanding and identify new design strategies. PACY Lab develops new PEC procedures and uses them to develop cryptographic protocols for authentication and access control, processing of data and transactions, and secure messaging.

In the design and implementation of new PEC approaches, PACY Lab deploys mathematical techniques that are commonly used in cryptography, such as elliptic curves and bilinear maps, and now, more increasingly, techniques from lattice-based cryptography in order to realize the desired security against future quantum computers. Other PEC techniques used at PACY Lab include secret sharing and zero-knowledge proofs.

PEC for Data: Access control and data processing

Traditional encryption methods can provide data confidentiality but cannot be used directly for processing encrypted data. Modern PEC methods allow a variety of operations on encrypted data without having to decrypt it during processing. PACY Lab is working on functional encryption schemes offering better flexibility in access control and data exchange as well as enabling direct processing of encrypted data in distributed multi-user applications. This includes approaches for homomorphic encryption and attribute-based encryption as well as cryptographic protocols supporting operations (e.g., search queries) on encrypted data, along with their use in distributed applications.

PEC for Users: Authentication and message exchange

Digital signatures form the backbone of modern PKI. With them, users can authenticate themselves or establish end-to-end secure communication channels. The verification of PKI-based signatures reveals a lot of sensitive information, such as identities, public keys, and all attributes. PACY Lab is researching advanced signature techniques to combine authentication with anonymity or untraceability. Current research includes hierarchical attribute-based signature schemes for building privacy-protecting PKIs, group signatures, and related anonymous credentials schemes. In addition, PACY Lab is researching security protocols for private messaging in dynamic groups that ensure privacy as well as end-to-end encryption. Protocols for distributed and delegable authentication, for example, in connection with the new FIDO2 standard for web authentication, are also the subject of ongoing research.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

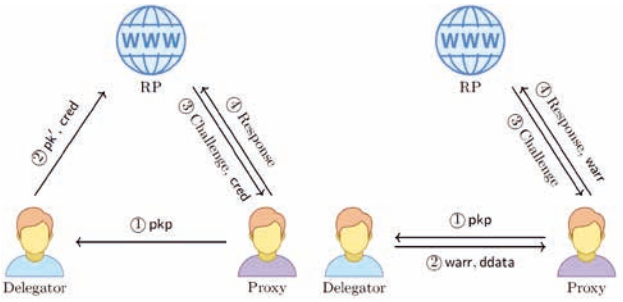
www.unibw.de/pacy

FIG.: ADOBE STOCK / A. YALANSKYI; RI CODE

Delegation of Access Rights in WebAuthn / FIDO2

Strong Authentication with Delegation Capabilities for Private Web Accounts

In the latest standard for web authentication, passwords and one-time codes are replaced by cryptographically secure digital signatures that can only be created with suitable private keys. These keys are managed by hardware-based security keys held by users who own the accounts. This project is about creating new mechanisms for users to securely delegate access rights to their web accounts to other people.



Approaches for delegation in WebAuthn.

WebAuthn and Backup of Security Keys

The WebAuthn standard (also known as FIDO2), which has been in development since 2019, is intended to make user authentication in web services both more secure and more user-friendly. The standard is already widely used. Unlike less secure authentication methods, such as passwords or one-time codes, WebAuthn relies on digital signatures. WebAuthn also improves user privacy – an independent key pair is used for each web account, so different web accounts of one user cannot be linked to each other. The user's cryptographic key pairs for their web accounts are managed by hardware-based authenticators, also called security keys. Their loss would lock the user out of their accounts. In 2020, PACY Lab and its cooperation partner Yubico have already developed a standards-compliant solution allowing users to back up their security keys. Part of this solution was ARKG, a new protocol for asynchronous distributed generation of cryptographic key pairs consisting of a private and a public key.

Delegation of Access Rights with Security Keys

In 2022, PACY Lab addressed another problem, namely, how to delegate access to own web accounts to other users via WebAuthn without losing security and privacy. The problem is that the other person may not have any web account with that web service at all. And, unlike passwords, which could be shared in an emergency, cryptographic keys cannot be exported or shared for security reasons. We have succeeded in solving this problem in an elegant and standards-compliant way based on ARKG.

Two approaches to delegating access rights in WebAuthn were developed. In the first approach (shown on the left in the image), the owner of the web account configures the access rights directly with the web service. As part of this process, certain cryptographic credentials – a public signature key generated by ARKG as well as auxiliary data – are uploaded to the web service using the security key of the account owner. When the other authorized person accesses remotely, these credentials are processed by that person's security key to compute the appropriate private signing key and create the signature for the access. The second approach (shown on the right in the image) is to forward the required credentials directly to the other person's security key without the owner having to upload them to the web service. This approach is based on a new class of proxy signatures that offer additional privacy properties when compared to previously known proxy signature constructions.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

FIG.: RI CODE / M. MANULIS

Privacy-protecting Digital Signatures and PKI

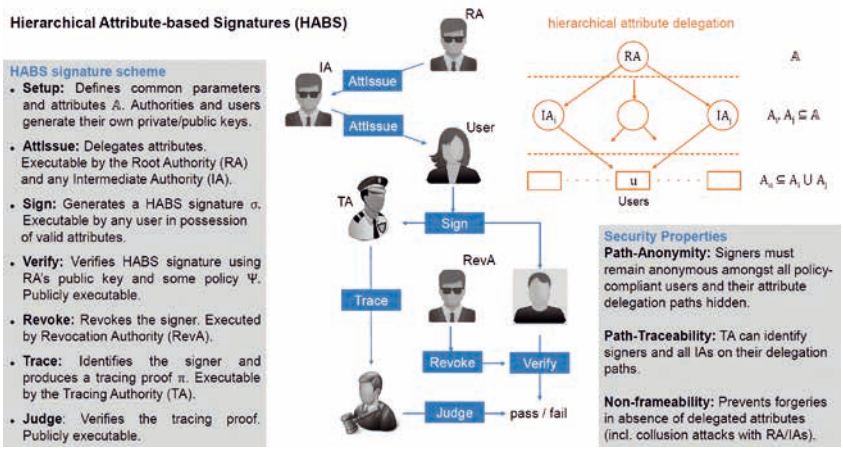
Anonymous Issuance of Digital Signatures and Their Verifiability Based on Properties and Rights

Digital certificates used in modern public key infrastructures are cryptographically linked to user identities, which cannot be disguised during the verification of certificates. For a better protection of privacy, new signing methods are being developed in this project, allowing to verify issued signatures with respect to the properties and rights of otherwise anonymous signers.

Privacy Problems in Modern Public Key Infrastructures

Digital signatures and certificates (in accordance with the X.509 standard) form the backbone of modern public key infrastructures (PKI) and are used in many ways. They provide authentication and thus protection against impersonation and man-in-the-middle attacks in numerous IT security protocols and applications, including protection of email messages, documents, and in identification and access control procedures. X.509 certificates contain information about their holders, such as public keys, identities, and other properties, all of which can be read and verified during signature verification.

In applications that are only geared towards verifying certain rights and properties of the certificate holders, such as in role- or policy-based authentication and access control procedures, X.509 certificates and modern PKI do not offer sufficient protection of privacy. Attribute-based signatures (ABS) were developed precisely for such scenarios. They offer improved privacy protection for certificate holders by keeping all properties (attributes) secret during verification and only disclosing whether the set of used attributes meets the verification criteria. Because these criteria can potentially be met by a variety of different individuals with appropriate attributes, each individual's privacy, such as keeping their own identity secret, is greatly enhanced. ABS schemes nevertheless offer the possibility to reveal the signer's identity in a controllable way in order to detect any occurred abuses.



Hierarchical attribute-based signatures.

Hierarchical Attribute-based Signatures

PACY Lab is researching ABS constructions enabling realization of privacy-protecting PKIs. For this purpose, it is necessary to expand the functionality of existing ABS schemes with regard to hierarchical management of ABS certificates in order to bring them closer to the hierarchical structure and functionality of classic PKIs. The first hierarchical ABS schemes were already presented by members of the PACY Lab in 2018 and have been continuously developed since then. In 2022, the first realization of hierarchical ABS was presented using lattice-based cryptographic techniques, which are assumed to provide the desired level of security against future quantum computers. In addition, this new scheme allows certification authorities that are organized into a hierarchy to revoke any previously issued ABS certificates by means of a specially developed verifier-local-revocation procedure.

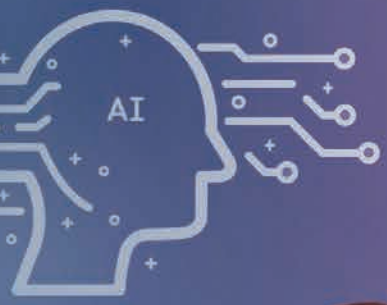
Prof. Dr.-Ing. Mark Manulis
+49 89 6004 7365
mark.manulis@unibw.de
www.unibw.de/pacy

FIG.: RI CODE / M. MANULIS

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

The Artificial Intelligence and Machine Learning (AIML) group, established in August 2022 by Prof. Dr. Eirini Ntoutsi, aims at developing artificial intelligence and machine learning methods that address real-world challenges and promote the social good.



THE ARTIFICIAL INTELLIGENCE and Machine Learning (AIML) group develops new AI/ML methods that address real-world challenges, such as non-stationarity and data scarcity, while promoting trustworthy decision-making. Ongoing research directions include: a) continuous learning over evolving data, b) trustworthy AI (including fairness-aware and explainable AI), and c) Generative AI for new data and solutions.

Continuous Learning

Dynamic environments with continuously arriving data and changing characteristics, such as communication networks, electric power grids, and production processes, are the sources of many interesting applications. Our focus is on developing intelligent algorithms that learn continuously from data, taking into account resource constraints such as memory and response time, much like how humans learn cumulatively. Our research questions address how to update ML models with new data, handle outdated or erroneous data/models without catastrophic forgetting, adapt to evolving feature spaces, and monitor and explain changes over time.

Trustworthy AI

AI-based systems are widely employed nowadays to make decisions that have far-reaching impact entailing concerns about potential human rights issues. To ensure that these systems benefit society, it is essential to move beyond traditional algorithms optimized for predictive performance and integrate ethical and legal principles into their design, training, and deployment. One area of focus is fairness-aware learning, which involves creating ML models that do not discriminate based on protected attributes such as gender, ethnicity, or age. We study methods for multi-fairness, multi-task fairness, and the intersection of fairness with other data challenges, such as class imbalance. Another area of interest is explainable AI (XAI), which helps end-users understand AI-based decisions and helps designers build more robust models. We focus on counterfactual explanations, explanations for sequential and stream data, and modeling uncertainty in explanations.

Generative AI

AI is no longer limited to analyzing historical data; it can now generate new content, including text, images, and tabular data. Generative AI can benefit society by helping engineers design better products, creating new products, and even writing books. However, like any technology, there are downsides, including security issues, biased content, copyright concerns, and creativity limits. One area of interest is using generative AI to address data challenges, such as data scarcity and lack of representative data. Another area of interest is generating real-world structures, such as wind turbines, by combining simulation models, analytical models, and data-driven models.

Development of the Research Group

The group will be expanding with new PhD students and postdocs joining in Munich in 2023, while some members will remain in Berlin (at the Free University of Berlin) and Hannover (at the Leibniz University/L3S Research Centers), where Prof. Ntoutsi was previously affiliated. In 2022, the group's third-party funding portfolio grew with two new EU projects: MAMMOth, focused on fairness-aware machine learning for complex data, and STELAR, focused on AI methods for smart agriculture.

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

https://go.unibw.de/aiml

FIG.: ADOBESTOCK / PARRADEE, PINKEYES

Project MAMMOth

Multi-attribute, Multimodal Bias Mitigation in AI Systems

MAMMOth focuses on developing tools and techniques for the discovery and mitigation of (multi-)discrimination to ensure the accountability of AI systems for multiple protected attributes and for traditional tabular data and more complex network and visual data.

AI Discrimination

AI-based decision-making offers big opportunities for automation in different sectors and daily life, but at the same brings risks for discrimination of minority and marginal population groups on the basis of the so-called protected attributes such as gender, race, and age. Fairness-aware ML develops methods for bias detection and mitigation. However, the proposed methods work in limited settings and under very constrained assumptions, and they do not reflect the complexity and requirements of real world applications. To this end, MAMMOth focuses on multi-discrimination detection and mitigation for tabular, network, and multimodal data. The developed solutions will be demonstrated in: a) finance/loan applications, b) identity verification systems, and c) academic evaluation.

Main Objectives

- Fairness definitions and bias mitigation methods that move beyond the simple setting of a single protected attribute to many protected attributes.
- Recognition of bias in network data, e.g., as a result of the inequalities that arise from the different positioning of individuals in the context of an underlying network of connections or interactions.
- Recognition of bias in multimodal data, with an emphasis on visual media, where different forms of bias, often hard to measure, emerge and may affect the performance of critical AI systems (e.g., face verification) or could be the reason for perpetuating and diffusing harmful behaviours online (e.g., through images that target in a stereotypical and harmful manner specific marginalized communities).
- Explainability methods that account for the above complexities of AI systems.

A multi-disciplinary team of computer scientists and AI experts together with social scientists and ethics experts as well as numerous communities of vulnerable and/or underrepresented groups in AI research will work together to make sure the actual user needs are at the center of the research agenda.

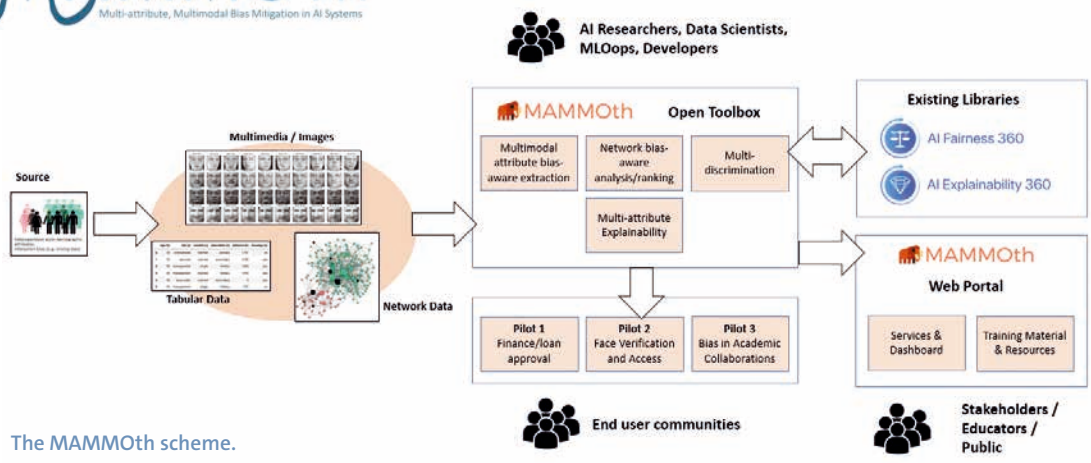
Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

https://mammoth-ai.eu/

Funded by: EU H2020



The MAMMOth scheme.

FIG.: MAMMOTH PROPOSAL (2)

Collaborative Research Center 1463

Integrated Design and Operation Methodology for Offshore Megastructures

The Collaborative Research Center (CRC) researches the design and operating conditions of offshore megastructures of the future, whereby the complete life cycle of a structure can be represented, from planning and manufacturing to operation, dismantling, and recycling.

Offshore Wind Turbines of the Future

Modern offshore wind turbines (OWTs) are expected to make a significant contribution to the success of the energy transition. Future turbines will be significantly larger than today's: over 300 meters in total height and with rotors more than 280 meters in diameter. This means that they will be subject to hardly any known effects or conditions that can develop at heights of over a hundred meters. Due to their dimensions and the more filigree design required for them, environmental influences as well as interactions between individual components become more relevant. Today's established methods for the design and operation of wind turbines are no longer applicable to structures of this size. Therefore, new concepts for offshore megastructures are being developed in the CRC 1463.

Offshore wind turbines.

FIG.: UNSPLASH / N. DOHERTY; SFB1463

Subproject B1: Integrated design process for offshore structures

Our group is part of Subproject B1, which aims at improving the design of OWT support structures, one of the main cost drivers for OWTs traditionally designed by engineers based mainly on its operational behavior.

Main Objectives

- Developing an integrated design methodology that considers the entire life cycle of OWTs.
- Developing ML models that can predict the quality of a design, taking into account the complete life cycle and the experience and intuition of the engineers.
- Providing actionable feedback to the engineers using explainable AI (XAI), for example, in the form of feature attributions or counterfactual explanations.
- Generating new offshore structure designs.

Main Challenges and Methodology

- Data sparsity, as there are only a few instances of real OWTs and do these not cover the various phases of the life cycle. To this end, we combine traditional evolutionary approaches with generative AI methods.
- Label acquisition regarding existing real and synthetic designs. To this end, expert feedback will be collected, taking into account human label variation and label scarcity.
- Evaluation of new designs considering the entire life cycle. To this end, a multi-objective optimization approach is followed, leading to a set of Pareto optimal solutions.
- XAI methods to provide actionable insights to the engineers and understand the trade-offs between the different solutions.
- Creativity of new generated designs: Can AI generate novel, unexpected, and yet useful designs?

SFB Offshore-Megastrukturen

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

https://www.sfb1463.uni-hannover.de/

Funded by: DFG

Prof. Dr. Arno Wacker

Privacy and Compliance

Don’t just teach data privacy and compliance, live it!

ONE OF OUR MOST IMPORTANT GOALS is not only to research and teach data privacy and IT security, but also to bring it into everyday life. In this way, complex topics could be communicated in a persuasive and authentic way to the students. Additionally, we also want to demonstrate to the public that technologies that support data privacy can be integrated in everyday life, in private life as well as in business.

Teaching

In the professorship, teaching is divided into penetration testing, data privacy, privacy-enhancing technologies, cryptology, and secure networks and protocols. This teaches the students what privacy is and why it is important, not only for the individual but also for a democratic society. Penetration testing deals with the examination of single systems, complex IT services, and IT infrastructures, as well as real-world attacks oriented on documented established good practice. The fundamentals of cryptography and knowledge about methods for secure data communication in modern communication networks are imparted.

Research

A special focus of the professorship is on methods and mechanisms that support privacy and data privacy. These are subdivided into three different research areas:

- Privacy supporting mechanisms have the goal of strengthening the privacy of the individual as well as the communication rules for the age of the Internet.
- Increasing IT security awareness is concerned, among other things, with the area of personal data protection. For this, the professorship develops and researches, among other things, methods and tools for increasing security awareness in the development of software tools and in their use.
- Cryptoanalytics of classic ciphers examines the field of classic encryption methods with the help of modern (meta-)heuristic techniques. With this, not only the effectiveness of the analysis but also the security of the algorithms are examined.

FIG.: ISTOCK / MATEJMO, M. BUHLINGER

Knowledge Transfer

An important objective of our professorship is to educate, enlighten, and inform interested citizens about issues related to IT security. This task is achieved with the help of presentations and workshops that, for example, deal with the topics of penetration testing, secure email correspondence in everyday life, and the reconstruction of security breaches.

Prof. Dr. Arno Wacker
arno.wacker@unibw.de
+49 89 6004 7325
www.unibw.de/datcom

CrypTool

CrypTool at Privacy and Compliance as of 2023

The goal of the CrypTool project is to develop the e-learning application CrypTool for the fields of cryptography and cryptanalysis. With the help of CrypTool, many cryptographic methods can be applied and analyzed in order to practically illustrate basic and advanced concepts of cryptology to the user.

Cryptography also plays an increasingly important role in everyday life.

THE PROJECT includes, among other topics, CrypTool2 and JCrypTool, several actively developed programs for the PC, and the Internet service CrypTool-Online. All in all, CrypTool offers an exciting insight into the world of cryptology. A variety of ciphering methods as well as coding and analysis tools are presented in a simple way and enhanced by examples. The emphasis is on an understandable explanation, which should arouse interest in cryptography and cryptanalysis. Many of the methods presented can be tried and experimented with directly in the program or on the website itself.

In a short time, interested people can learn how historically significant cryptographic methods work and encrypt texts themselves with the tools offered. For example, one can take a look at the modern cipher AES or have good passwords generated. For people who want to go a little deeper, CrypTool also offers options for decrypting and analyzing cipher texts, for example, to find weak points in a cipher.

History

The development of CrypTool began in 1998 as part of an IT security initiative for in-company training at Deutsche Bank. From 2000, CrypTool was made available as freeware and, for example, distributed on the German Federal Office for Information Security's (BSI) publicly available CD "Sicher ins Internet" in 2002. After three years as freeware, CrypTool finally became an open source project in 2003. While companies and universities were already using CrypTool as freeware, it was only through open source that the direct participation and integration of volunteer developers became possible. The open-source approach improved cooperation with universities in particular. As a result, numerous extensions to CrypTool were and are being developed as part of seminar papers or diploma theses.

The Professorship of Data Privacy and Compliance at the University of the Bundeswehr Munich, headed by Prof. Dr. Arno Wacker, has supported the CrypTool project for many years and, among other things, provides the infrastructure required for the website.

Starting in 2023, the leadership of the project will be transferred from Prof. Dr. Esslinger (University of Siegen) to Prof. Dr. Wacker (University of the Bundeswehr Munich).

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

FIG.: ISTOCK / NICOELNINO

Trusted Platform Module (TPM)

TPM Communication Within Windows 11 and Linux

TPMs can protect data from unauthorized access without the user having to deal intensively with the security mechanisms behind them. However, this requires the operating system to fully support these mechanisms.

TO PROTECT SENSITIVE DATA, it is often stored on data carriers in encrypted form. In order to gain access, decryption is then required. Typically, this is possible by entering the corresponding key (password) via the keyboard.

A Trusted Platform Module (TPM) in the form of a separate component on the motherboard can securely store the key and communicate it to the main processor for decryption via a data bus. Under Windows, the BitLocker software uses the TPM to protect the data in the specified way. With TPM 2.0, it is possible to only transmit the key in encrypted form and furthermore to confirm the request for the key in advance with a PIN.

Last year, the DOLOS Group discovered that the TPM transmits the key in plain text under Windows 10. This was not surprising since the specification did not allow encrypted communication via the data bus until TPM version 1.2. With version 2.0, support for encrypted communication over the bus was added.

Since Microsoft requires the presence of a TPM in version 2.0 with Windows 11, it was assumed that this attack vector would be restricted by the encryption. However, this is not the case. Even with Windows 11, the key is still transmitted in plain text. Microsoft is aware of this and recommends the use of an additional PIN, which is entered by the user. But even with this, the parameter encryption remains unused. The key is still transmitted in plain text via the data bus.

Furthermore, the TPM-based encryption is analyzed with the Linux Unified Key Setup (LUKS) as used by systemd. Up to version v250 of systemd, neither a PIN nor parameter encryption is supported. Under version v251, both options are implemented and parameter encryption is mandatory, which greatly limits the attack vector.

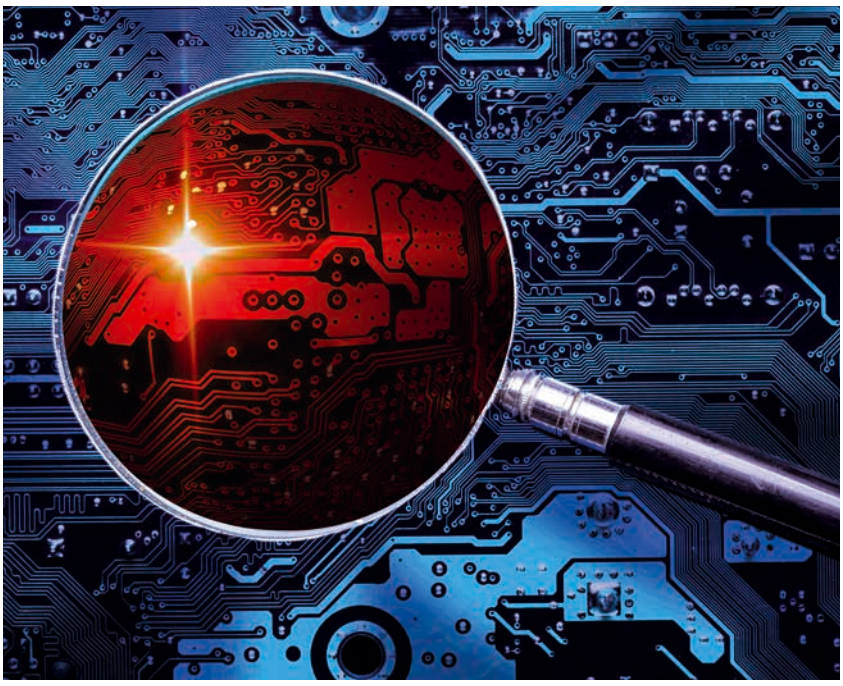
The protection of the data is thus largely given under Linux with the current systemd. However, this is still not the case under Windows. Not only do users have to activate the protection themselves the security is also not significantly increased. The project is therefore investigating measures to increase the security of the data despite physical access, taking usability into account.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom



TPMs protect against prying eyes.

FIG.: ISTOCK / ELEN11

Hon.-Prof. Dr. Udo Helmbrecht

Quantum Communication

Within the framework of dtec.bw, the MuQuaNet project is constructing a quantum network in the Munich metropolitan area in cooperation with partners in academia and industry. The goal is to test and research the operations of a quantum communication network with selected civil and military applications.

Insights into the MuQuaNet Laboratory

Quantum-secure Communication in Practice

The MuQuaNet project is constructing a quantum network in the greater Munich area. In June 2022, the latest QKD devices were delivered, which will connect two buildings on the UniBw M campus as of next year. The devices are currently being extensively tested in the MuQuaNet lab. As part of the study of military use cases of QKD, a robot was controlled remotely using quantum-safe communication.

QUANTUM KEY distribution (QKD) enables provably secure exchange of symmetric keys, so-called quantum keys. While the functionality of QKD is often explained, the practical side of what a QKD device looks like from the inside, or how an experimental setup for quantum-safe encryption is designed, usually remains hidden. Therefore, this article gives insights into the laboratory of MuQuaNet.

Quantum Keys in Action

This year, the quantum-safe remote control of a robot was demonstrated using entanglement-based QKD.

For this, a control PC (called "Alice") and a robot (called "Bob") were each connected to a receiver for photons. A photon source located between Alice and Bob distributes entangled qubits to the two receivers.

The receivers analyze the photons and generate a secure key based on a QKD protocol. However, in order to use the key for encrypted communication, Alice and Bob have to request it from their receivers. The transmission of the quantum keys is currently cable-bound, since QKD devices cannot be integrated into end devices yet.

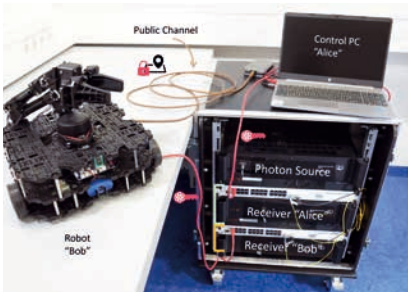
Therefore, the MuQuaNet project develops miniaturized QKD devices in cooperation with LMU.

Development of Miniaturized QKD Devices

In order for QKD to become more widespread as a technology, the devices used must become smaller and cheaper. The miniaturized QKD devices developed within the project will be used to realize a free-space link between the cooperation partner Airbus and the UniBw M faculty ETTI.

The transmitter module shown in the picture is able to prepare the required quantum states for a polarization-based decoy-state BB84 protocol. The module can be connected to a PC via USB-C and is thereby also supplied with power. The transmitter module measures around 11 x 11cm² and weighs approximately 200 g including micro-optics in a silver colored Kovar case. This high level of integration allows the transmitter to be used in many applications.

Compact transmitter electronics in a 3D printed case.



A photon source distributes entangled photons to the two receivers via the fiber-optic cables. The receivers analyze the light particles and generate a key from them. The control PC and the robot can request a quantum key from their local receiver via the red Ethernet cables. The keys can be used to remotely control the robot in a quantum-safe manner via the public channel.

Hon.-Prof. Dr. Udo Helmbrecht
udo.helmbrecht@unibw.de
+49 89 6004 7308
www.unibw.de/muquanet

Funded by:
dtec.bw
Funded by the European Union
NextGenerationEU

FIG.: TAUSENDBLAUWERK.DE / M. KRÄMER; RI CODE / M. AUER, S. KASTRUP

Jun. Prof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

Jun. Prof. Moll's research focuses, on the one hand, on reinforcement learning, where he is particularly interested in the possible combinations with classical operations research as well as the applications in prescriptive analytics and prescriptive intelligence. On the other hand, he is researching the interfaces of quantum computing with optimization and machine learning.

Quantum Computing Environment Study

The media and economic interest in the new technology of quantum computing is growing steadily. However, applied research in this area is still relatively in its infancy, and in many areas, it is not clear how and from when corresponding techniques and algorithmic optimization processes can be used. The Deutsche Bundesbank, Germany's central bank, has taken a first step with Accenture and scientific support.

Quantum Computing – Machine Learning: Research & Application

The rapid development of machine learning has already shown that increased computing power can be a good catalyst. In the last 5 years, quantum computing has also made its way from pure theory to algorithm- and application-oriented development. This novel technology is attracting more and more attention, especially with the wide availability of the first hardware.

RI CODE: Central role in the German research landscape

Since 2018, the Research Institute CODE has played a key role as the first hub in IBM's network in Germany, as its researchers had early access to the latest hardware. The speed at which the size and quality of individual processors is growing makes this an essential advantage in research.

NISQ Era

For meaningful applications, this growth is essential because quantum computing is currently in the NISQ era, where only medium-sized, error-prone processors exist. Developed solutions must therefore be able to deal with low computing power and imprecise results.

Deutsche Bundesbank as Pioneer

Because of the fundamental differences to classical computer science, it is important for companies to address the potential for quantum computing early on. The Deutsche Bundesbank has embraced its pioneering role here and has commissioned a corresponding study from Accenture.

Optimization Potential and Intelligent Benchmarking

Research Institute CODE, represented by Maximilian Moll and Stefan Pickl, was part of the scientific support. In this context, RI CODE developed well-founded assessments for the applicability, possible benchmarks, and the time horizon of quantum computing for banks in general and the Bundesbank in its supervisory function. In 2010, the COMTESSA research group had already established initial contacts with IBM in Rüschlikon, Switzerland, in this subject area in order to evaluate OR applications and optimization potentials in particular.

Quantum computer IBM Q System One.

FIG.: ADOBE STOCK / TIERNEY

Use Cases & Recommendations

To prepare the Bundesbank, RI CODE set up an overview of hardware, OR-related algorithms, and the research landscape in Germany. However, a much more central task was the elaboration of concrete use cases that the Bundesbank helped to identify. For each use case, the team assessed urgency, the added value of quantum technologies, and the algorithms to be used.

The final step involved working out, a development time line that clearly and plausibly shows the competencies to be trained as well as the appropriate team sizes and constellations required for sustainable development in the quantum sector.

Jun. Prof. Dr.
Maximilian Moll

maximilian.moll@unibw.de

+49 89 6004 2248

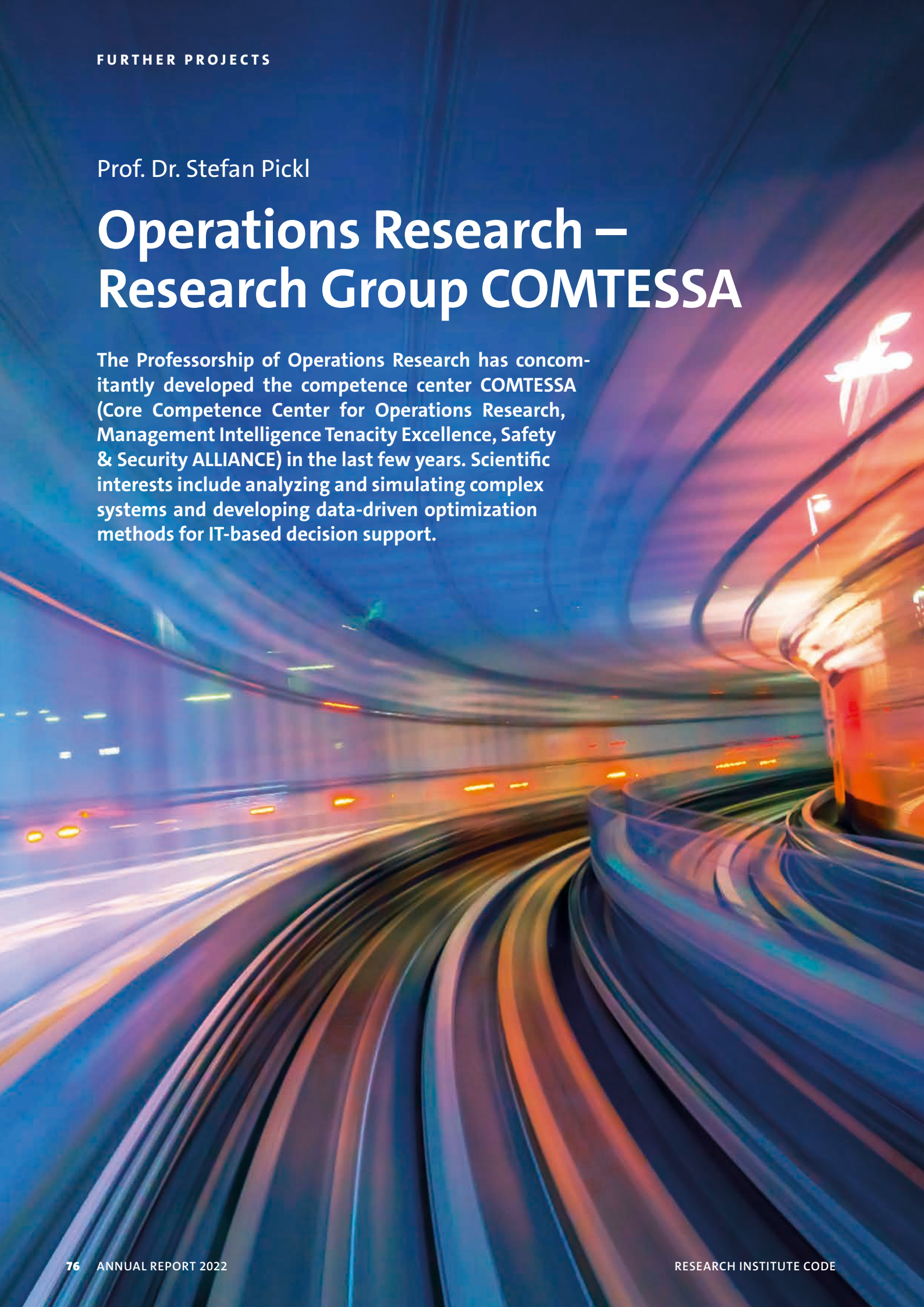
https://www.unibw.de/comtessa

Cooperation partners:
Deutsche Bundesbank & Accenture

Prof. Dr. Stefan Pickl

Operations Research – Research Group COMTESSA

The Professorship of Operations Research has concomitantly developed the competence center COMTESSA (Core Competence Center for Operations Research, Management Intelligence Tenacity Excellence, Safety & Security ALLIANCE) in the last few years. Scientific interests include analyzing and simulating complex systems and developing data-driven optimization methods for IT-based decision support.



REAVRS Project

Identifying Existing Attack Potentials for the Railroad System

Due to the increasing applications of big data, IT, etc., the rail system is more vulnerable to attacks from the outside. A general approach for uniform attack security has not yet been established. REAVRS identifies potential dangers in the railroad system in order to develop intelligent measures against both physical and cyber dangers.

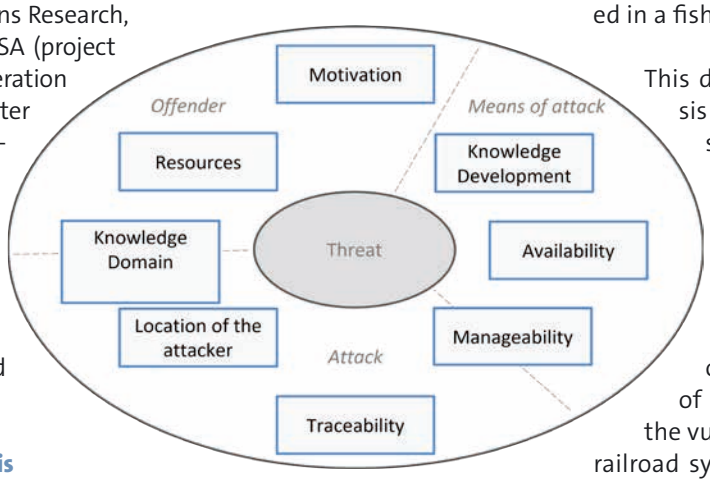
THE AIM OF REAVRS – a research project of the German Centre for Rail Traffic Research (DZSF) – to characterize and analyze the current vulnerability of the German railroad system. The partners are the University of the Bundeswehr Munich, Faculty of Computer Science – Institute 1, Chair for Operations Research, Research Group COMTESSA (project management) in cooperation with the Research Center CODE, the Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH), Crea-Lab GmbH, and TU Braunschweig's Institute of Transportation, Railway Construction and Operation (IVE).

OR-based System Analysis

The project focuses on a detailed system definition. This involves developing a functional mapping of the (German) railroad system, followed by precisely characterizing and analyzing attacks that have occurred and describing the corresponding contexts. The project also systemizes attack opportunities and threat scenarios and uses an OR-based system analysis to identify threats.

Cyber-vignettes and Attack Scenarios

After pre-selecting potential attack points, these are developed into exemplary model vignettes. By systematizing the means of attack,



Identification of parameters for the threat.

more than 500 physical and nearly 1000 possible cyber attacks have been identified. A root cause analysis of these is performed with a selection of representative vignettes. The final step involves embedding the developed methodology is embedded in a convenient IT-based decision support environment and innovative management cockpit.

Identification of Parameters

When looking at the vignettes in more detail, the parameters shown in the figure above can be derived.

Automation, Overall Situation and Management Cockpit

After identifying the threat metrics, the values from 1 to 5 are assigned to each threat metric (from barely threatening (1) to highly threatening (5)) and the results are illustrated in a fishbone diagram.

This detailed root cause analysis is incorporated into the subsequent complex risk analysis. Currently, an automated version of the threat model as well as a supporting management cockpit are being developed in order to develop a picture of the situation regarding the vulnerability of the German railroad system and to prepare the integration of a "Safety & Security" living lab at the House of Logistics and Mobility (HOLM) for security analysis.

Prof. Dr. Stefan Pickl

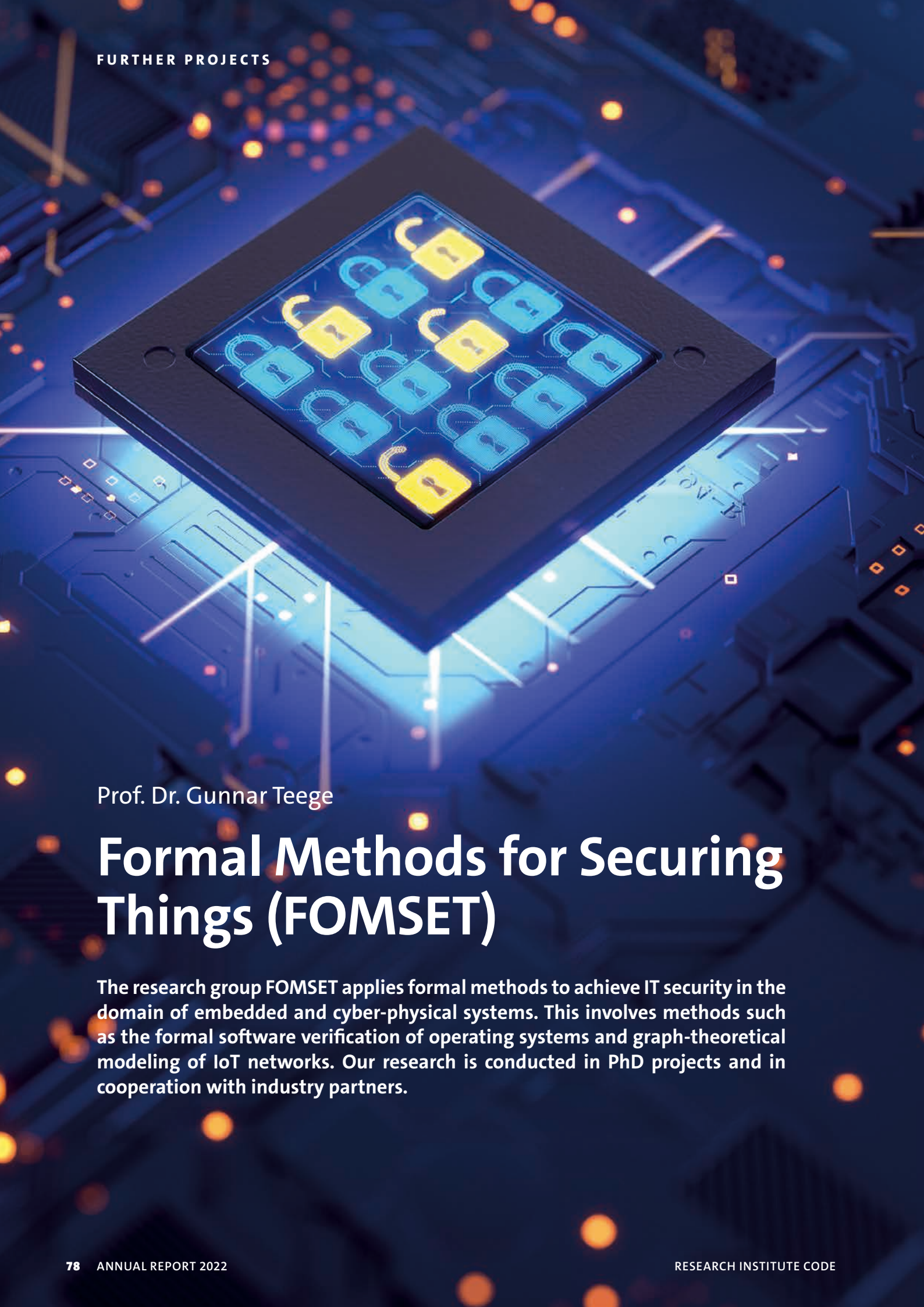
stefan.pickl@unibw.de

+49 89 6004 2400

www.unibw.de/comtessa/forschung/reavrs

Funded by:
German Centre for Rail Traffic Research (DZSF)

FIG.: ADOBE STOCK / NAKA; PICKL S., BUCHETMANN B., ALONSO VILLOTA M., LORETH T. UNIVERSITÄT DER BUNDESWEHR MÜNCHEN; SIEFER T., STUTE F. TU BRAUNSCHWEIG; JELINSKI M. IVE MBH, HANNOVER; NEUBECKER K. A., SCHMITZ W. CRE-ALAB GMBH, FELDKIRCHEN-WESTERHAM



Prof. Dr. Gunnar Teege

Formal Methods for Securing Things (FOMSET)

The research group FOMSET applies formal methods to achieve IT security in the domain of embedded and cyber-physical systems. This involves methods such as the formal software verification of operating systems and graph-theoretical modeling of IoT networks. Our research is conducted in PhD projects and in cooperation with industry partners.

Mathematics Provides Security

Applying Formal Software Verification to Real-world Software Development

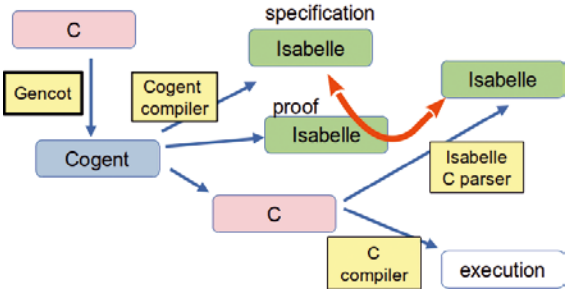
The security of software-based systems is hampered by programming errors. Formal software verification has the potential of changing this. However, this requires an extreme effort for real-world programs, such as especially security-critical operating systems. In their projects HoBIT und SW_GruVe projects, the team of the research group has joined forces with an industrial partner to increase the level of automation of formal verification and bring it closer to practical application.

SYSTEMS AND DEVICES with embedded information technology (IT) are only as secure as the operating system (OS) used as the basic building block on top of the hardware. The OS kernel runs in the most permissive hardware mode and, if compromised, it can alter the behavior of every hardware and software component in the system. To mitigate this menace, the system components in microkernel-based OS are strictly separated from each other.

But programming errors in the components can still directly lead to unwanted behavior or they can be exploited to attack and control the kernel. The best defence against errors is a formal proof that the program code does not contain any errors. The seL4 microkernel has already been successfully formally verified, but the required effort was enormous. Other system components may be of substantially larger size, so it is currently impracticable to prove that the system is free of errors in commercial development.

Formal Verification

Formal software verification develops a mathematical proof that a program behaves according to an abstract mathematical specification. Since the proofs are much more complex than the programs themselves, it is crucial to use computer support for their development. Such support is provided by proof assistant systems such as Isabelle or Coq.



Gencot translates from C to Cogent and makes formal verification easier.

Formal verification works best if a program is written from the beginning with this goal in mind, possibly in a high-level language suitable for formally proving its properties. For the Cogent language, developed by an Australian research group, the compiler together with the executable code generates the abstract specification and a proof that the code behaves as specified.

In reality, OS components are most often written in C, which is a low-level language and rather ill-suited for formal verification. Still, in December 2022, C finishes second in the Tiobe index of the most used programming languages. Therefore, the formal verification of C code is highly relevant for the software industry

Projects HoBIT and SW_GruVe

The two projects, HoBIT and SW_GruVe, aimed at improving the practical applicability of formal verification to C code. To achieve this, the researchers developed the tool Gencot for a largely automatic translation from C code to Cogent. The correctness of the translation is not proven. Hence, it is not 100 % certain that the resulting Cogent program does the same as the original C program. However, one does obtain a provably correct, abstract specification of its behavior. As a proof of concept, Gencot has been successfully applied to components of the TRENTOS OS. The C code of these components has been provided by the developers of the project partner Hensoldt Cyber.

Prof. Dr. Gunnar Teege

gunnar.teege@unibw.de

+49 89 6004 3353

https://go.unibw.de/fomset

Funded by: StMWi

FIG.: [M] SHUTTERSTOCK / BLUE ANDY; ISTOCK / MATEJMO; FI CODE / G. TEEGE

Cooperations

Germany and the World

FIG.: ADOBE STOCK / GREENBUTTERFLY

National Partners

The RI CODE is working with 52 partners in 32 cities and municipalties in Germany.

THE COOPERATION WITH other universities, public institutions and companies is part of RI CODE's self-image: We learn with and from our partners and can take the first steps towards implementing our research results in practice.

At the same time, this close exchange ensures that we understand the specific questions and problems of our partners and can consider them from a scientific perspective.

Within Germany, our network is particularly tight-knit. As part of the University of the Bundeswehr Munich, we work with 52 institutions in 32 cities and municipalties nationwide. The focus is on Bavaria and the Munich area, North Rhine-Westphalia, and Hessia.

	Institution	Location
1	Aalen University	Aalen
2	University of Bamberg	Bamberg
3	University of Bayreuth	Bayreuth
4	IOTA Foundation	Berlin
5	Moysies & Partners GmbH	Berlin
6	DFN e.V.	Berlin
7	Bielefeld University of Applied Sciences	Bielefeld
8	Ruhr University Bochum (RUB)	Bochum
9	Federal Office for Information Security (BSI)	Bonn
10	Chemnitz University of Technology	Chemnitz
11	SoSafe GmbH	Cologne
12	German Aerospace Center (DLR)	Cologne/Oberpfaffenhofen
13	Darmstadt University of Applied Sciences (h_da)	Darmstadt
14	National Research Center for Applied Cybersecurity ATHENE	Darmstadt
15	Technical University of Darmstadt	Darmstadt
16	Technical University of Dresden (TUD)	Dresden
17	University of Duisburg-Essen (UDE)	Duisburg/Essen
18	Friedrich-Alexander University of Erlangen-Nuremberg (FAU)	Erlangen/Nuremberg
19	secunet Security Networks AG	Essen
20	Frankfurt University of Applied Sciences	Frankfurt a. M.
21	neosfer GmbH	Frankfurt a. M.
22	nuix	Frankfurt a. M.
23	Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities (LRZ)	Garching

	Institution	Location
24	Helmut Schmidt University / University of the Bundeswehr Hamburg (HSU)	Hamburg
25	Leibniz University Hannover (LUH)	Hannover
26	Technical University Ilmenau	Ilmenau
27	BWI GmbH	Meckenheim
28	Bavarian State Office for Taxes (BayLfSt)	Munich
29	Bavarian State Ministry for Digital Affairs (BayStMD)	Munich
30	BMW AG	Munich
31	Center for Digital Technology and Management (CDTM)	Munich
32	ESG Elektroniksystem- und Logistik-GmbH	Munich
33	FAST-DETECT GmbH	Munich
34	Google Munich	Munich
35	H&D GmbH	Munich
36	LMU Munich	Munich
37	Rohde & Schwarz GmbH & Co. KG	Munich
38	Technical University of Munich (TUM)	Munich
39	Central Office for Information Technology in the Security Sector (ZITiS)	Munich
40	Bavarian State Office for IT Security (BayLSI)	Nuremberg
41	IABG Industrieanlagen-Betriebsgesellschaft mbH	Ottobrunn
42	Paderborn University (UPB)	Paderborn
43	University of Passau	Passau
44	University of Siegen	Siegen
45	Airbus Cybersecurity GmbH	Taufkirchen
46	HENSOLDT Cyber GmbH	Taufkirchen
47	Airbus Defence and Space GmbH	Taufkirchen/Ottobrunn/ Manching
48	Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE	Wachtberg/Bonn
49	Hesse State Criminal Police Office (HLKA)	Wiesbaden
50	Hessian Police Headquarters for Technology (HPT)	Wiesbaden
51	Federal Criminal Police Office (BKA)	Wiesbaden/Berlin
52	Julius Maximilian University of Würzburg (JMU)	Würzburg


24
Hamburg
4
5
6
51
Berlin
25
Hannover
7
Bielefeld
42
Paderborn
8
Duisburg
Bochum
17
Essen
19
16
Dresden
10
Chemnitz
11
12
Cologne
44
Siegen
26
Ilmenau
27
9
Meckenheim
Bonn
Wachtberg
48
49
50
51
20
21
22
Wiesbaden
Frankfurt/Main
2
Bamberg
3
Bayreuth
52
Würzburg
Darmstadt
13
14
15
18
Erlangen
40
Nuremberg
1
Aalen
28
29
30
31
32
33
34
35
36
37
38
39
47
Manching
43
Passau
23
Garching
Munich
Ottobrunn
41
47
Oberpfaffenhofen
26
Taufkirchen
45
46
47
Map legend
1
Location number of partners
Partner locations

Internationality

The RI CODE maintains a large international network. In 2022, employees came from 17 countries. We cooperated with 80 partners in 25 countries.

Employees

Nationality	Total
Argentine	1
Austrian	8
Bangladeshi	1
Benini	1
Bosnian	1
British	1
Bulgarian	1
Croatian	1
Egyptian	2
Finnish	1
French	2
Greek	1
German	105
Indic	1
Italian	1
Slowenian/German	1
South Korean	1

International Cooperation Partners

Country	Partner
Australia	University of Melbourne
	University of New South Wales
Austria	Austrian Armed Forces
	Johannes Kepler University Linz
	Plasser & Theurer GmbH
	PwC Österreich GmbH
	SBA Research
	Software Competence Center Hagenberg
Belgium	EIT Digital
	KU Leuven
Canada	evolutionQ Inc.
	University of Waterloo
Cyprus	Cyprus University of Technology
Czech Republic	Flowmon Networks
	Masaryk University (MUNI)

FIG.: ISTOCK / BLUE PLANET STUDIO

Country	Partner
Denmark	Aarhus University
Egypt	European Universities in Egypt
	German University in Cairo
France	Centre de Recherche de l'Ecole de l'Air (CREA)
	CyberDetect
	INRIA/Université de Lorraine
	Université catholique de l'Ouest (UCO)
Greece	ATHENA Research Center
	Foundation for Research and Technology Hellas
	National Cyber Security Authority of the Minstry of Digital Governance
	Ubitech
Hungary	Budapest University of Technology and Economics (BME)
	Eötvös Loránd University
Israel	Ben-Gurion University of the Negev
Italy	Centro Ricerche Fiat
	Telecom Italia
	University of Insubria
	University of Milan
Luxembourg	University of Luxembourg
Netherlands	Arthur's Legal B.V.
	SIDN – Stichting Internet Domeinregistratie Nederland
	SURFnet
	University of Twente
	Utrecht University
Norway	Norwegian University of Science and Technology
	Oslo Metropolitan University
	Telenor Group
	University of Oslo
Portugal	Efacec Electric Mobility
	University of Lisbon
Romania	Babes-Bolyai University
	Bitdefender

Country	Partner
Slowenia	Jožef Stefan Institute
	University of Maribor
South Korea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Spain	Atos Spain S.A.
	CaixaBank
	i2CAT
	IMDEA Software Institute
	NTT Data
	Telefonica I+D
	Universitat Autònoma de Barcelona
Sweden	Chalmers University of Technology
	Ericsson
	RISE Research Institutes of Sweden
	University of Gothenburg
	Uppsala University
Switzerland	École Polytechnique Fédérale de Lausanne
	ID Quantique SA
	RUAG
	University of Lausanne
	University of St. Gallen
	University of Zurich
United Kingdom	Imperial College London
	King's College London
	Lancaster University
	University College London
	University of Glasgow
	University of Surrey
USA	Auburn University, College of Engineering
	Davidson College
	George Marshall Center
	University of Arizona, College of Engineering
	University of North Carolina at Charlotte

Young Science

Offers and Opportunities

FIG.: ADOBE STOCK / MONTRI

Study Award of the Research Institute CODE 2022

Efficient Exploitation of Vulnerabilities in Telecommunication Devices

This year, the Research Institute Cyber Defence and Smart Data (CODE), together with the company Giesecke + Devrient GmbH, is awarding Mr. Lars Fuchs the CODE Study Prize. In his Master's thesis, the computer scientist dealt with the efficient exploitation of vulnerabilities in telecommunications devices.

END-TO-END encryption on mobile devices is becoming increasingly important. The technology is used in instant messaging applications such as Signal and WhatsApp, where it protects users from unwanted read-along. This has major advantages. But like any technology that brings innovations, it also has disadvantages. Encryption technology gives criminals and suspected terrorists the opportunity to evade preventive protection and prosecution by authorities. At the same time, telecommunications surveillance is an important tool in the authorities' repertoire. It can be used both repressively and preventively. The measures help in criminal prosecution and have the potential to prevent terrorist attacks in Germany. In particular cases, so-called source telecommunication surveillance can be used as an alternative to the classic method. This involves installing software on the target's device in order to extract the relevant data.

Mr. Fuchs' Master's thesis, which was prepared in cooperation with ZITiS, contributes to simplifying and increasing the efficiency of such operations. In his work, he developed a system for identifying, evaluating, selecting, and exploiting vulnerabilities. This allows usable exploits to be found or developed more quickly for known vulnerabilities. While the search for and development of so-called zero-day exploits – i.e., vulnerabilities that are yet unknown to companies – is very time-consuming, known vulnerabilities can be exploited quickly and efficiently with the help of the system developed in the thesis.

Furthermore, the work contributes to the responsible use of vulnerabilities. The vulnerability assessment system incorporates, among other things, legal frameworks as well as impact on the target device in order to be able to issue a handling recommendation for certain vulnerabilities. This ensures that exploitation of exploits does not unnecessarily impact the target device.

The CODE Study Award was presented at the annual Master's Ceremony on December 10, 2022 on the campus of the University of the Bundeswehr Munich by Vice President Prof. Eva-Maria Kern in the presence of RI CODE Managing Director Prof. Wolfgang Hommel and Dr. Michael Tagscherer from G+D. ■

A total of 18 graduates from the class of 2022 were awarded study prizes for their excellent achievements.

FIG.: ADOBE STOCK / KANNAPAT; UNIBW M / SIEBOLD

Study Awards of the University of the Bundeswehr Munich

Every year, the University of the Bundeswehr Munich awards several study prizes donated by different partners. Since 2018, the RI CODE study award has been given to outstanding master's graduates with a relevant thesis in the field of cyber defence. The award is funded by Giesecke + Devrient GmbH and endowed with €1,000. ■

Laureates of the last years

Year	Name	Subject of the Thesis
2018	Christian Siegert	Automated detection of vulnerabilities in IT security
2019	Philipp Sammeck	Security analysis of an electronic safe lock
2020	Robert Jurisch-Eckardt	Development of a system to fight cybercrime
2021	Martin Lukner	Synthesizing malware traces for digital forensics
2022	Lars Fuchs	Efficient exploitation of vulnerabilities in telecommunication devices

Studying at the Research Institute CODE

The **Master's program in Cyber Security** at the RI CODE of the University of the Bundeswehr Munich covers information processing – including planning, formal modeling, implementation, and deployment – with a focus on technical and organizational information security. In addition to well-founded theoretical methods, practical are taught: e.g., the identification and elimination of security-relevant vulnerabilities, the development and implementation of security concepts, and the detection and mitigation of attacks on IT systems. In addition, legal and ethical issues as well as selected topics concerning the human factor in information security are covered.

The Bundeswehr supports civilian students with a **scholarship for the Master's program in Cyber Security** at the UniBw M. Requirements for this support are a degree (Bachelor or FH) in the STEM field as well as successful participation in a selection process conducted by the Assessmentcenter für Führungskräfte der Bundeswehr. Besides study programs at a level of excellence and an outstanding level of supervision by teaching staff, the UniBw M offers its students a wide range of leisure activities and amenities. Affordable housing options in one of Germany's most livable and diverse cities complete the benefits.

Further Information

Master's program Cyber Security:
https://go.unibw.de/80
(in German)

Scholarship of the Bundeswehr:
https://go.unibw.de/stipendium
(in German)

Award

Schwärzel Award for Leonhardt Kunczik

Reinforcement Learning with Hybrid Quantum Approximation in the NISQ Context


Prof. Dr. Heinz Schwärzel, Dr. Leonhardt Kunczik, Prof. Dr. Stefan Pickl (f. l. t. r.)

THE HEINZ SCHWÄRZEL AWARD for Fundamentals of Computer Science has been awarded annually since 2006. and honors outstanding PhD students from the three Munich universities. The initiator and honorary member of the Gesellschaft für Informatik e. V., Prof. Heinz Schwärtzel, is particularly interested in promoting fundamental computer science research with this award. The Research Institute CODE is pleased that this year its member Dr. Leonhard Kunczik received the award. The award was presented by Prof. Heinz Schwärtzel on December 2, 2022, at the TU Munich.

Quantum Reinforcement Approach

The award-winning thesis starts from the observation that complex optimization environments still reach their complexity limits even with modern methods of so-called reinforcement learning and are thus hardly algorithmically manageable. In his primarily fundamentals-oriented work, Mr. Kunczik on the one hand theoretically extends the approaches in the classical reinforcement learning context. On the other hand, he specifically tries to integrate "applicable" methods of quantum computing into the more comprehensive solution approaches and methods in order to make the complexity "algorithmically manageable." In particular, Leonhardt Kunczik develops a so-called quantum reinforcement approach, which is characterized by embedding the theoretical concept of Circuits Quantum Variational as a central element in the corresponding complex algorithmic optimization framework.

Interdiction Games: Attacker-Defender Scenario

In his work, Mr. Kunczik evaluates his methods against classical established optimization approaches. Here, he starts from the general frozen lake scenarios, which can be transferred to general more complex interdiction examples by his investigations. In doing so, he shows the individual obstacles, addresses model extensions and simplifications, and demonstrates the added value that lies in the performance improvement. These model developments are additionally characterized by the fact that these methods are considered in the appropriate context for the first time in a practical way on a current quantum computer architecture from IBM. This is done in the context of the Noisy Intermediate-Scale Quantum (NISQ) hardware environment. The extensive scientific investigations are laid out in great detail, and in some places have almost (theoretical) textbook character, so that a comprehension of the proposed solution path and the obtained results is very well possible.

Complex Optimization Scenarios

The work is a very comprehensive fundamental work with high scientific quality within computer science. It starts from a central current problem in the context of the RI CODE within complex optimization scenarios ("frozen lake environment"), and derives a very high scientific standard first by formulating the two core research questions. Both sets of issues are convincingly addressed, and also answered within the framework of current scientific theoretical possibilities. Mr. Kunczik has not only developed performance improvements, he has also analyzed interconnections of the problems in the work, thus for the first time providing the theoretical basis for further investigations.

Optimization Framework

With his work, Mr. Kunczik has presented a comprehensive optimization framework and comprehensibly embedded it in a novel theoretical treatment of complex optimization scenarios, which lends itself to further investigation. ■

"Thus, quantum RL provides a fruitful path to solve even more challenging problems in the context of complex ... (Frozen Lake) ... scenarios".

Leonhardt Kunczik

FIG.: UNIBW M

DOCTORATES 2022

Gonzalo Barbeito

"Design of a relief distribution framework in anticipation of a catastrophic blackout"

A CENTRAL ISSUE in humanitarian operations during severe power outages is the timely distribution of relief to the affected population. This thesis models central challenges for relief distribution during a blackout as a Rich Vehicle Routing Problem capturing a novel combination of taxonomic attributes and presents an interactive experiment environment for profound analysis of problem solutions.

Gonzalo Barbeito received his PhD in June 2022 with Prof. Pickl. He is currently employed at Amazon Web Services as a professional services consultant. ■

Michael Fröhlich

"Usable Cryptocurrency Systems"

MICHAEL FRÖHLICH'S research examines the usability challenges of cryptocurrencies and blockchain technology, and presents several approaches for addressing these challenges. His dissertation is divided into three main sections: a systematic review of existing human-computer interaction research on cryptocurrencies, a study of user behavior and challenges, and an evaluation of different approaches for improving application usability. The dissertation concludes by reflecting on the future role of human-computer interaction research in the field of cryptocurrency and blockchain technology.

Michael Fröhlich was supervised by Prof. Dr. Florian Alt and defended his thesis in December 2022. He is currently employed at the Center for Digital Technology and Management (CDTM), a joint institute of LMU and TUM. ■

Sarah Prange

"Usable Privacy and Security in Smart Homes"

SARAH PRANGE'S thesis contributes to usable privacy and security research in the context of smart homes by a) understanding users' privacy perceptions and requirements for usable mechanisms and b) investigating concepts and prototypes for privacy and security mechanisms. Hereby, the focus is on two specific target groups: namely, inhabitants and guests of smart homes.

Her thesis provides valuable insights to help researchers and practitioners in designing and evaluating privacy and security mechanisms for future smart devices and homes, particularly targeting awareness, control, and authentication, as well as various roles.

Sarah Prange was supervised by Prof. Dr. Florian Alt and defended her thesis in December 2022. She is currently employed at the Research Institute CODE as a research assistant. ■

FIG.: ADOBE STCOK; PRIVAT (5)

Radiah Rivu

"Out-of-the-Lab Virtual Reality Studies"

RADIAH RIVU'S dissertation explores how virtual reality studies can be conducted outside of laboratory settings. The work is motivated by the fact that many people today own a VR setup. Accordingly, they can participate in studies from home, which not only reduces the burden on study participants, but also allows for larger and more diverse samples. The dissertation addresses challenges from both the technical side (e.g., platforms for study implementation and data collection) and the user side (e.g., recruiting challenges, implementation without the physical presence of a study leader, etc.).

Radiah Rivu was supervised by Prof. Dr. Florian Alt and defended her thesis in October 2022. She is currently employed at the Research Institute CODE as a research assistant. ■

Robert Rödler

"Profile Matching Across Online Social Networks Based on Metadata"

PROFILE MATCHING across online social networks based on metadata investigates to what extent two or more profiles in different social networks can be matched to one and the same person solely only on the basis of metadata. Using a meta model, the metadata available and retrievable in a social network are introduced and explained, and three approaches are evaluated on the basis of this data. Depending on the used approach, it could be shown that even small amounts of metadata can achieve an almost 100% matching accuracy. Therefore, possible measures to ensure personal data protection rounds off this work.

Robert Rödler received his doctorate with Prof. Dr. Wolfgang Hommel as primary advisor in May 2022. He meanwhile works as Programme Manager Digitization Land at IABG mbH in the Defence & Security division. ■

Michael Steinke

"Framework Designs for Management Platforms in Federated Software Networks"

THE DOCTORAL thesis describes suitable architectural components for management platforms for modern virtual and centrally manageable computer networks. Their suitability especially aims at the management of network components in a federated context with multiple sovereign organizations. The components are described in the form of software frameworks along with interfaces between them and can be used to either extend existing management platforms or for the development of novel platforms from scatch. Consequently, the thesis contributes to secure operation of modern decentralized IT infrastructures such as cloud computing.

Michael Steinke received his doctorate with Prof. Wolfgang Hommel as primary advisor in July 2022. He works as a postdoc in the university's computer science department in the dtec.bw project DEFINE. ■

Capture the Flag 2022

“The Spanning Tree – Catching B8tes”

At the eighth edition of the Capture the Flag event organized by the Research Institute CODE with support from ITIS e.V. and Team localos, more than 40 teams competed against each other online and in presence on the campus of the University of the Bundeswehr Munich in numerous exciting challenges.

ON NOVEMBER 25 AND 26, 2022, it was that time again – the annual hacking competition Capture the Flag took place at the UniCasino on the campus of the University of the Bundeswehr Munich. Since 2015, the event has been a set date for many. Participants can not only train their skills in the field of cyber security and show their knowledge and skills, but also combine it all with a lot of fun and action at the same time.

Of the more than 80 teams that participated in the qualifying in October, only about half received an invitation to show their skills at the competition at the end of November. In addition to the 21 teams on site, another 20 teams took part virtually in a separate online track, as in the previous year. After the welcoming words by the Executive Director of the Research Institute CODE,

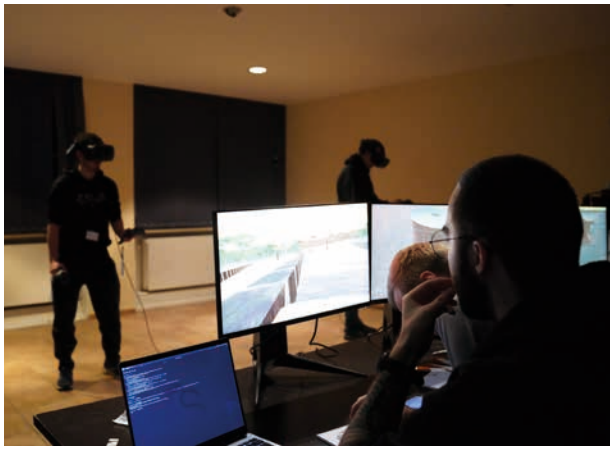
Prof. Dr. Wolfgang Hommel, he officially started the competition on Friday evening at 6:00 p.m. on the dot.

This year, the competition was themed "The Spanning Tree – Catching B8tes". In reference to the film "The Hunger Games – Catching Fire", the task during the 18-hour event was to solve a series of tasks, so-called challenges, from various categories and thus collect points. As in the film, the challenges were arranged on a playing field consisting of a round arena with different sectors. Each of the sectors corresponded to one of the categories crypto, web, forensics, misc, reversing/pwning and virtual reality/hardware.

Among the 41 challenges that the teams had to solve on site, the five hardware challenges in particular required all the participants' skills. For example, data transmitted in encrypted form over a Zigbee network first had to be recorded and decrypted. To tap the key, the participants had to insert a new node. Another task involved overcoming a gate control system that prevented two gates from opening at the same time. By cleverly exploiting the Modbus protocol, the teams had to pretend to the controller that one of the gates was closed, even though it had already been opened.

Throughout the night, the teams worked intensively on the tasks set and fought an exciting competition. Then, towards morning, a group of four teams slowly broke away and had a neck-and-neck race until shortly before the end at 12:00 noon on Saturday. In the end, last year's winner Team Nemesis won the battle of four, leaving the teams 0x90, 40 Years the Bitflippers, and Sabobatage behind. The online track was won by team Winnie the pwnd ahead of rckwrtz and Ignorital. After the award ceremony by Wolfgang Hommel and Marcus Knüpfer, the lucky defending champions could perpetuate their names on the Flag-of-Fame with their signatures. All three top teams also received prizes such as scientific books. "It is a particular interest of ours to ensure that the cyber security experts of tomorrow are trained in the most practical way possible – whether through events like this, our master's degree program in cyber security, the offerings of our Cyber Range, or through third-party training," said the Executive Director at the awards ceremony. For all participants, the CTF event was once again great fun and many teams have already announced their participation for next year.

Last but not least, the organizers would like to express their sincere thanks to the numerous supporters, without whose generosity the event could not have been held in comfort. ■

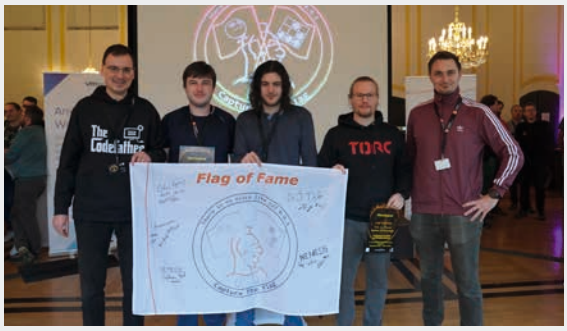


During the Virtual Reality Challenge, the participating teams had to be fully concentrated.

FIG.: RI CODE / B. BELLGRAU (3)

What is a "Capture the Flag" (CTF) competition?

CTFS OFFER THE opportunity to develop skills in the field of cyber security in a playful way and thus contribute to the practical training of experts. RI CODE's "Capture the Flag" is a hacking competition focusing on knowledge acquisition, team building and fun, which has been held once a year since 2015 on the campus of the University of the Bundeswehr Munich in Neubiberg. During the event, students can put their theoretical knowledge to the test by taking part in various practical challenges.



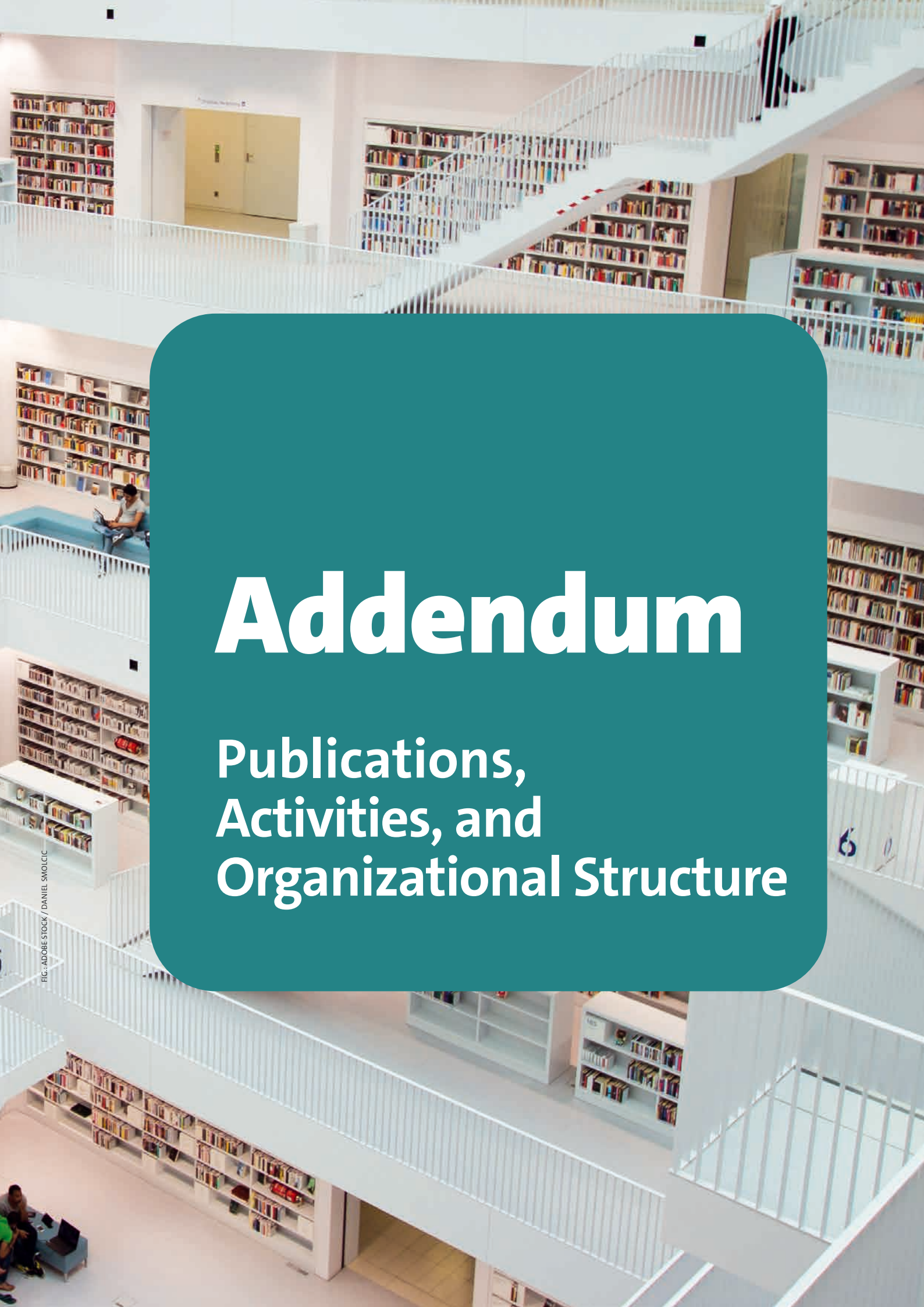
Wolfgang Hommel (l.), Executive Director of RI CODE, and Marcus Knüpfer (r.), Acting Managing Director of RI CODE, together with the successful defending champion "Team Nemesis."

More information:

www.unibw.de/code/events/ctf

www.unibw.de/code/events/capture-the-flag-2022-the-spanning-tree-catching-b8tes

ctf@unibw.de



Addendum

Publications, Activities, and Organizational Structure

FIG.: ADOBE STOCK / DANIEL SMOLCIC

Prof. Dr.
Florian Alt

Usable Security and Privacy

PUBLICATIONS

ABDELRAHMAN, Y., MATHIS, F., KNIERIM, P., KETTLER, A., ALT, F., KHAMIS, M.: Cuevr: Studying the Usability of Cue-based Authentication for Virtual Reality. AVI'22, ACM, 2022.

ABDRABOU, Y., RIVU, R., AMMAR, T., LIEBERS, J., SAAD, A., LIEBERS, C., GRUENEFELD, U., KNIERIM, P., KHAMIS, M., MÄKELÄ, V., SCHNEEGASS, S., ALT, F.: Understanding Shoulder Surfer Behavior and Attack Patterns Using Virtual Reality. AVI'22, ACM, 2022.

ABDRABOU, Y., RIVU, R., AMMAR, T., LIEBERS, J., SAAD, A., LIEBERS, C., GRUENEFELD, U., KNIERIM, P., KHAMIS, M., MÄKELÄ, V., SCHNEEGASS, S., ALT, F.: Understanding Shoulder Surfer Behavior and Attack Patterns Using Virtual Reality. Adjunct proceedings SOUPS'22, USENIX Association, 2022.

ABDRABOU, Y., SCHÜTTE, J., SHAMS, A., PFEUFFER, K., BUSCHEK, D., KHAMIS, M., ALT, F.: Identifying Password Reuse from Gaze Behavior and Keystroke Dynamics. Adjunct proceedings SOUPS'22, USENIX Association, 2022.

ABDRABOU, Y., SCHÜTTE, J., SHAMS, A., PFEUFFER, K., BUSCHEK, D., KHAMIS, M., ALT, F.: "Your Eyes Say You Have Used This Password Before": Identifying Password Reuse from Gaze Behavior and Keystroke Dynamics. CHI'22, ACM, 2022.

ABDRABOU, Y., RIVU, R., AMMAR, T., LIEBERS, J., SAAD, A., LIEBERS, C., GRUENEFELD, U., KNIERIM, P., KHAMIS, M., MÄKELÄ, V., SCHNEEGASS, S., ALT, F.: Understanding Shoulder Surfer Behavior Using Virtual Reality. Adjunct Proceedings IEEE VR, 2022.

ALT, F.: Wie die Forschung auf das Metaversum blickt. Inside.unibw, vol. 9, p. 3, 2022.

ALT, F., KOSTAKOS, V., OLIVIER, N.: Out-of-the-Lab Pervasive Computing (Editorial). IEEE Pervasive Computing, 2022.

DELGADO RODRIGUEZ, S., MECKE, L., ALT, F.: Sensehandle: Investigating Human-door Interaction Behaviour for Authentication in the Physical World. Adjunct proceedings SOUPS'22, USENIX Association, 2022.

DELGADO RODRIGUEZ, S., PRANGE, S., KNIERIM, P., MARKY, K., ALT, F.: Experiencing Tangible Privacy Control for Smart Homes with PriKey. MUM'22 Demo, ACM, 2022.

DELGADO RODRIGUEZ, S., PRANGE, S., VERGARA OSSENBERG, C., HENKEL. M., ALT, F., MARKY, K.: PriKey – Investigating Tangible Privacy Control for Smart Home Inhabitants and Visitors. NordiCHI'22, ACM, 2022.

ESTEVES, A., BOUQUET, E., PFEUFFER, K., ALT, F.: One-Handed Input for Mobile Devices via Motion Matching and Orbits Controls. Proc. acm interact. mob. wearable ubiquitous technol., vol. 6, iss. 2, 2022.

FROEHLICH, M., VEGA VERMEHREN, J. A., ALT, F., SCHMIDT, A.: Implementation and Evaluation of a Point-of-sale Payment System Using Bitcoin Lightning. NordiCHI'22, ACM, 2022.

FROEHLICH, M., VEGA VERMEHREN, J. A., ALT, F., SCHMIDT, A.: Supporting Interface Experimentation for Blockchain Applications. NordiCHI'22, ACM, 2022.

FROEHLICH, M., VEGA VERMEHREN, J. A., PAHL, A., LOTZ, S., ALT, F., SCHMIDT, A., WELPE, I.: Prototyping With Blockchain: A Case Study for Teaching Blockchain Application Development at University. ICL'22, 2022.

FROEHLICH, M., WALTENBERGER, F., TROTTER, L., ALT, F., SCHMIDT, A.: Blockchain and Cryptocurrency in Human Computer Interaction: a Systematic Literature Review and Research Agenda. DIS'22, ACM, 2022, p. 155–177.

GOETZ, L., RIVU, R., ALT, F., SCHMIDT, A., MÄKELÄ, V.: Methods for Autobiographical Recall in Virtual Reality. NordiCHI'22, ACM, 2022.

GUZIJ, K., FROEHLICH, M., FINCKE, F., SCHMIDT, A., ALT, F.: Designing Trustworthy User Interfaces for the Voluntary Carbon Market: a Randomized Online Experiment. DIS'22, ACM, 2022, p. 71–84.

KHAMIS, M., MARY, K., BULLING, A., ALT, F.: User-centred Multimodal Authentication: Securing Handheld Mobile Devices Using Gaze and Touch Input. Behaviour & information technology, pp. 1-23, 2022.

LE, T., DIETZ, F., PFEUFFER, K., ALT, F.: A Practical Method to Eye-tracking on the Phone: Toolkit, Accuracy and Precision. MUM'22, ACM, 2022.

MA, Y., ABDELRAHMAN, Y., PETZ, B., DREWES, H., ALT, F., HUSSMANN, H., BUTZ, A.: Enthusiasts, Pragmatists, and Sceptics: Investigating Users' Attitudes Towards Emotion- and Personality-aware Voice Assistants across Cultures. MuC'22, ACM, 2022.

MÄEKELÄ, V., WINTER, J., SCHWAB, J., KOCH, M., ALT, F.: Pandemic Displays: Considering Hygiene on Public Touchscreens in the Post-Pandemic Era. CHI'22, ACM, 2022.

PRANGE, S., DELGADO RODRIGUEZ, S., DÖDING, T., ALT, F.: "Where did you first meet the owner?" – Exploring Usable Authentication for Smart Home Visitors. CHI EA'22, ACM, 2022.

PRANGE, S., DELGADO RODRIGUEZ, S., MECKE, L., ALT, F.: "I saw your partner naked": Exploring Privacy Challenges During Video-based Online Meetings. MUM'22, ACM, 2022.

PRANGE, S., SHAMS, A., PIENING, R., ABDELRAHMAN, Y., ALT, F.: PriView – Exploring Visualisations Supporting Users' Privacy Awareness. Adjunct proceedings SOUPS'22, USENIX Association, 2022.

PRANGE, S., THIEM, N., FRÖHLICH, M., ALT, F.: "Secure settings are quick and easy!" – Motivating End-users to Choose Secure Smart Home Configurations. AVI'22, ACM, 2022.

REITER, K., PFEUFFER, K., ESTEVES, A., MITTERMEIER, T., ALT, F.: Look & Turn: One-Handed and Expressive Menu Interaction by Gaze and Arm Turns in VR. In 2022 Symposium on Eye Tracking Research and Applications (ETRA'22), ACM, 2022.

RAUSCHNABEL, P. A., FELIX, R., HINSCH, C., SHAHAB, H., ALT, F.: What is XR? Towards a Framework for Augmented and Virtual Reality. Computers in human behavior, vol. 133, p. 107289, 2022.

RENZ, A., BALDAUF, M., MAIER, E., ALT, F.: Alexa, It's Me! An Online Survey on the User Experience of Smart Speaker Authentication. MuC'22, ACM, 2022.

RIVU, R., BAYERL, H., KNIERIM, P., ALT, F.: 'Can You Set It Up on Your Own?' – Investigating Users' Ability to Participate in Remote-Based Virtual Reality Studies. MUM'22, ACM, 2022.

SAAD, A., GRUENEFELD, J., MECKE, L., KOELLE, M., ALT, F., SCHNEEGASS, S.: Mask removal isn't always convenient in public! – The Impact of the Covid-19 Pandemic on Device Usage and User Authentication. CHI EA'22, ACM, 2022.

SAHOO, L., MIAZI, N. S., SHEHAB, M., ALT, F., ABDELRAHMAN, Y.: You Know Too Much: Investigating Users' Perceptions and Privacy Concerns Towards Thermal Imaging. Privacy'22, 2022.

SCHNEEGASS, S., SAAD, A., HEGER, R., DELGADO RODRIGUEZ, S., POGUNTKE, R., ALT, F.: An Investigation of Shoulder Surfing Attacks on Touch-based Unlock Events. Proc. acm hum.-comput. interact., vol. 6, iss. MHCI, 2022.

SUDAR, C., FROEHLICH, M., ALT, F.: Trueyes: Utilizing Microtasks in Mobile Apps for Crowdsourced Labeling of Machine Learning Datasets. arXiv, 2022.

VOLK, V., PRANGE, S., ALT, F.: PriCheck – An Online Privacy Assistant for Smart Device Purchases. CHI EA'22, ACM, 2022.

RESEARCH PROJECTS

Voice of Wisdom

The Voice of Wisdom project explores approaches to prevent human-centric cyber attacks. By analyzing human behavior and physiological states, signs that people are at risk are identified. In addition, novel human-centric security mechanisms are being developed and the long-term effects of these are being studied.

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGeneration EU.
Duration: 01/2021 – 12/2024

PrEvoke – Supporting Users in Informed Privacy Permission Revocation

PrEvoke addresses the consequences of revoking privacy decisions (e.g., when users revoke apps' access to personal data). The consequences expected by users with regard to the revocation of privacy permissions are examined and compared with reality. Appropriate concepts are also created to counter misunderstandings and concerns.

Funded by: Google Inc.
Duration: 12/2021 – 12/2022

Scalable Biometrics

The Scalable Biometrics project explores how pervasive computing environments can leverage behavioral biometrics for identifying and authenticating users. The main question is how behavioral biometrics approaches scale to different pervasive computing environments that contain multiple users with changing behavior, different physicalities, and changing sensing and interaction capabilities.

Funded by: DFG
Duration: 04/2020 – 03/2023

ubihave

Ubiquitous computers serve as both everyday companions and environmental sensors. Such devices generate user-specific data, enabling the creation of behavioral models and applications. This project develops models that describe, analyze, and predict user behavior. Promising application areas are: usable security, touch interaction, text input, and context-sensitive, adaptive systems.

Funded by: DFG
Duration: 01/2019 – 02/2023

TEACHING

3665-V1	**Secure Human-Computer Interfaces**
36651	**Usable Security**
36653	**Practical Course Design of Usable and Secure Systems**
10123	**Human Factors in Computing Systems**

FAIRS, CONFERENCES, SEMINARS

- Mensch und Computer 2022: Inclusive Security by Design Workshop
- Mensch und Computer 2022: (Be-)Greifbare Interaktionen Workshop
- AFCEA Trade Exhibition 2022: Representation of the Research Institute CODE

PRIZES AND AWARDS

- ACM SIGMM Test of Time Honorable Mention in the category of Multimedia Interfaces and Applications - Müller, J., Alt, F., Michelis, D., and Schmidt, A. Requirements and Design Space for Interactive Public Displays
- ICL 2022 Best Paper Award - Fröhlich, M., Vega Vermehren, J. A., Pahl, A., Lotz, S., Alt, F., Schmidt, A., Welpe, I. Prototyping with Blockchain: A Case Study For Teaching Blockchain Application Development at University

ADDITIONAL FUNCTIONS

- Associate Chair for CHI 2023
- Associate Editor for IMWUT
- Editorial Board Member and Department Editor for IEEE Pervasive Computing
- Guest Editor for IEEE Special Issue on Out-of-the-Lab Pervasive Computing
- Steering Committee Chair for the Mobile and Ubiquitous Multimedia (MUM) Conference Series

Prof. Dr. Harald Baier

Digital Forensics

PUBLICATIONS

GÖBEL, TH., MALTAN, ST., TÜRR, J., BAIER, H., MANN, F.: "ForTrace – A Holistic Forensic Data Set Synthesis Framework", in Journal Forensic Science International: Digital Investigation, Volume 40, 2022.

GÖBEL, TH., UHLIG, F., BAIER, H., BREITINGER, F.: "FRASHER – A Framework for Automated Evaluation of Similarity Hashing", in Journal Forensic Science International: Digital Investigation, Volume 42, 2022.

GONCALVES, P., ATTENBERGER, A., BAIER, H.: "Smartphone Data Distributions and Requirements for Realistic Mobile Device Forensic Corpora", Proceedings of 20th Annual IFIP WG 11.9 International Conference on Digital Forensics, pp. 47–63, Springer, online, January 2022.

GONCALVES, P., DOLOS, K., STEBNER, M., ATTENBERGER, A., BAIER, H.: "Revisiting the Dataset Gap Problem – On Availability, Assessment and Perspective of Mobile Forensic Corpora", in Journal Forensic Science International: Digital Investigation, Volume 43, 2022.

KLIER, S., BAIER, H.: "Towards Efficient Onsite CSAM Triage by Clustering Images from a Source Point of View", in Proceedings of the 13th EAI International Conference on Digital Forensics & Cyber Crime (ICDF2C), Boston, MA, USA, November 2022.

LUKNER, M., GÖBEL, TH., BAIER, H.: "Realistic and Configurable Synthesis of Malware Traces in Windows Systems", Proceedings of 20th Annual IFIP WG 11.9 International Conference on Digital Forensics, pp. 21–44, Springer, online, January 2022.

MUNDT, M., BAIER, H.: "Cyber Crime Undermines Data Privacy efforts – On the Balance Between Data Privacy and Security", in Proceedings of the 13th EAI International Conference on Digital Forensics & Cyber Crime (ICDF2C), Boston, MA, USA, November 2022.

MUNDT, M., BAIER, H.: "Mapping and Simulating Cyber-Physical Threats for Critical Infrastructures", in Proceedings of the 17th International Conference on Critical Information Infrastructures Security (CRITIS), Munich, Germany, September 2022.

TEACHING

1162	**Advanced Digital Forensics**
3824	**Digital Forensics**
5001/1009	**Seminar Digital Forensics**
5501/1009	**Seminar Forensic Methods in Computer Science**
5505 IT	**Forensics**

FAIRS, CONFERENCES, SEMINARS

Preparation and moderation of the CAST Forensics/Cybercrime workshop on 12/15/2022, URL: https://cast-forum.de/workshops/infos/318

ADDITIONAL FUNCTIONS

- Reviewer for "Journal of Digital Investigation" and "Computers & Security"
- Membership in program committees: Digital Forensics Research Workshop (DFRWS) EU 2022, Digital Forensics Research Workshop (DFRWS) APAC 2022, GI Sicherheit 2022, CAST Grant Award 2022, CAST-GI Doctoral Award 2022, SKILL 2022
- Support of the program director in establishing the study program "IT Security" at the Vietnamese-German University in Ho-Chi-Minh City, Vietnam

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

RESEARCH PROJECTS

ACSE – Airborne Cybersecurity Enhancement

The Research Institute CODE collaborates with Airbus DS on comprehensive research in order to understand and address cybersecurity problems in the avionics domain. The project provides answers to pressing issues arising from the introduction of new technologies in existing and future aircraft developments. A key objective is the holistic understanding of potential threats and their mitigations.

Funded by: Airbus Defence and Space
Duration: 2020 – 2024

APERITIF – Analysis Pipeline for Effective Vulnerability Identification Through Fuzzing

APERITIF is a joint project with Prof. Dr. Kinder's PATCH Research Group. The goal is to increase the scalability of fuzzing up to datacenter scales, and subsequently perform basic research on novel parallelization and optimization of fuzzers to increase their coverage and, consequently, vulnerability yield.

Funded by: BMVg/BAAINBw
Duration: 2021 – 2023

DEMISEC – Detecting Malicious Implants in Source Code

Modern software depends on many external open source components written by many different parties. If the contributions of only one such party are compromised, the security of the entire product is at risk. In DEMISEC, the researchers investigate how to detect malicious source code modifications before they can subvert the development process.

Funded by: BMVg/BAAINBw
Duration: 2021 – 2023

DEPS – Dependable Production Environments with Software Security

The DEPS project endeavors to devise a whole family of novel techniques to protect software and intellectual property by binding software to hardware. As a result, neither will regular, known ways to attack software systems be less effective, nor will reverse engineering be an effective way to maliciously obtain intellectual property.

Funded by: Austrian Research Promotion Agency (FFG), Software Competence Center Hagenberg
Duration: 2022 – 2025

TEACHING

1009 **Seminar Language-based Security**

1009 **Seminar Optimization of Programming Languages**

1010 **Machine-oriented Programming**

3647 **Compiler Construction**

55071 **Language-based Security**

FAIRS, CONFERENCES, SEMINARS

ECOOP 2022

ADDITIONAL FUNCTIONS

Program Committee

- IEEE European Symposium on Security and Privacy (EuroS&P 2023)
- Network and Distributed System Security Symposium (NDSS 2023)

Prof. Dr. Michaela Geierhos

Data Science

PUBLICATIONS

BLANC, O., PRITZKAU, A., SCHADE, U., GEIERHOS, M.: CODE at CheckThat! 2022: Multi-class Fake News Detection of News Articles with BERT. In: Faggioli, Guglielmo; Ferro, Nicola; Hanbury, Allan; Potthast, Martin (Ed.). Proceedings of the Working Notes of CLEF 2022. Conference and Labs of the Evaluation Forum. Bologna, Italy, September 5th to 8th, 2022. 2022. S. 444–455. CEUR Workshop Proceedings. 3180.

DENISOV, S., BÄUMER, F. S., GEIERHOS, M.: Track Me If You Can: Insights into Profile Interlinking on Social Networks. In: Kersting, Joschka (Ed.). PATTERNS 2022. The Fourteenth International Conferences on Pervasive Patterns and Applications, April 24 – 28, 2022 Barcelona, Spain: IARIA XPS Press. 2022. S. 18–21.

GEIERHOS, M. (ED.): DHd2022: Kulturen des digitalen Gedächtnisses. 2022. 418 S. https://doi.org/10.5281/zenodo.6304590

GEIERHOS, M.: Crawler (fokussiert / nicht fokussiert). In: Gronau, Norbert; Becker, Jörg; Kliewer, Natalia; Leimeister, Jan Marco; Overhage, Sven (Ed.). Berlin: GITO. 2022. Enzyklopädie der Wirtschaftsinformatik – Online-Lexikon. 11. Auflage.

GEIERHOS, M.: Sentimentanalyse. In: Gronau, Norbert; Becker, Jörg; Kliewer, Natalia; Leimeister, Jan Marco; Overhage, Sven (Ed.). Berlin: GITO. 2022. Enzyklopädie der Wirtschaftsinformatik – Online-Lexikon. 11. Auflage.

GEIERHOS, M.: Text Mining. In: Gronau, Norbert; Becker, Jörg; Kliewer, Natalia; Leimeister, Jan Marco; Overhage, Sven (Ed.). Berlin: GITO. 2022. Enzyklopädie der Wirtschaftsinformatik – Online-Lexikon. 11. Auflage.

GEIERHOS, M.: Webmonitoring. In: Gronau, Norbert; Becker, Jörg; Kliewer, Natalia; Leimeister, Jan Marco; Overhage, Sven (Ed.). Berlin: GITO. 2022. Enzyklopädie der Wirtschaftsinformatik – Online-Lexikon. 11. Auflage.

KERSTING, J., AHMED, M., GEIERHOS, M.: Chatbot-enhanced Requirements Resolution for Automated Service Compositions. In: Stephanidis, Constantine; Antona, Margherita; Ntoa, Stavroula (Ed.). HCI International 2022 Posters. 24th International Conference on Human-Computer Interaction, HCII 2022, Virtual Event, June 26 – July 1, 2022, Proceedings, Part I. Cham: Springer. 2022. S. 419–426. Communications in Computer and Information Science. 1580.

MEISSNER, A., FRÖHLICH, A., GEIERHOS, M.: Keep It Simple: Local Search-based Latent Space Editing. Proceedings of the 14th International Joint Conference on Computational Intelligence - Volume 1: NCTA. Setúbal: SCITEPRESS. 2022. S. 273–283.

PRITZKAU, A., BLANC, O., GEIERHOS, M., SCHADE, U.: NLytics at CheckThat! 2022: Hierarchical Multi-class Fake News Detection of News Articles Exploiting the Topic Structure. In: Faggioli, Guglielmo; Ferro, Nicola; Hanbury, Allan; Potthast, Martin (Ed.). Proceedings of the Working Notes of CLEF 2022. Conference and Labs of the Evaluation Forum; Bologna, Italy, September 5th to 8th, 2022. 2022. S. 629–648. CEUR Workshop Proceedings. 3180.

RESEARCH PROJECTS

KIMONO – Campaign Identification, Monitoring and Classification Using Social Media Mining Methods for Integration in an AI-based Early Warning System

The aim of the KIMONO project is the detection and modeling of short- and long-term disinformation and influence campaigns in social media such as Twitter and Facebook. In particular, the focus is on campaigns that are driven by stately actors.

Funded by: BMVg/BAAINBw
Duration: 09/2021 – 12/2024

AI-based Speech Signal Decoder

The goal of this proof-of-concept is to prototype a neural network for decoding existing vocoder data to improve reception quality.

Duration: 09/2021 – 12/2024

NAWI – News Articles and Knowledge

The NAWI project deals with knowledge extraction and modeling from news articles.

Duration: 12/2021 – 11/2024

Synthetic Data Generation and Detection

The research project focuses on methods for generating and detecting synthetically created or manipulated data using artificial intelligence. In this context, methods are being developed that are capable of recognizing synthetically created and manipulated images, videos, and audio files accurately.

Funded by: Central Office for Information Technology in the Security Sector
Duration: 06/2022 – 05/2025

VIKING – Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen

The subproject "Explainability of Trustworthy AI Language Models for Transparent Use in Security Agencies for Text Classification" is dedicated to the research of trustworthy AI methods for text classification within the joint project VIKING.

Funded by: BMBF
Duration: 01/2022 – 12/2024

TEACHING

1144 **Knowledge Discovery in Big Data**

3850 **Natural Language Processing**

3851 **Information Retrieval**

3852 **Data Science Applications**

3853 **Analysis of Unstructured Data**

ADDITIONAL FUNCTIONS

- Faculty council member (since 10/2022)
- Member of the advisory board "German Biography" of the Historical Commission at the Bavarian Academy of Sciences and Humanities
- Expert for the European Commission
- Expert for VDI/VDE Innovation + Technik

Program Committee

- CLEF 2022 – Conference and Labs of the Evaluation Forum Information Access Evaluation meets Multilinguality, Multimodality, and Visualization
- DHd 2022 – 8th Annual Conference of the Digital Humanities Association in German-speaking Countries (Chair)
- EMNLP 2022 – The 2022 Conference on Empirical Methods in Natural Language Processing
- PATTERNS 2022 – The Fourteenth International Conference on Pervasive Patterns and Applications
- SEMANTiCS 2022 – 18th International Conference on Semantics Systems

Hon.-Prof. Dr. Udo Helmbrecht

Quantum Communication

PUBLICATIONS

AUER, M., FREIWANG, P., BALIUKA, A., KNIPS, L., WEINFURTER, L.: A Portable Decoy-state QKD Sender. DPG22 – Erlangen.

AUER, M., FREIWANG, P., BALIUKA, A., KNIPS, L., WEINFURTER, L.: A Portable Decoy-state QKD Sender. QKD Summerschool Waterloo 2022.

DENISOV, S., BÄUMER, F. S.: The Only Link You'll Ever Need: How Social Media Reference Landing Pages Speed up Profile Matching. ICIST 2022: International Conference on Information and Software Technologies 2022.

KÖRFGEN, H., FARINA, F., HELMBRECHT, U.: Architecture of the MuQuaNet Quantum Key Distribution Network. Quantum Alliance PhD Conference.

TEACHING

3695 **Quantum Communication**

FAIRS, CONFERENCES, SEMINARS

- Quantum Industry Days Switzerland
- Quantum Business Network Meeting on Quantum Communication
- Quantum Symposium on Operationalizing Quantum Technology for the Bundeswehr (QT4Bw)
- QR.X Workshop on the implementation of optical fiber links (Berlin)
- Pan-European Quantum Internet Hackathon 2022 (Amsterdam)

Prof. Dr. Wolfgang Hommel

Software and Data Security

PUBLICATIONS

HOMMEL, W., PÖHN, D., GRABATIN, M.: Die Identitäten der Zukunft: Selbstbestimmter Umgang mit digitalen Identitäten. In: moysies & partners (Ed.). 2022. S. 56-61. Der Schlüssel zur digitalen Verwaltung; Konten für Bürger:innen und Unternehmen.

HOMMEL, W., PÖHN, D., GRABATIN, M.: Eine digitale Identität für alles: So funktioniert die Technik hinter dem Verbund der Nutzerkonten. In: moysies & partners (Ed.). 2022. S. 16-28. Der Schlüssel zur digitalen Verwaltung; Konten für Bürger:innen und Unternehmen.

PÖHN, D., GRUSCHKA, N., ZIEGLER, L.: Multi-account Dashboard for Authentication Dependency Analysis. Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES). ACM. 2022.

PÖHN, D., HOMMEL, W.: Reference Service Model Framework for Identity Management. IEEE Access. Vol. 10. 2022. S. 1-26.

PÖHN, D., HOMMEL, W.: TaxIdMA: Towards a Taxonomy for Attacks Related to Identities. Proceedings of the 17th International Conference on Availability, Reliability and Security (ARES). ACM. 2022. S. 1-13.

RÖDLER, R.: Profilzuordnung über soziale Netze anhand von Metadaten. Dissertation, UniBw M. 2022. 177 S.

STEINKE, M.: Framework-Konzepte für Managementplattformen in föderierten softwarebasierten Netzen. Dissertation, UniBw M. 2022. 338 S.

WILKENING, F., STIEMERT, L., SCHOPP, M., PÖHN, D., HOMMEL, W.: Investigating Leaked Sensitive Information in Version Control Systems with the Kraulhorizon Framework. In Ude, Albrecht (Ed.). Sicherheit in vernetzten Systemen: 29. DFN-Konferenz. 2022. S. C1-C21.

RESEARCH PROJECTS

ACSE – Airborne Cybersecurity Enhancement

Airborne Cybersecurity Enhancement (ACSE) is a research cooperation between RI CODE and Airbus Defence and Space. The project tackles challenges in the area of cybersecurity resulting from operation and maintenance of complex, networked systems of airborne platforms. The focus of our team are concepts for secure software development as well as network security.

Funded by: Airbus Defence and Space
Duration: 12/2019 – 12/2023

DEFINE – DC-Grids for Reliable Power Supply

DC grids represent a more efficient alternative to current AC power distribution grids and consequently can be a building block of energy revolution. In this project, deployable medium voltage direct current (MVDC) grids are being researched. The focus of the RI CODE is the development of suitable management solutions for a secure and reliable operation of MVDC networks.

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.
Duration: 01/2021 - 12/2024

LIONS – Ledger Innovation and Operation Network for Sovereignty

The project LIONS builds a research platform for enhancing the resilience and digital sovereignty of digitalization using distributed ledger technologies. As part of the inter-disciplinary research project, the research group focuses on the topic of self-sovereign identity management and the technical support of project partners.

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr. dtec.bw is funded by the European Union – NextGenerationEU.
Duration: 01/2021 – 12/2024

TEACHING

1006 **Introduction to Computer Science 1**

1007 **Introduction to Computer Science 2**

3459 **Selected Chapters of IT Security**

5501 **Seminar Information Security Management**

5501 **Seminar Security Aspects of LoRa-based Wide Area Networks**

5507 **Secure Networked Applications**

5508 **Information Security Management**

ADDITIONAL FUNCTIONS

- Faculty council member (until 09/2022)
- Board of examiners for Master of Intelligence & Security Studies
- Member of the Operating Committee of the German Research and Eduction Network

Program Committee

- IEEE/IFIP Network Operations and Management Symposium (NOMS 2022)
- IEEE International Conference on Communications (ICC 2022)
- DFN Conference Security in Networked Systems 2022
- Workshop on Avionics Systems and Software Engineering 2022
- International Journal of Critical Infrastructure Protection
- International Journal of Electronic Government
- International Journal of Innovation and Technology Management
- HMD Praxis der Wirtschaftsinformatik

Prof. Dr. Johannes Kinder

PATCH: Program Analysis, Transformation, Comprehension and Hardening

PUBLICATIONS

PONCE DE LEÓN, H., KINDER, J.: Cats vs. Spectre: An Axiomatic Approach to Modeling Speculative Execution Attacks. In Proc. IEEE Symp. Security and Privacy (S&P), pp. 1415–1428, IEEE, 2022.

PONCE DE LEÓN, H., HASS, T., MEYER, R.: Dartagnan: SMT-based Violation Witness Validation (Competition Contribution). In Proc. Tools and Algorithms for the Construction and Analysis of Systems (TACAS), pp. 418–423, Springer, 2022.

TEACHING

38191 **Reverse Engineering**

38192 **Reverse Engineering Lab**

38491 **Dynamic Program Analysis**

38492 **Fuzzing Lab**

38381 **Static Program Analysis**

38382 **Static Program Analysis Lab**

55011 **Seminar Software Hardening**

55011 **Seminar Machine Learning in Reverse Engineering & Malware Detection**

ADDITIONAL FUNCTIONS

Advisory Board Member, Centre for Doctoral Training in Cyber Security for the Everyday, Royal Holloway, University of London

Program Committee

- IEEE Symposium on Security & Privacy
- Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
- International Colloquium on Theoretical Aspects of Computing (ICTAC)
- GI Sicherheit
- Workshop on Offensive and Defensive Techniques in the Context of Man At The End attacks (CheckMATE)
- Workshop on Principles of Secure Compilation (PriSC)

Prof. Dr.-Ing. Mark Manulis

PACY: Privacy and Applied Cryptography

PUBLICATIONS

CABALLERO, M. et al.: ICT in Healthcare: the role of IoT and the SECANT solution, IEEE International Conference on Cyber Security and Resilience (CSR) (2022), pp. 104–111.

FRYMANN, N., GARDHAM, D., MANULIS, M.: Unlinkable Delegation of WebAuthn Credentials, Computer Security – ESORICS 2022 - 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26-30, 2022, Proceedings, Part III, Springer, 2022: pp. 125–144.

GARDHAM, D., MANULIS, M.: Revocable Hierarchical Attribute-based Signatures from Lattices. Applied Cryptography and Network Security – 20th International Conference, ACNS 2022, Rome, Italy, June 20-23, 2022, Proceedings, Part II, Springer, 2020: pp. 40–61.

YANG, Y. et al.: TAPESTRY: A De-centralized Service for Trusted Interaction Online, IEEE Trans. Serv. Comput. 15(3) (2022), 1385–1398.

RESEARCH PROJECTS

EU H2020 Project SECANT: Security and Privacy Protection in Internet of Things Devices

The project is developing an innovative cybersecurity risk assessment platform to address cascading cyber threats and increase privacy and data protection across the connected ICT ecosystem. PACY Lab is working on cryptographic protocols based on blockchain technology to enable privacy-preserving search over encrypted sensitive data.

Funded by: EU H2020
Duration: 09/2021 – 08/2024
Participation via University of Surrey, UK

TEACHING

55481 **Modern Cryptography**

55482 **Research Trends in Cryptography**

FAIRS, CONFERENCES, SEMINARS

- 20th International Conference on Applied Cryptography and Network Security (ACNS) 2022 (Session Chair Cryptographic Protocols)

ADDITIONAL FUNCTIONS

- Associate Editor of IEEE Transactions on Information Forensics and Security (IEEE TIFS)
- Associate Editor of International Journal of Information Security (IJIS), Springer
- Co-Affiliation and Supervision of PhD students at the University of Surrey, UK

Program Committee

- 25th Information Security Conference (ISC) 2022
- 17th ACM Symposium on Information, Computer, and Communications Security (ACM ASIACCS) 2022
- 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec) 2022)

Jun. Prof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

PUBLICATIONS

MOLL, M.; WELLER, D. (2022): "Routing in Reinforcement Learning Markov Chains". Operations Research Proceedings 2021: Selected Papers of the International Conference of the Swiss, German and Austrian Operations Research Societies (SVOR/ASRO, GOR eV, ÖGOR), University of Bern, Switzerland, August 31–September 3, 2021, Springer.

NISTOR, M. S.; MOLL, M.; PHAM, S.; PICKL, S.; BUDDE, D. (2022): "Resource Optimization in Mass Casualty Management: A Comparison of Methods". Operations Research Proceedings 2021: Selected Papers of the International Conference of the Swiss, German and Austrian Operations Research Societies (SVOR/ASRO, GOR eV, ÖGOR), University of Bern, Switzerland, August 31–September 3, 2021, Springer.

RESEARCH PROJECTS

Digital Workplace and Human AI-assisted Training Through Touch

Considering the importance of artificial assistance systems, the project investigates their inclusion in the training process. This is done from the perspective of human learning (cognitive science), machine learning (computer science) and by analyzing trust in AI partners (philosophy).

Funded by: Bavarian Research Institute for Digital Transformation (bidt)
Duration: 04/2022 – 03/2025

TEACHING

10361 **Operations Research**

14901 **Selected Chapters of Operations Research and Decision Theory**

29941 **Selected Chapters of Data-driven Optimization**

22942 **Quantum Machine Learning & Optimization**

FAIRS, CONFERENCES, SEMINARS

Conference of the GOR Working Group: Simulation and Optimization of Complex Systems, House of Logistics and Mobility, Frankfurt

ADDITIONAL FUNCTIONS

- Research Group Leader "Data-driven Aviation Management", Munich Aerospace
- Working Group Leader "Simulation and Optimization of Complex Systems", German Operations Research Society

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

PUBLICATIONS

CAI, Y., ZIMEK, A., WUNDER, G., NTOUTSI, E. (2022). Power of Explanations: Towards Automatic Debiasing in Hate Speech Detection. In 2022 IEEE international conference on data science and advanced analytics (DSAA) (pp. 1-10). IEEE.

FABBRIZZI, S., PAPADOPOULOS, S., NTOUTSI, E., KOMPATSIARIS, I. (2022). A Survey on Bias in Visual Datasets. Computer Vision and Image Understanding, 223, 103552.

IOSIFIDIS, V., ROY, A., NTOUTSI, E. (2022). Parity-based Cumulative Fairness-aware Boosting. Knowledge and Information Systems, 64(10), 2737-2770.

LE QUY, T., NGUYEN, T. H., FRIEGE, G., NTOUTSI, E. (2023, January). Evaluation of Group Fairness Measures in Student Performance Prediction Problems. In Machine Learning and Principles and Practice of Knowledge Discovery in Databases: International Workshops of ECML PKDD 2022, Grenoble, France, September 19–23, 2022, Proceedings, Part I (pp. 119-136). Cham: Springer Nature Switzerland.

LE QUY, T., ROY, A., IOSIFIDIS, V., ZHANG, W., NTOUTSI, E. (2022). A Survey on Datasets for Fairness-aware Machine Learning. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery, 12(3), e1452.

ROY, A., NTOUTSI, E. (2022). Learning to Teach Fairness-aware Deep Multi-task Learning in Machine Learning and Knowledge Discovery in Databases. Research Track: European Conference, ECML PKDD 2022, Grenoble, France, September 19–22, 2022. Springer International Publishing.

ROY, A., IOSIFIDIS, V., NTOUTSI, E. (2022, November). Multi-fairness under Class-imbalance. In Discovery Science: 25th International Conference, DS 2022, Montpellier, France, October 10–12, 2022, Proceedings (pp. 286-301). Cham: Springer Nature Switzerland.

RESEARCH PROJECTS

STELAR – Spatio-temporal Linked Data Tools for the Agri-food Data Space

STELAR will design, develop, evaluate, and showcase an innovative Knowledge Lake Management System (KLMS) to support and facilitate a holistic approach for FAIR (Findable, Accessible, Interoperable, Reusable) and AI-ready (high-quality, reliably labeled) data that will be pilot tested in diverse, real-world use cases in the agrifood data space.

Funded by: EU
Duration: 09/2022 – 08/2025

Hephaestus – Machine Learning Methods for Adaptive Process Planning of 5-axis Milling

The project aims to research a framework for a learning 5-axes compensation of shape errors in milling processes based on a process-parallel material removal simulation and sophisticated machine learning (ML) strategies. Moreover, we aim to investigate the ability of knowledge transfer between different workpiece geometries, milling tools and machine tools for an enhanced process planning.

Funded by: DFG
Duration: 04/2021 – 12/ 2023

ITN NoBIAS – Artificial Intelligence without Bias

The core objective of NoBIAS is to research and develop novel methods for AI-based decision-making without bias. NoBIAS will deliver a cohort of 15 researchers trained to identify biased and discriminating AI-decision making and able to provide solutions that reconcile and fully exploit AI while ensuring compliance with legal and social norms.

Funded by: EU
Duration: 01/2020 – 12/2024
Participation via L3S Research Center, Hannover

BIAS – Bias and Discrimination in Big Data and Algorithmic Processing. Philosophical Assessments, Legal Dimensions, and Technical Solutions

We will provide philosophical analyses of the relevant concepts and principles in the context of AI (bias, discrimination, fairness), investigate their adequate reception in pertinent legal frameworks (data protection, consumer, competition, anti-discrimination law), and develop concrete technical solutions (debiasing strategies, discrimination detection procedures etc.).

Funded by: Volkswagen Foundation
Duration: 12/2018 – 05/2023
Participation via L3S Research Center, Hannover

Prof. Dr. Stefan Pickl

Operations Research – Research Group COMTESSA

TEACHING

10245	**Operations Research Lab – Decision Support**
10252	**Seminar BINF+BWIN**
10371	**Introduction to Business Information Systems**
10372	**Principles of Information and Communication Technology**
10401/2	**Introduction to Business Intelligence**
12311	**Data Mining and IT-based Decision Support**
12325	**Operations Research Lab – Decision Support**
12326	**Seminar Selected Chapters of Operations Research**
2038-V1	**AI and Data-driven Optimization**
3481-V1	**Data Science and Analytics**

ICE-Lecture 2022
Intelligence Collection Europe together with Gerhard Conrad "Cyber and Its Implications for Intelligence, Analysis and Decision Making"

FAIRS, CONFERENCES, SEMINARS

CRITIS2022 – The 17th International Conference on Critical Information Infrastructures Security, September 14 – 16, 2022, Universität der Bundeswehr München

ADDITIONAL FUNCTIONS

- Vice-President German Committee on Disaster Prevention
- Chair of the Advisory Board German Operations Research Society
- Member DEU NATO SAS Panel

Prof. Dr. Gunnar Teege

Formal Methods for Securing Things (FOMSET)

RESEARCH PROJECTS

MiKscHA – Microkernel for Static and Cloud Based High Security Applications

The project evaluates state-of-the-art methods for the highly secure operation of microkernel-based applications. The focus is on the secure start of the system. The methods used shall be sufficient to support a successful system certification.

Funded by: Airbus CyberSecurity
Duration: 01/2021 – 12/2023

SW_GruVe – Extending the Basics of Formal Verification for Software and Its Applications

The goal is to make formal verification amenable to the practical application in software development. The focus is hardware related software in the C programming language as part of operating systems. The verification uses the programming language Cogent and the proof assistant Isabelle.

Funded by: Bavarian Ministry of Economic Affairs, Regional Development and Energy (StMWi)
Duration: 10/2020 – 09/2023

TEACHING

1016 **Introduction to Operating Systems**

5505 **Operating Systems Security**

Prof. Dr. Arno Wacker

Privacy and Compliance

TEACHING

3480 **Secure Networks and Protocols**

55011 **Vulnerabilities and Attack Vectors Seminar**

55041 **Data Privacy**

55042 **Privacy Enhancing Technologies**

55061 **Introduction to Cryptography**

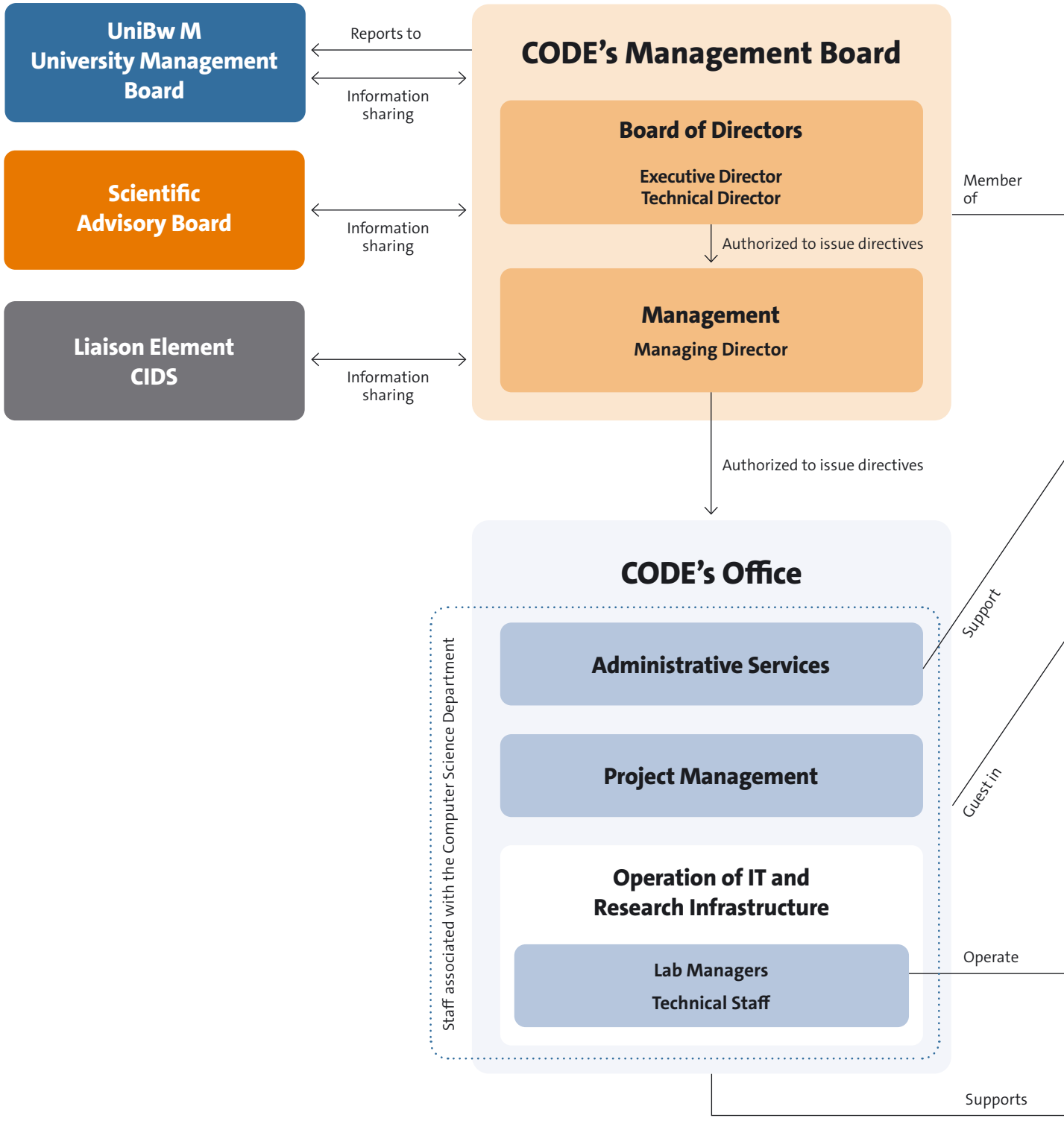
55091 **Penetration Testing**

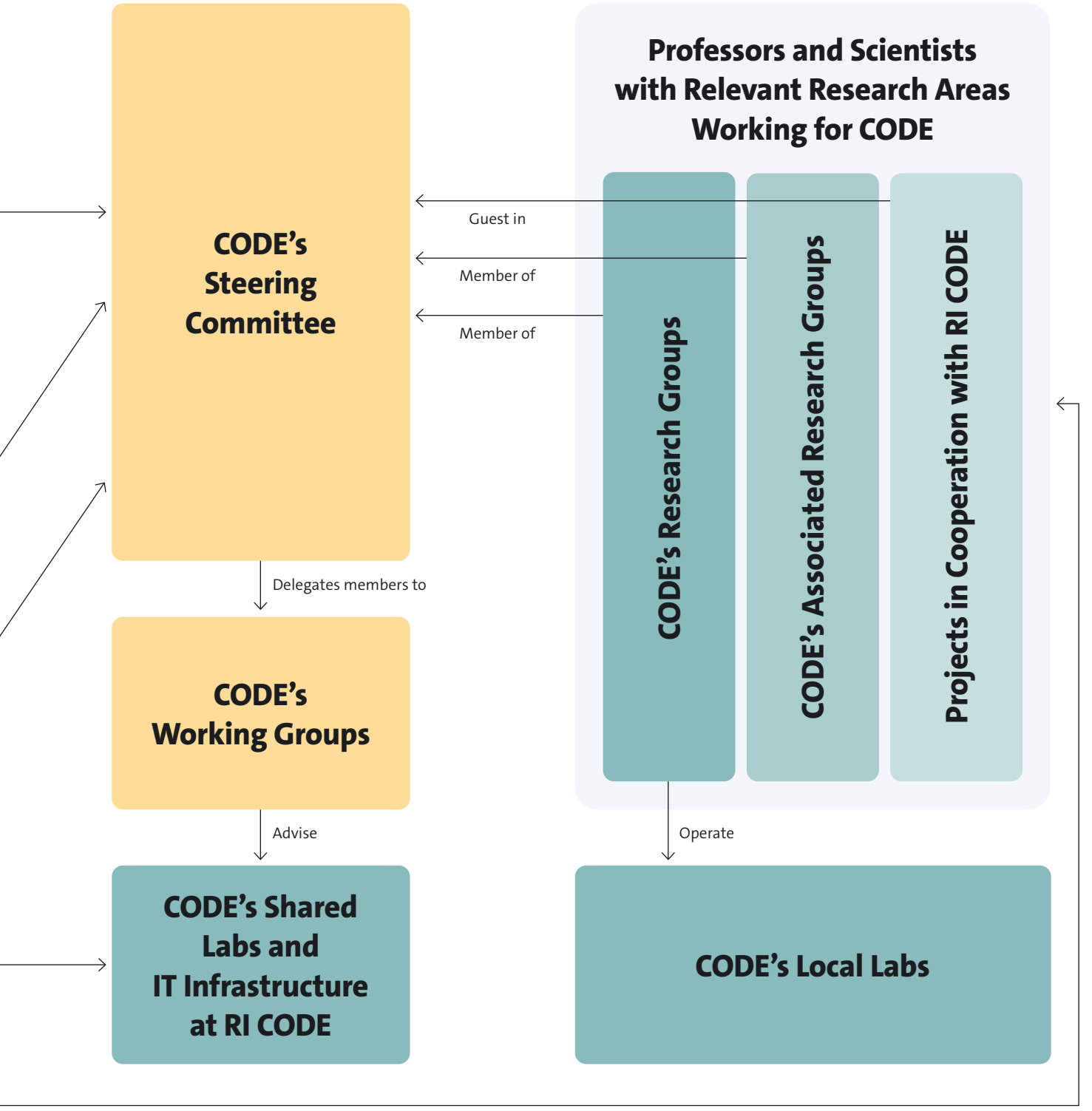
55093 **Penetration Testing Lab**

ADDITIONAL EVENTS

- 01.03.2022 – You're being watched – Tricks und Tools der Hacker
  - Students of the Anton-Bruckner-Gymnasium Straubing and the Max-Mannheimer-Gymnasium Grafing report on current research projects at the Universität der Bundeswehr München
- 05.10.2022 – Data-at-Rest – Also at Risk?
  - Talk at the Gymnasium Ulricianum Aurich in the context of the IT Security Day 2022, Kassel
- 06.10.2022 – Data-at-Rest – Also at Risk?
  - Talk at the am Gymnasium Ottobrunn, München

Organization of RI CODE




CODE's Steering Committee
Professors and Scientists with Relevant Research Areas Working for CODE
Guest in
Member of
Member of
CODE's Research Groups
CODE's Associated Research Groups
Projects in Cooperation with RI CODE
Delegates members to
CODE's Working Groups
Advise
Operate
CODE's Shared Labs and IT Infrastructure at RI CODE
CODE's Local Labs

How to Find Us

Research Institute Cyber Defence and Smart Data (CODE)
University of the Bundeswehr Munich
Carl-Wery-Straße 22
81739 Munich
Germany

code@unibw.de
+49 89 6004 7301 or 7306
www.unibw.de/code

Twitter: @FI_CODE
LinkedIn: Forschungsinstitut Cyber Defence (CODE)
YouTube: Forschungsinstitut Cyber Defence

Location Map

Editorial Information

PUBLISHER

Research Institute CODE
University of the Bundeswehr Munich
Carl-Wery-Str. 22
81739 Munich
Germany

MANAGEMENT OF RI CODE

Prof. Dr. Wolfgang Hommel,
Executive Director

Prof. Dr. Michaela Geierhos,
Technical Director

Marcus Knüpfer M. Sc.,
Acting Managing Director

PROFESSORS AT RI CODE

Prof. Dr. Florian Alt,
Professor for Usable Security and Privacy

Prof. Dr. Harald Baier,
Professor for Digital Forensics

Prof. Dr. Stefan Brunthaler,
Professor for Secure Software Engineering

Prof. Klaus Buchenrieder, PhD,
Professor for Embedded Systems/Computers in Technical Systems

Prof. Dr. Gabi Dreo Rodosek,
Professor for Communication Systems and Network Security

Prof. Dr. Michaela Geierhos,
Professor for Data Science

Prof. Dr. Udo Helmbrecht,
Honorary Professor at RI CODE

Apl. Prof. Dr. Marko Hofmann,
Professor for Serious Games

Prof. Dr. Wolfgang Hommel,
Professor for Software and Data Security

Prof. Dr. Johannes Kinder,
Professor for Computer Systems Hardening

Prof. Dr.-Ing. Mark Manulis,
Professor for Privacy

Prof. Dr.-Ing. Helmut Mayer,
Professor for Visual Computing

Jun. Prof. Dr. Maximilian Moll,
Junior Professor for Operations Research – Prescriptive Analytics

Prof. Dr. Eirini Ntoutsi,
Professor for Open Source Intelligence

Prof. Dr. Stefan Pickl,
Professor for Operations Research

Prof. Dr. Oliver Rose,
Dean of the Faculty for Computer Science at UniBw M,
Professor for Modeling and Simulation

Prof. Dr. Gunnar Teege,
Professor for Distributed Systems

Prof. Dr. Arno Wacker,
Professor for Data Privacy and Compliance

MEMBERS OF THE ADVISORY BOARD (IN 2022)

From the Department for Computer Science at the University of the Bundeswehr Munich:

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Ulrike Lechner

Prof. Dr.-Ing. Helmut Mayer

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

Other Members

Prof. Dr. Johann Pongratz,
TU Dortmund

Wolfgang Sachs,
Head of Division CIT I.2, Federal Ministry of Defence

Dr. Norbert Gaus,
Executive Vice President of Siemens AG

Dr. Ralf Wintergerst,
Chairman of the Management Board of Giesecke + Devrient

EDITING AND COORDINATION

Benjamin Bellgrau, M. Sc.,
Acting Public Relations Officer

ART DIRECTION

Tausendblauwerk Design Agency
Michael Berwanger

www.tausendblauwerk.de

PROOFREADING

Dr. Michelle Ruth Büscher,
Technical Translator/Editor

PRINTED BY

Holzer Druck und Medien

www.druckerei-holzer.de

REGULATIONS

Editorial deadline: March 2023

Title illustration: Adobe Stock / KanawatTH

ISBN: 978-3-943207-72-9 | ISSN: 2748-9485

Also published as an electronic publication
(ISBN: 978-3-943207-73-6 | ISSN: 2748-9507)
as well as in German language
(ISBN: 978-3-943207-70-5 | ISSN: 2748-8780).


Universität der Bundeswehr München
CODE RI
Research Institute
Cyber Defence
Universität der Bundeswehr München