Universität der Bundeswehr München

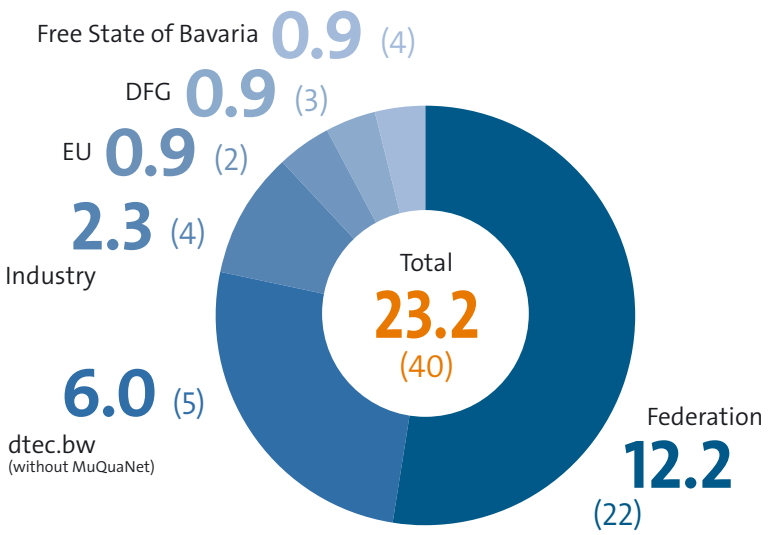
CODE
ANNUAL REPORT
2021

Research Institute Cyber Defence
Universität der Bundeswehr München

Project Funding

In 2021, a total of 40 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 greater Munich area Quantum Internet

MuQuaNet

Participating Professorships

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 2021, CODE employees came from 15 countries.

Cooperation Partners***

In 2021, RI CODE cooperated with 70 partners in 25 countries.

Legend

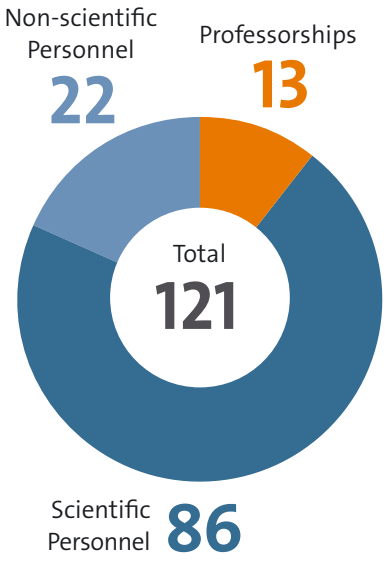
- Location of RI CODE
- 1 — Number of CODE employees from the Country of origin
- 1 — Number of international cooperation partners in the respective country
- Countries with cooperation partners and employees

*** More information about contacts and cooperation partners can be found from p. 66.

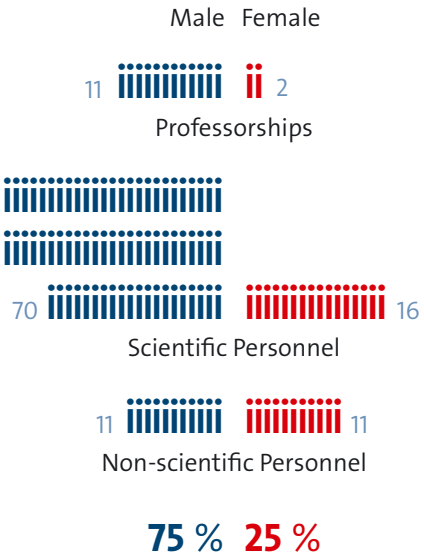
Staff Structure

**RI CODE had a total of 121 employees in 2021.
The percentage of women was 25.**

Employees



Gender Share

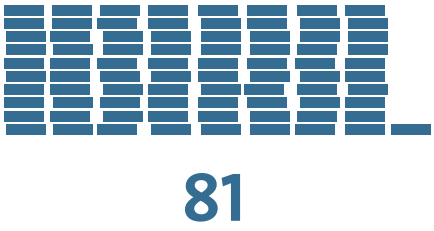


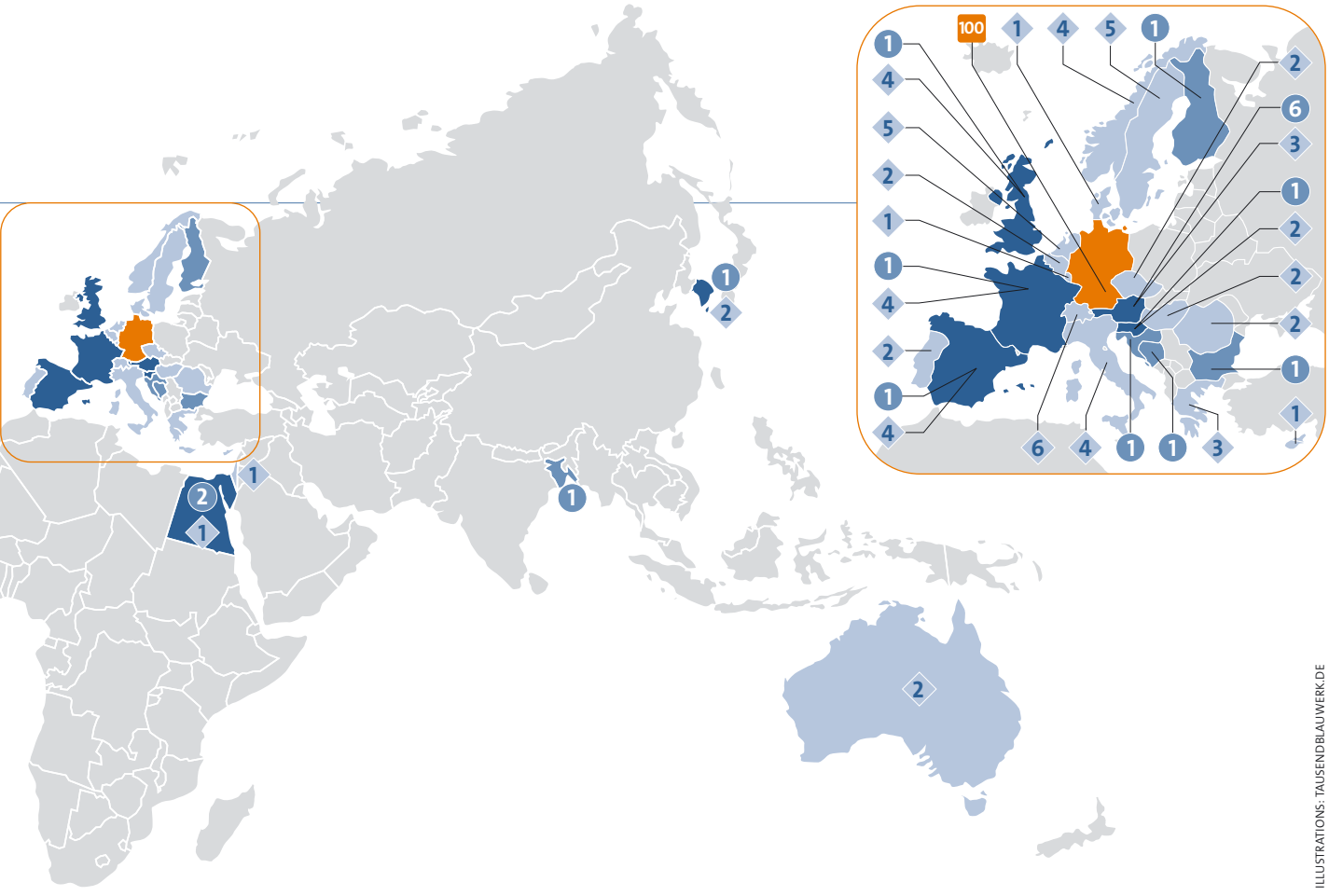
Research Work

Overview of doctorates and publications at RI CODE 2021

Doctorates

Publications





ILLUSTRATIONS: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
ANNUAL REPORT
2021

Research Institute
Cyber Defence
Universität der Bundeswehr München

Preface by the President

Global crises are on the rise, and so are the threats to our free, democratic society. The COVID-19 pandemic is not yet over, and the military conflict between Russia and Ukraine, for which Vladimir Putin is responsible, is keeping us on tenterhooks. Again there is war in Europe with much suffering and destruction, which seemed unimaginable after the fall of the Iron Curtain. Once again, the dangerous political developments show us how great the need for scientifically based knowledge is.

With its research centers, the Universität der Bundeswehr München focuses decidedly on topics of security and crisis management. This involves both technical aspects, such as the problem of digital attacks on computer systems, as well as how society deals with the new challenges. Our Research Institute CODE (RI CODE) for Cyber Defence and Smart Data addresses precisely these university priorities and we can look back on a successful development since its founding as a research center in 2013, which has most recently led to a sharpening of its profile towards the needs of the Federal Ministry of Defence (BMVg) and the Bundeswehr (German Armed Forces).

Globally, there is a growing number of cyberattacks, including on software systems used to supply food and other essential raw materials. In addition, disinformation campaigns and the systematic spread of fake news are becoming more frequent, which in the worst case can lead to the destabilization of entire political systems. To meet these challenges, the Bundeswehr and society depend on scientifically trained, well-educated specialists and innovative research results. As one of the leading research institutes, RI CODE offers both basic and application-oriented university research in the fields of cybersecurity, smart data/AI and quantum technology.

I am therefore extremely pleased that the institute continues to grow: In 2021, more than a dozen projects were launched in the research groups, some of which are still very young, and more than 80 publications were written. The number of employees increased to 121.

In 2021, there was a change at the top of RI CODE: Wolfgang Hommel, Technical Director until October 2021, took over as Executive Director and succeeded Gabi Dreo Rodosek, who will devote herself to new research priorities after eight years in office. The new Technical Director is Michaela Geierhos. I wish the new Board of Directors every success and all the best for a promising future of the institute!

The excellent cooperation with the BMVg is also reflected in the transfer of the previous CODE Managing Director to the CIT I 2 unit, where Volker Eiseler will coordinate the further development of RI CODE and the cyber cluster at the Universität der Bundeswehr München from a ministerial perspective.

I am pleased to recommend the informative reading of this annual report. With best regards and wishes,

Prof. Dr. Merith Niehuss
President Universität der Bundeswehr München


Marcus Knüpfer, Michaela Geierhos, Wolfgang Hommel

Dear Readers,

The only constant in life is change. In the past year, numerous innovations and some personnel changes shaped CODE. With this annual report, we would like to give you an overview of the activities of our research groups and our annual highlights.

We are particularly pleased that CODE's steady growth continued in 2021. Numerous qualification positions for young scientists were created within the CODE professorships in more than a dozen new research projects – predominantly with partners from the Bundeswehr, federal authorities and the Digitalization and Technology Research Center of the Bundeswehr (dtec.bw). Added to this were further collaborative projects by colleagues Prof. Dr.-Ing. Helmut Mayer and Prof. Dr. Stefan Pickl. Under the scientific leadership of Dr. Sabine Tornow, our new research pillar in the field of quantum technology has been continuously expanded since April 2021. You can read more about the technical foundations of quantum computing and our latest activities in this area in the "Highlights" section.

Another highlight in 2021 was the CODE Annual Conference, this time addressing the topic of "Supply Chain Sovereignty". Hundreds of guests dialed in virtually to the three-day event to follow high-profile panel discussions, participate in workshops, or listen to pitches on innovative ideas in cyber/IT. Then, in fall, RI CODE hosted participants from seven nations to practice cybersecurity together during the "Multi-Lateral Cyber Defense Exercise". RI CODE's annual "Capture the Flag" event, successfully held hybridly for the first time, saw 14 teams participate on-site and 15 in online competition.

Coordinating virtual and hybrid events and, in many cases, doing research from home is proving to be an elaborate feat, despite becoming increasingly routine. We would therefore like to thank all members of the CODE office and our colleagues who are committed to the joint success of CODE with their research groups. Special thanks also goes to the Head of Department CIT, Lieutenant General Vetter, the Inspector CIDS, Vice Admiral Dr. Daum, our direct contacts in the Federal Ministry of Defence and in the management of the Universität der Bundeswehr München for their great support in the past year.

As the new CODE Management Board – which includes Marcus Knüpfer as acting Managing Director – we are grateful for the trust placed in us, which we hope to live up to in the future by successfully developing the RI CODE together. We wish you a great deal of enjoyment and exciting impulses while reading our annual report 2021!

FIG.: PRIVAT; FI CODE

Prof. Dr. Wolfgang Hommel

Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Management of the Research Institute CODE

Contents

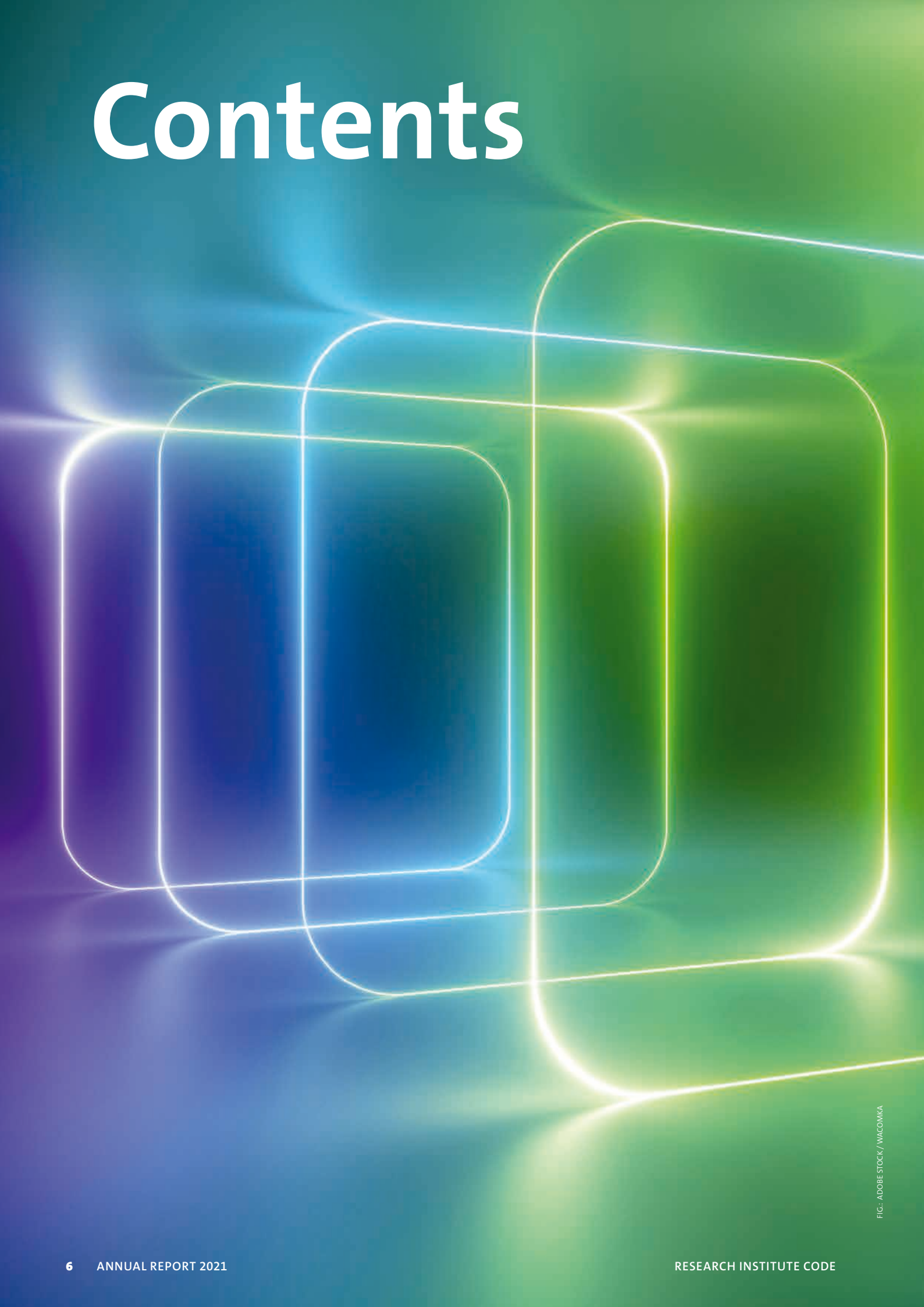


FIG.: ADOBE STOCK / WACOMKA

OUR MISSION STATEMENT

MISSION

Our goal is to research and develop technical innovations and concepts for the protection of data, software and systems in a holistic and interdisciplinary manner.

RESEARCH

We conduct both basic and applied research and technology development in the fields of cyber defence, smart data and quantum technology for the benefit of society and the Bundeswehr.

VALUES

Our identity is characterized by solidarity, respect for the individual, a genuine culture of discussion, and loyalty.

FIG.: STNAZKUL / ADOBE STOCK

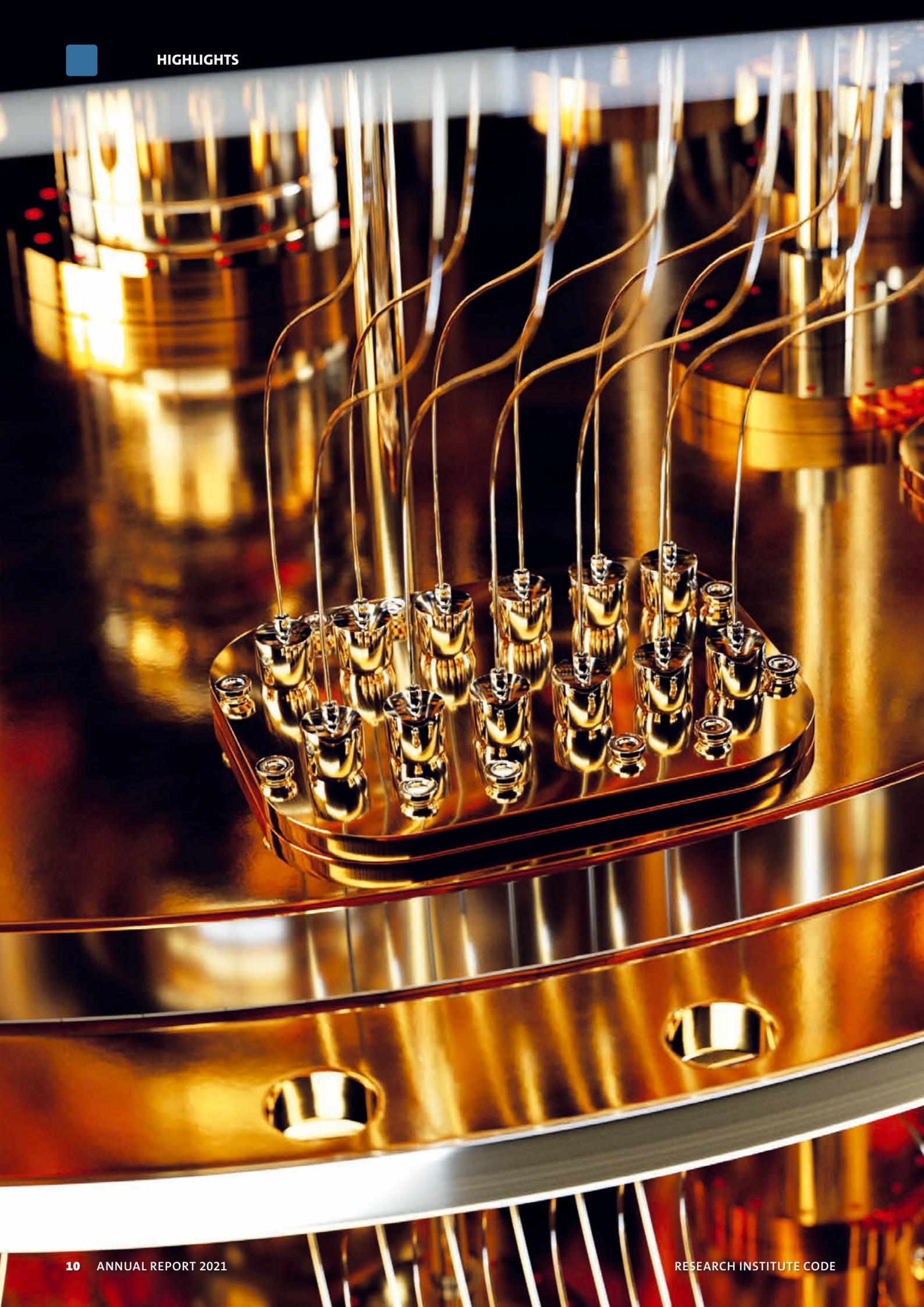
The Research Institute CODE is a central scientific institution of the Universität der Bundeswehr München and, with its expertise, creates innovation in the field of cyber/IT for the Bundeswehr.

WE CONDUCT both basic and applied research and technology development in the fields of cyber defence, smart data and quantum technology for the benefit of society and the Bundeswehr.

Our goal is to research and develop technical innovations and concepts for the protection of data, software and systems in a holistic and interdisciplinary manner. To this end, we pool scientific expertise and work closely with partners from the Bundeswehr, government agencies, research and industry. An essential element of our work is the transfer of results and new technologies into practice, so that they can add value and be used in our partners' operational areas. In addition, we want to create acceptance for tomorrow's privacy-compliant and secure technologies and are committed to our role model function not solely in teaching, in which we prepare students at the Universität der Bundeswehr München for the IT challenges of their professional lives.

We want to make Germany safer. To this end, we conduct research, maintain long-term cooperations and stimulate networking and knowledge transfer. With the broadly diversified competencies of our professorships and research groups, we provide advice to decision-makers from the Bundeswehr as well as from politics. Direct access to quantum computers enables us to find solutions today for tomorrow's challenges. Our Cyber Range and teaching infrastructure meet the latest standards, enabling us to fulfill our statutory mission of providing advanced training for the Bundeswehr. It is not only in this context that our young academics are our most valuable asset. Together with them, we shape the future and drive innovation. That is why individual academic development is so important to us at RI CODE.

We are open to scientific discourse and actively engage in public relations work. In doing so, we are aware of our responsibility towards society and the Federal Republic of Germany. With its broad professional expertise, the Scientific Advisory Board actively supports the RI CODE in its strategic development. Our organizational structure is designed for cooperation. At the same time, the RI CODE is not a mere working community: Our identity is characterized by solidarity, respect for the individual, a genuine culture of discussion, and loyalty. We give our best every day and are willing to be measured against it. ■



Highlights

From the Institute

FIG.: ADOBE STOCK / BARTEK WRÓBLEWSKI

The participants of the multi-day exercise came from seven nations.

Multi-Lateral Cyber Defense Exercise at RI CODE

Training for Cybersecurity

24 participants, seven nations, six teams and five days: those are the key figures of the Multi-Lateral Cyber Defense Exercise (MLCD), which was conducted by the Cyber and Information Domain Services of the Bundeswehr (CIDS) at the Research Institute CODE from October 4th to 8th, 2021. The MLCD is a defensive-oriented international cybersecurity exercise that promotes knowledge sharing and cooperation. It was held for the second time in 2021.

Teamwork in the Cyber Range

The Cyber Range "ICE & T" of RI CODE provided an ideal environment for the international event: On the technically well-equipped premises, there was opportunity for the participants to exchange ideas and work together to develop solutions for the complex cybersecurity scenarios. A special feature of the MLCD exercise: the national delegations were divided into multinational teams in accordance with the cooperative nature of the exercise. The idea of mutual learning was also reflected in the decision not to score points as well as in joint debriefings on the individual scenarios in form of open discussions, moderated by the trainers. In this way, the participants were able to learn about different approaches and techniques for mastering the tasks.

Individualized Approach and Personal Support

In the run-up to the event, the ICE & T trainers developed the scenarios, adapted them to the needs of the participants, and assessed various options for evaluation and debriefing. During the event, the trainers conducted the morning situation briefings, guided the scenarios to generate the greatest learning impact, fostered teamwork, and provided thought-provoking input to the participants. During the daily debriefing, the lessons learned were collected in an instructional discussion with all the teams. A possible solution as well as the attack vectors were presented, and appropriate measures for defence were developed together. The evaluation of the exercise helped to further develop and improve scenarios, the technical infrastructure and the didactic approach.

Malware, Phishing, Ransomware: Varied Scenarios

The scenarios trained during the exercise aimed at the detection, analysis and mitigation (defence) of the simulated cyberattacks. All five were based on or modeled in accordance with real incidents. They included complete sequences from the initial attack to the exfiltration of data to the covering of traces. The "Hi Jack!" scenario, for example, involved a cyberattack on an online banking portal, in which parts of the inter-

FIG.: UNIBW M / SIEBOLD

Vice Admiral Dr. Thomas Daum, Inspector CIDS, personally visited the exercise to learn about its course and contents.

nal network were taken over using malware to steal access data. In the "Dirty Dancing" task, a manipulated Word document made its way onto an unsecured file storage system, causing the encryption of data by the well-known WannaCry ransomware, along with a ransom demand. "The Whole Nine Yards" represented the most complex scenario of the exercise: here, the exposure of a smartphone to initially obtain credentials via a phishing email was simulated. In this scenario, a variety of other attack vectors ultimately led to sensitive company data being stolen.

All cyberattacks were partially automated, and each of the six teams, working together on threat mitigation was placed in the same situation in parallel. In the course of the exercise, it became apparent that the groups approached the tasks differently and achieved success in very different ways.

High-Ranking Guests from all over Europe

Overall, the exercise, given its international focus, attracted a great deal of interest: On the second day, high-ranking military representatives from Great Britain, France, Poland, Luxembourg, Austria, the Netherlands, Switzerland and Germany accepted the invitation of Vice Admiral Dr. Thomas Daum, Inspector Cyber and Information Domain Services (CIDS), and visited the Research Institute CODE as well as the campus of the Universität der Bundeswehr München in Neubiberg. During their stay, Dr. Daum and the guests learned about the scope of the MLCD and the setup of RI CODE's Cyber Range: ICE & T provides education and training for cybersecurity experts, and not just in the context of the exercise. For example, UniBw M's computer science and cybersecurity degree programs include various internships that are conducted in the Cyber Range. In addition, ICE & T serves as a laboratory for scientific projects addressing various technical questions, for example in the context of the EU project CONCORDIA. ■

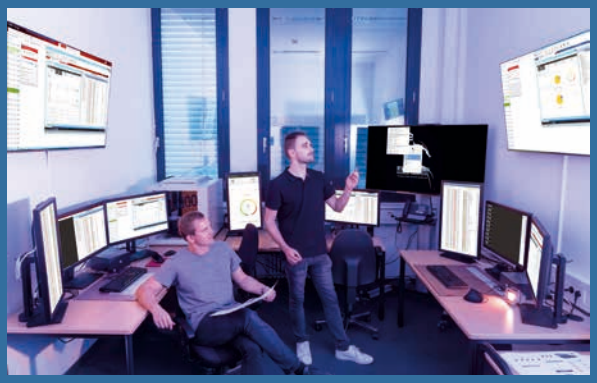
More about the MLCD Exercise

https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/uebungen/mlcdi-ueben-fuer-die-cyber-sicherheit-5231754

Military representatives from Great Britain, France, Poland, Luxembourg, Austria, the Netherlands, Switzerland and Germany.

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 cybersecurity 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 cybersecurity products and approaches.

During training, cybersecurity 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 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.

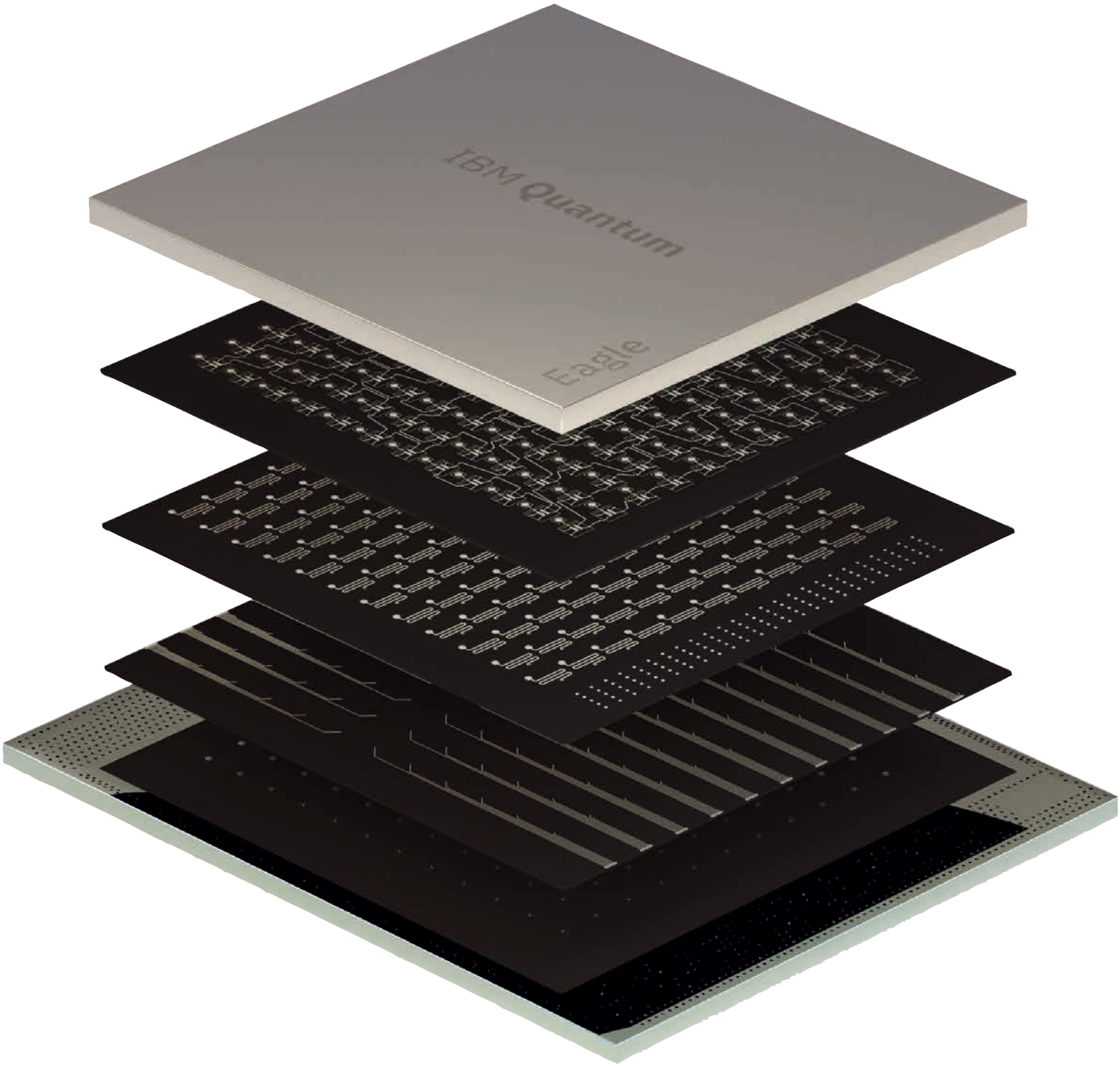
ICE T
IT Competence
Education & Training

More Information

code@unibw.de

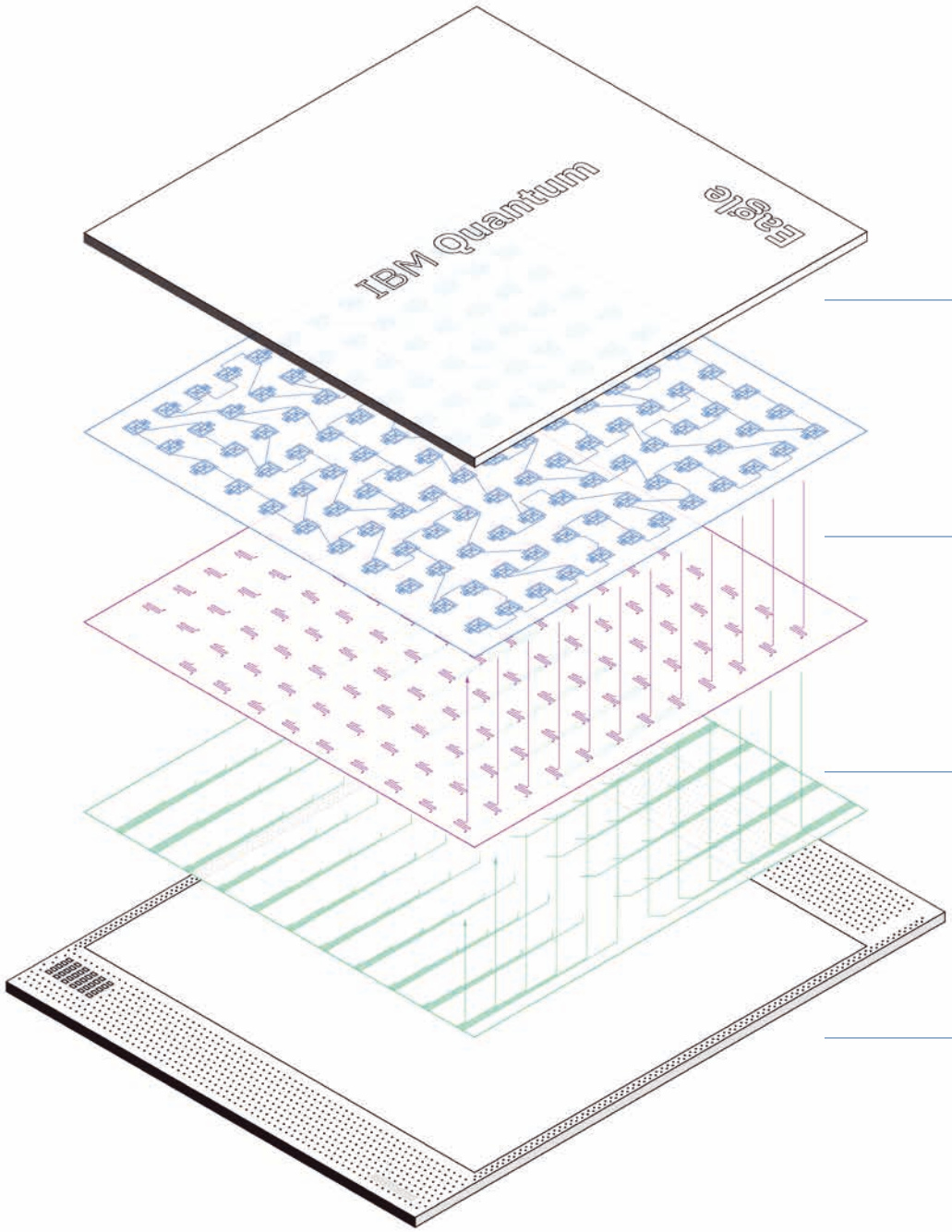
Information flyer
"Cyber Range":
https://go.unibw.de/84

FIG.: UNIBW M / SIEBOLD.



Quantum technologies

Towards the practical relevance of quantum computing



Qubit plane
Transmon qubits attached to an interposer chip through bump bonds offer hardware simplicity in a scalable architecture with controllable features.

Resonator plane
Resonators for qubit readout wired through connectors. Measured shifts in the frequency of the resonator depend on the state of the qubit.

Wiring plane
Buried wiring layer connects to the other planes through superconducting thru-substrate vias, providing the flexibility to efficiently route signals to the qubit plane with low crosstalk.

Interposer
Leverages CMOS packaging techniques, including thru-substrate vias, to exploit the third dimension to electrically connect the qubits to the other planes and deliver the signals while protecting their coherence.

FIG.: CARL DE TORRES OF STORYTK FOR IBM.

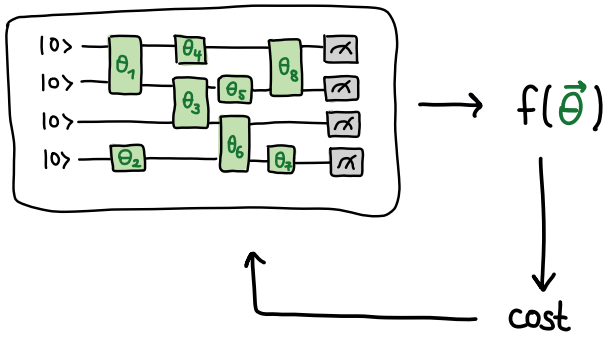
The experimental control of quantum systems enables the development of new quantum technologies, by exploiting the quantum properties of superposition and entanglement. This leads to novel kinds of navigation, sensing, data transmission and data processing, which can potentially also be of great relevance for the Bundeswehr.

QUANTUM COMPUTING basically is the backbone of quantum technologies: 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. Although most of these technologies are still at a very early stage, it is possible to explore them at the Research Institute CODE. Since 2018, RI CODE at the Universität der Bundeswehr München has, as an IBM Quantum Hub, one of only a few exclusive access points to the IBM

IBM Q Computation Center.

quantum computing infrastructure existing in the world. The current availability of quantum computers (up to 127 qubits) enables researchers at RI CODE to test quantum algorithms and heuristics, as well as error mitigation schemes, and to conduct experiments to explore and apply quantum information processing.

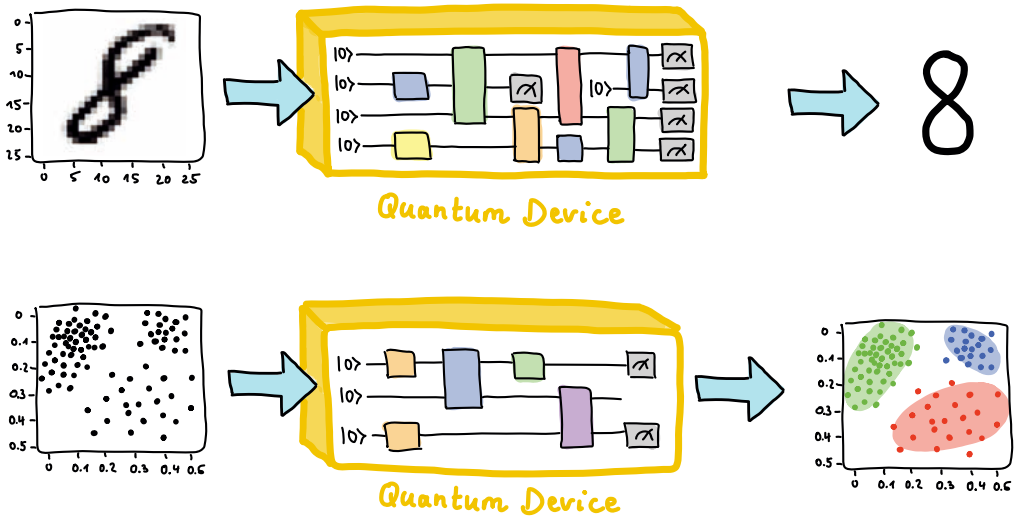
Qiskit, a software development kit, can be used to program quantum computers at the circuit, pulse, and algorithm levels. It should be noted that, when programming quantum algorithms, the "jobs" cannot simply be sent to the quantum computer. Some more work is required here, e.g., by applying error mitigation techniques and transpiler optimizations. On the way of quantum computing becoming practically relevant, various applications in the area of optimization, machine learning and quantum simulation are being pursued at RI CODE, and methods for circuit optimization and error mitigation are being developed.



Visualization of a circuit for quantum variational algorithms.

One of these important applications is **quantum optimization**. Many problems from logistics, supply chain management, or cryptanalysis can be transformed into an optimization task whose output is a state, a bit sequence, or a distribution. For many of these problems, only approximate solutions can be found using supercomputers. Therefore, even small improvements by heuristic quantum algorithms are of economic interest. Quantum variational algorithms enable a learning-based approach. The parameters of the circuit are found by optimizing a cost function. Quantum variational algorithms are continuously improved with regard to theory and their experimental implementation.

Supervised and unsupervised quantum machine learning can also be realized using quantum variational algorithms. These include quantum clustering, quantum Boltzmann machines, kernel methods, quantum convolutional neural networks, quantum support vector machines, quantum autoencoders, and generative adversarial quantum networks.

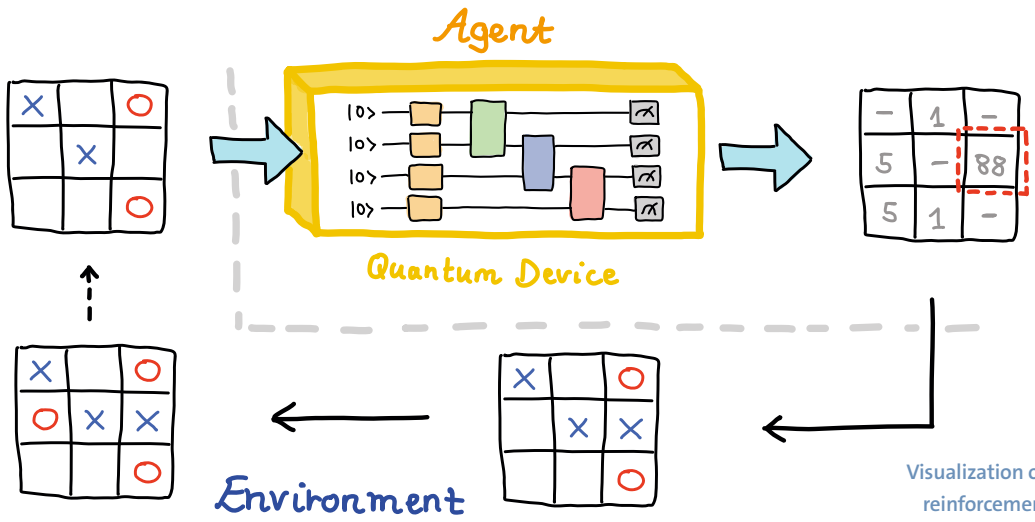


Visualization of supervised and unsupervised quantum machine learning.

Generative adversarial networks are a powerful tool for classical machine learning: a so-called generator tries to generate statistics for data that resemble those of a real data set, while a discriminator tries to distinguish between real and fake data. The learning process for the generator and discriminator can be viewed as an adversarial game, and under reasonable assumptions it converges to the point where the generator produces the same statistics as the real data and the discriminator is unable to distinguish between real and generated data. Generative adversarial quantum networks work in a similar way, with the data consisting of either quantum states or classical data, and the generator and discriminator represented by quantum circuits. Their applications include, for example, anomaly detection.

Reinforcement learning, another main area of machine learning, is concerned with the data-based optimization of multi-step decision-making processes within a given system, applied to various attacker-defender scenarios. The goal of the algorithms is to identify a strategy that achieves a given state of the system over multiple time steps. The unique feature of reinforcement learning is that the algorithm has no information about the system it is interacting with. Through interaction alone and evaluating the actions performed, the algorithm in training learns to achieve the goal.

Quantum computing offers enormous potential to reduce the required computing power in reinforcement learning through the concepts of superposition (see info box “Quantum Computing”, p. 21) and entanglement. Policy-gradient-based reinforcement learning approaches have been used to develop quantum hybrid algorithms that replace classical neural networks with quantum variational circuits. This offloads the computationally intensive part of the algorithm to the



Visualization of quantum reinforcement learning.

FIG.: IBM CORPORATION/CORINNE ZHOU; RI CODE (3)

IBM quantum computer. The results show a huge advantage of the new algorithm in terms of the required computational power and thus faster training.

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

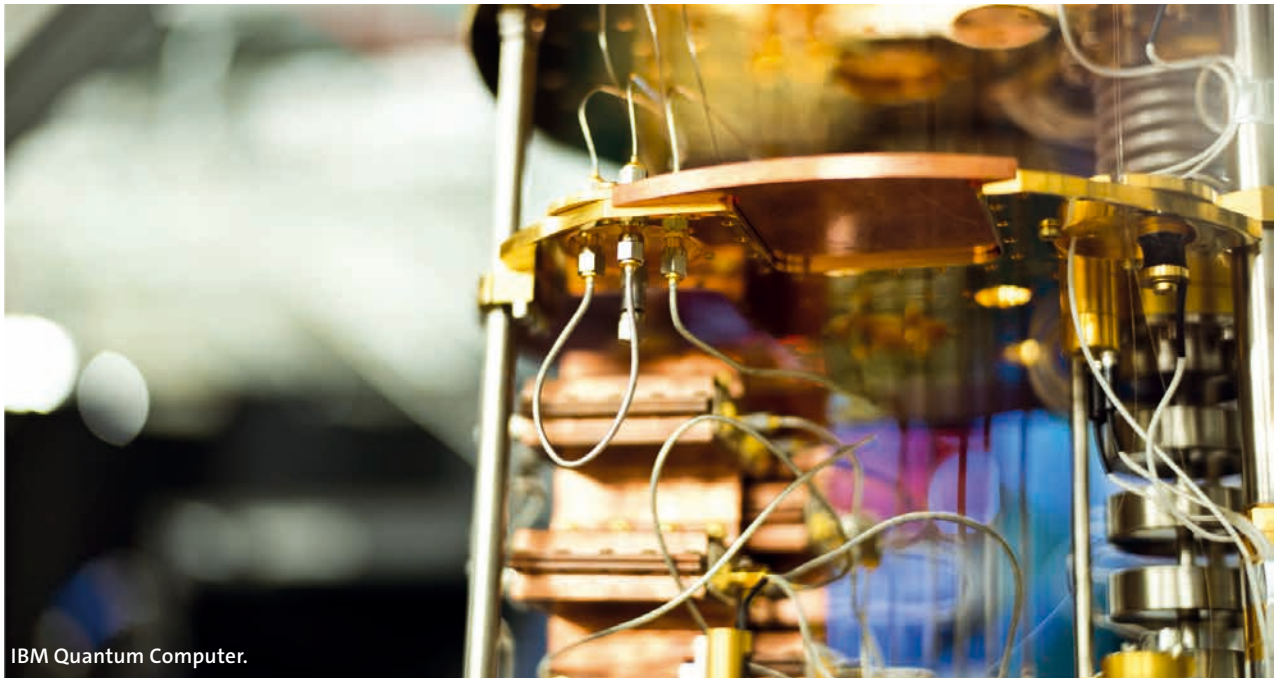
To explore quantum information processing, various **experiments can be performed on a superconducting quantum computer**, such as Entanglement Measurement, Tomography, Quantum Optimal Control, Calibration or Pulse Level Programming, Learning from Experiments or Quantum Algorithmic Measurement. In addition, 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.

Until now, the depth of quantum circuits that can be reliably executed on current quantum computers has been limited by their noisy operations and the small number of qubits. Therefore, scaling remains a current problem that must 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, small quantum computers can execute an algorithm requiring more qubits than are available, and runtime and accuracy can be optimized.

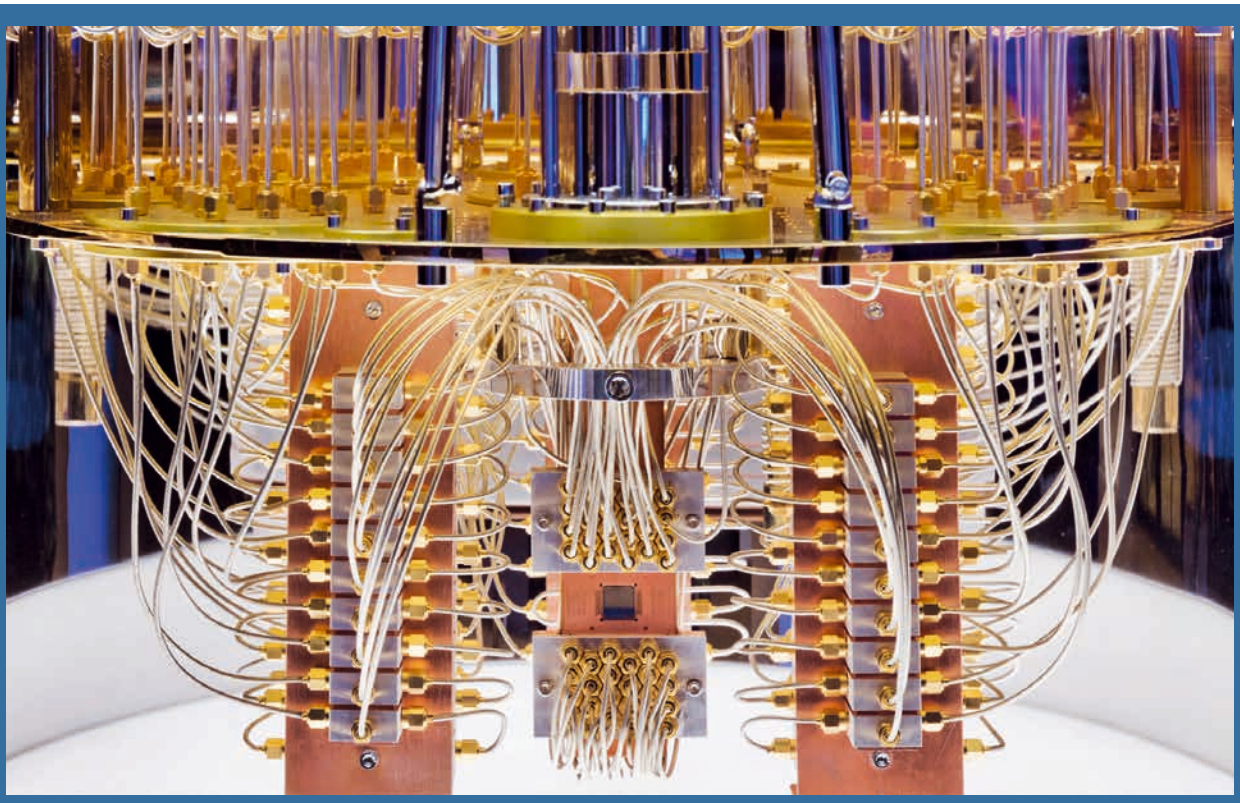
Methodological aspects of quantum computing are explored using tensor network methods, for which appropriate simulators are available on the IBM quantum network, and the ZX calculus, a graphical language that can be used to represent arbitrary linear mappings between qubits. The ZX graphs are equipped with a complete set of graphical rewriting rules that allow diagrammatic rather than equality-based reasoning. This calculus has been successfully used to optimize quantum circuits.

The topics from applied research were passed on to students and employees of service providers close to the Bundeswehr in practice-oriented lectures at Munich universities and in **workshops** and presented in lectures at conferences and seminars. In addition, Bachelor's and Master's theses were supervised. The scientists organized three online workshops on the topics of quantum sensors, quantum computing and quantum communication. ■



IBM Quantum Computer.

FIG.: IBM CORPORATION



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 7370

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

Dr. Leonhard Kunczik
leonhard.kunczik@unibw.de
+49 89 6004 3023

Report on the Annual Conference “CODE 2021”

Secure supply chains, digitally sovereign Europe?

From July 20 to 22, 2021, the Annual Conference of the Research Institute CODE under the motto “Supply Chain Sovereignty: Reality or Illusion?” took place in an on-line-only form due to the pandemic. The focus of CODE 2021 was on supply chains, which on the one hand are at risk from analog threats, but on the other hand have also increasingly become the target of hackers. Several hundred guests dialed in to the three-day event.

THE COVID-19 PANDEMIC has shown how important collaboration and digital processes have become in our everyday lives. More than ever, it is clear that we can tackle the major challenges in Europe only together. In this context, international supply chains are important: If one partner is compromised, this affects all parts of the supply chain. For instance, entire production lines can fail or business units that depend on a specific software can become incapacitated. Examples are the SolarWinds hack in 2020 or the attacks on the Kaseya software, which led to food shortages in Sweden in the summer of 2021. Reason enough to put "Supply Chain Sovereignty" in the focus of the CODE Annual Conference 2021, which featured once again renowned experts from industry, research, military and authorities.

The welcome address by the President of the Universität der Bundeswehr München, Prof. Dr. Merith Niehuss, kicked off the three-day event. Prof. Dr. Gabi Dreo Rodosek, as RI CODE's Executive Director, then warmly welcomed the guests and briefly briefly presented the latest developments at the institute. One of the topics was the first CODE Annual Report, which contains around 70 pages on the highlights, research projects and other activities of the institute in the reporting year 2020.

Opening Statements and Impulses

Opening statements followed – from German Defence Minister Annegret Kramp-Karrenbauer, Bavarian Digital Minister Judith Gerlach and Dr. Florian Herrmann, Head of the Bavarian State Chancellery. Defence Minister Kramp-Karrenbauer spoke positively about the Research Institute CODE: "CODE is rightly one of the top institutes in Europe when it comes to questions of cyber defence. Large-scale projects such as CONCORDIA bring together the key players in cybersecurity, pool IT competence, encourage innovation. This way they strengthen Europe's digital sovereignty." Dr. Flo-

Federal Minister of Defence Annegret Kramp-Karrenbauer made a video statement after being welcomed by president Prof. Dr. Merith Niehuss (left) and Prof. Dr. Gabi Dreo Rodosek.

FIG.: ADOBESTOCK/ MAHA HEANG 245789; UNIBW M / SIEBOLD

Dr. Annegret Bendiek (top left) moderated a panel discussion with Laura Carpini, StS Benedikt Zimmer and StS Dr. Markus Richter.

rian Herrmann emphasized the relevance of the CODE Annual Conference: "This international format on cybersecurity and digitalization bluntly reveals where action is urgently needed."

The rest of the morning's program included keynote speeches by Benedikt Zimmer, State Secretary at the Federal Ministry of Defence, and Dr. Markus Richter, State Secretary at the Federal Ministry of the Interior as well as Federal Government Commissioner for Information Technology. Among other points, Richter highlighted the importance of protecting critical infrastructures, saying, "We need to secure our critical infrastructures, especially the 5G networks. 5G creates a strong industrial ecosystem in the area of mobile networks in Germany and Europe."

Debates on Functional Supply Chains for Europe

In a total of three high-profile panel discussions throughout the day, guests from academia, business, the military, and authorities addressed the following questions, among others: How can governments and companies counter security risks in supply chains? What are the biggest obstacles that need to be removed? How can resilience be increased?

The panelists' responses consistently referred to three points that are important requirements for functional supply chains: A commitment to innovation and flexibility, a need to establish European standards or certifications for key critical infrastructure components, and collaboration at the international level, especially across Europe. Laura Carpini, Cybersecurity Coordinator at the Italian Ministry of Foreign Affairs and International Cooperation, commented, "We live in a connected world – international relations are key. They can make a really significant difference. Together, we are stronger."

Workshop Session and Innovation Conference

As the Technical Director, Prof. Dr. Wolfgang Hommel chaired the second day of the CODE Annual Conference: Within the framework of workshops and the innovation conference, current issues were addressed, including those relating to the motto "Supply Chain Sovereignty". As on the first day of CODE, conference guests were able to learn about new developments in the field of cybersecurity and make contact with partners from industry at the virtual trade fair that took place in parallel. In addition, a social platform provided opportunity for casual exchange and networking.

In the run-up to the annual conference, a call for workshop proposals took place for the first time in 2021. Numerous representatives from research institutes, authorities and commercial enterprises responded to the call and submitted ideas on technical and political aspects of cybersecurity and smart data. The proposals were diverse and covered areas such as international politics and economics, methods of future defence policy, the health sector, and quantum computing. As a result, the number of parallel workshops was particularly high this year: a total of 10 workshops took place and enjoyed lively participation. More detailed insights are provided in the following two exemplary descriptions.

Workshop "Bio-Cyber-Security Risks and Opportunities at the Intersection of Health Service, Biotechnology and Cyber"

Bio Cyber Security (BCS) is a relatively new research area that aims to protect digitized bio and health data. The goal here is to secure individuals, the public, healthcare infrastructure, and the development of biotechnological innovations. The exponential growth in the digitization of biology and biotechnology is beneficial to several sectors in research and the bioeconomy. However, these advances should also raise concerns about new risks and threats that are neither exclusive to cybersecurity nor "biosecurity" but are a hybrid field in their own right. Therefore, this workshop addressed the following questions: How should a BCS index be designed to be useful for technical, security, and policy purposes? Where should the focus be to identify vulnerabilities, and where can efforts to address BCS threats be concentrated (e.g., in health infrastructure and cybersecurity)? What might a comprehensive interdisciplinary mechanism of collaboration among technical, industry, and policy experts look like to mitigate BCS threats beyond national security and to develop new paradigms for information gathering, intelligence, and analysis? In conclusion, the consensus was that BCS will become increasingly important in the future and therefore shows very high potential for development.

Workshop "Security and Sovereignty of Cloud Systems"

Digital sovereignty describes the ability of a community to develop, use, operate and control digital products and services. This includes the ability to ensure the use of trusted technology (both hardware and software,

FIG.: FI CODE

The virtual trade fair allowed guests to network and learn about new developments in cybersecurity.

considering the entire supply chain), secure connectivity, trusted operation of infrastructure, and continuous security monitoring. As far as cloud services are concerned, users seem to largely accept the dominance of non-European providers (e.g., Google or Amazon). However, individual governments and key European initiatives have recently recognized the demand for national sovereignty, particularly regarding their own cloud applications, leading to the GAIA-X [1] initiative to build a high-performance, competitive, secure, and trustworthy data infrastructure for Europe. In addition, cloud services continue to expand into the government ("Federal Cloud") and also into the military domain, where the need to protect national interests is becoming even more dominant. Participants in this workshop therefore discussed strategies and solutions for ensuring security and sovereignty for cloud systems. A particular focus was on the government and military sectors.

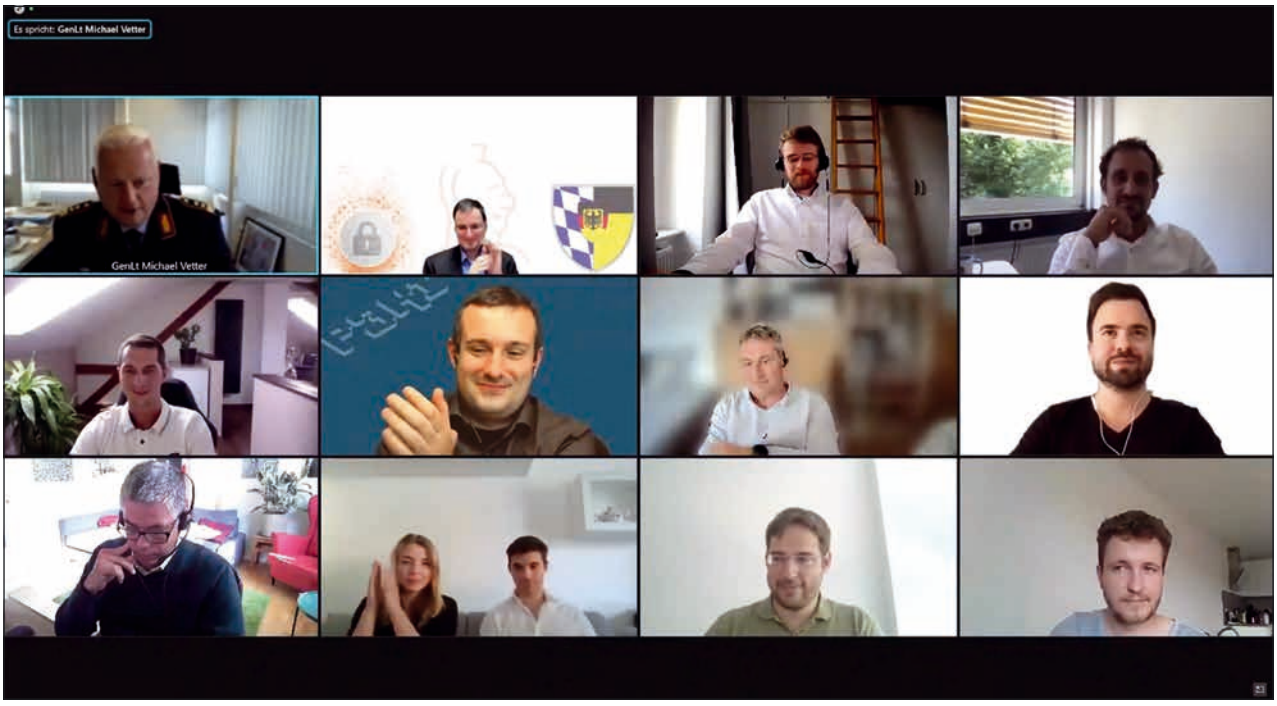
Innovation Conference: Twelve Innovative Ideas, Three Winners

Following the workshop session, the innovation conference on cyber and information technology took place in the afternoon of the second day. Lieutenant General Michael Vetter, Head of the Directorate-General for Cyber / Information Technology (CIT) at the Federal Ministry of Defence, which is responsible for research and technology as well as innovation management cyber/IT, emphasized the relevance of the task for promoting innovation for the benefit of greater digital sovereignty and also emphasized the importance of the newly established Digitalization and Technology Research Center of the Bundeswehr (dtec.bw) and the Agency for Innovation in Cybersecurity: both agencies could be established despite the pandemic situation. He added that, in this context, the innovation conference played an integral role in identifying, in a competitive process, technical innovations from academic and industrial research and development relevant to the Bundeswehr. This also helps to connect innovators and stakeholders.

The relevant topics for the Innovation Conference's call for proposals 2021 were cybersecurity, communication, geoinformation as well as information processing and management. From a large number of submissions, the jury selected twelve innovative ideas, which were presented to the expert audience in seven-minute short presentations. Afterwards, the conference guests had the opportunity to discuss their concepts with the speakers.

Dr. Kim Nguyen was delighted to take first place in the competition. His idea for intelligent composed algorithms resulted from the aim of combining well-known cryptographic algorithms and introducing them into

1) GAIA-X: www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html (17/10/2021)



The participants of the innovation conference during the award ceremony.

applications and public key infrastructures. At the same time, the combined algorithms are intended to prevent standards such as X.509 or CMS from having to be changed only because agility is to be achieved in the algorithms.

Second place went to Prof. Dr. Martin Werner from the Technical University of Munich. With their idea, he and his team addressed the effective processing of large data amounts from different areas and media and, in particular, the targeted search for specific information.

Erik Heiland from the Universität der Bundeswehr München reached third place in the competition. His idea aims at improving the proactive handling of threat situations and thus initiating appropriate countermeasures at an earlier stage.

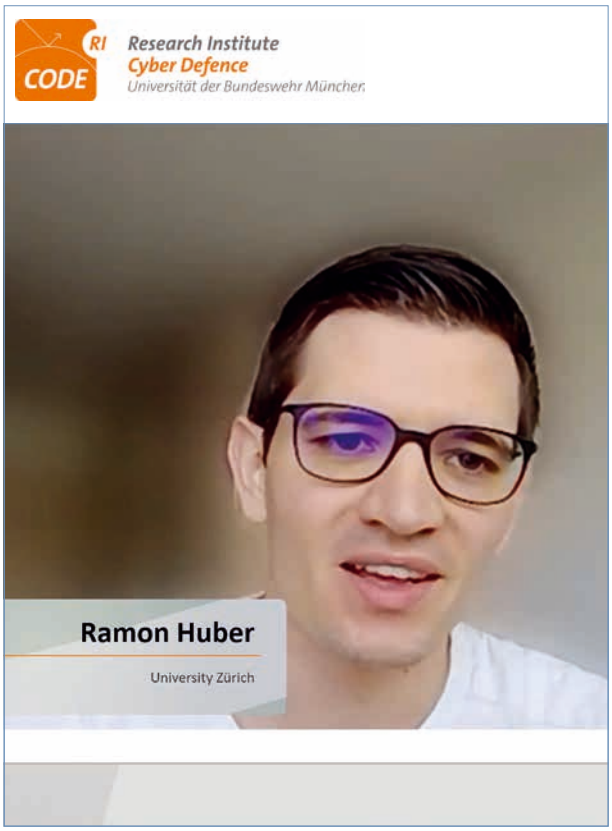
Forum for Young Scientists: Science Track

For the second time, the Science Track took place in 2021 as part of the CODE Annual Conference. The aim of the Science Track is to provide young PhD students with a forum for scientific exchange and networking. The event was divided into the "early stage PhD forum" and the "last stage PhD forum". The former provides a platform for prospective PhD students to present and discuss their PhD projects at an early stage, while the latter encourages more advanced PhD students to share their experiences with their younger counterparts.

From the submitted talks received in advance of the conference, six were selected by a scientific review process. Thematically, the program was a colorful mix from the field of IT security, ranging from presentations on the IT security of networked systems to applications from Data Science or Machine Learning.

The first part of the scientific program was opened by Ramon Huber from the University of Zurich with a talk on efficient communication in wireless sensor networks (WSN). The goal of the work is to implement the TinyIPFIX, which is derived from the IPFIX protocol, as a computationally and energy efficient approach towards push-based communication in Smart Home scenarios.

Mina Schütz from the Austrian Institute of Technology (AIT) opened the second part of the PhD forum. Schütz presented her work on automated detection of disinformation campaigns: She places a special focus on the explainability of the results by combining natural language processing (NLP) methods with approaches from the field of explainable AI (XAI).



Science Track: Ramon Huber's talk.

Scientific support for the conference was provided by Prof. Dr. Barbara Carminati from the University of Insubria (Italy), Prof. Dr. Burkhard Stiller from the University of Zurich (Switzerland), as well as Prof. Dr. Florian Alt, Prof. Dr. Harald Baier, and Prof. Dr. Wolfgang Hommel from the Research Institute CODE. The event was greatly popular and, despite its purely virtual form, achieved a good follow-up success compared to its premiere in 2020. The Science Track of the CODE Annual Conference is a central element for building a community for young scientists. ■

More information about the Annual Conference "CODE 2021":

www.unibw.de/code/events/jahrestagungen

www.youtube.com/c/FzcodeDeubw

code@unibw.de

FIG.: FI CODE

FIG.: ADOBE STOCK / NMEDIA

Research

Portraits and Projects

Research at RI CODE

Currently, there are 40 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.

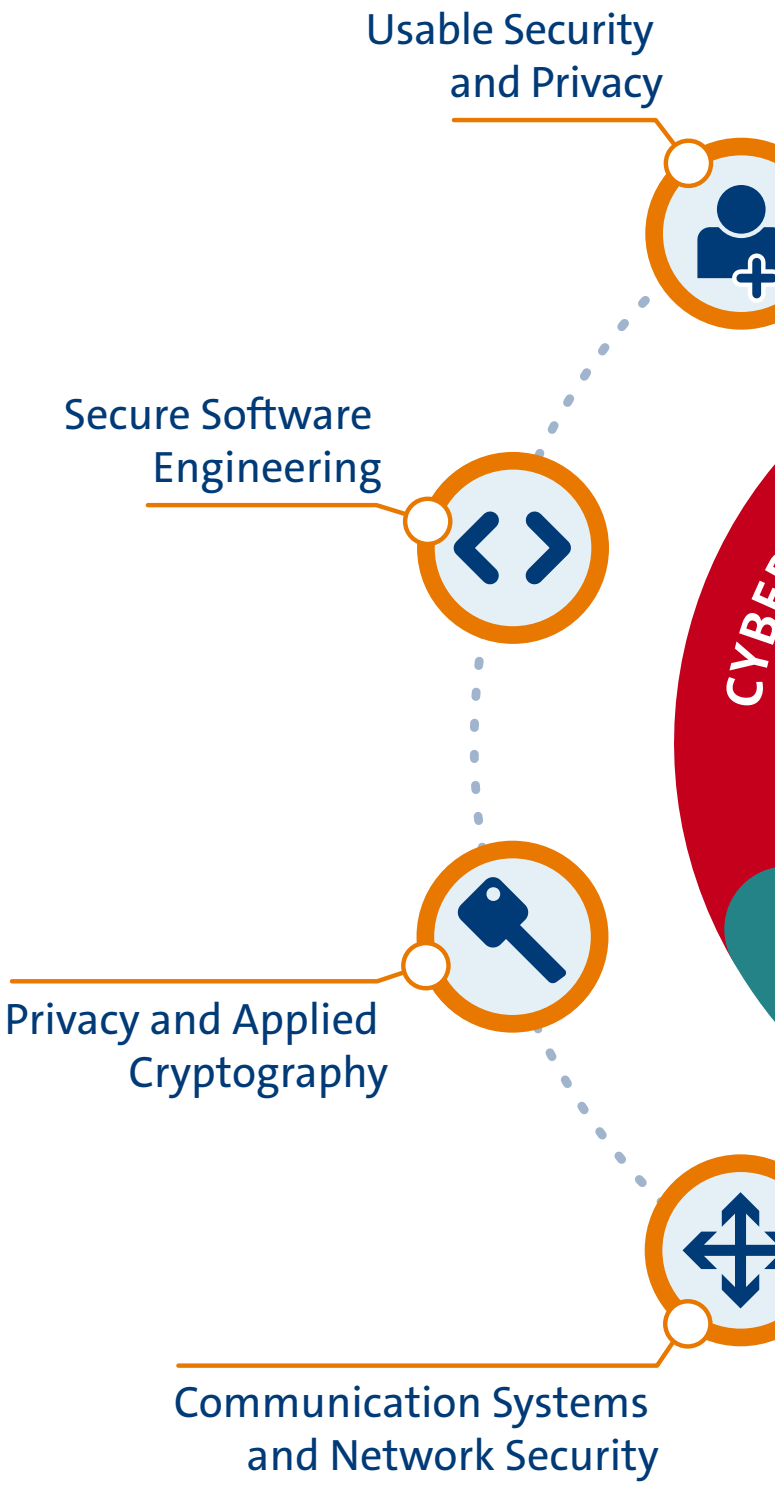
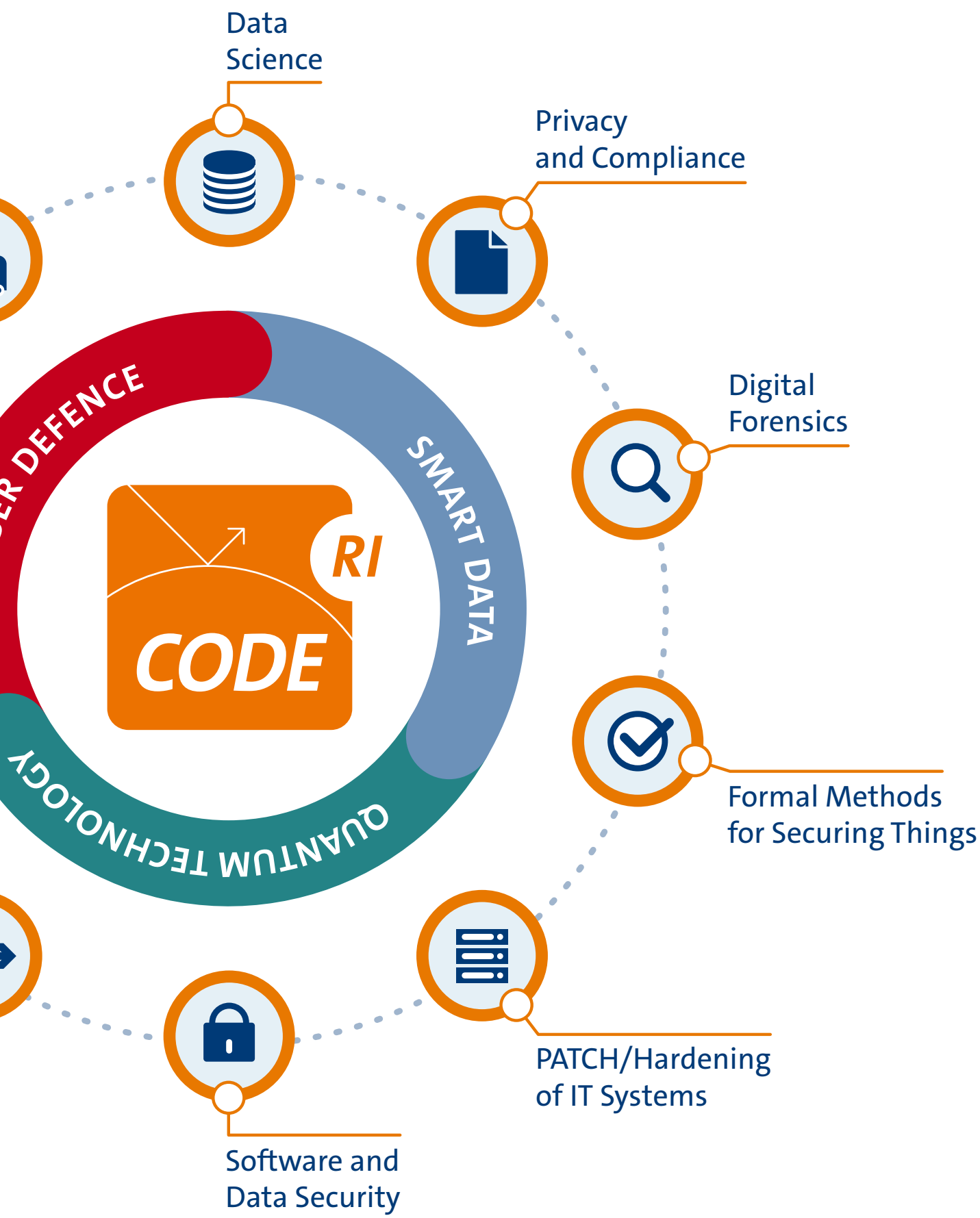


FIG.: TAUSENDBLAUWERK.DE


Data Science
Privacy and Compliance
Digital Forensics
Formal Methods for Securing Things
PATCH/Hardening of IT Systems
Software and Data Security
CODE
RI
SMART DATA
QUANTUM TECHNOLOGY
ER DEFENCE

Prof. Dr. Florian Alt

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 the 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. Those 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. In order 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. Florian Alt has published over 230 DBLP-listed scientific articles and won more than ten 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 Bavarian State Ministry of Education and Cultural Affairs, Science and the Arts, the Humboldt Foundation, the DAAD, Google, and the BMW Group.

Development of the Research Group in 2021

The research group Usable Security and Privacy grew in 2021 and currently includes 14 employees and four research assistants besides Prof. Florian Alt. Among the research group's scientific staff are nine PhD students and four postdocs, who contributed to more than 30 publications in 2021.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

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

The group uses technologies such as Augmented or Virtual Reality to visualize privacy/IT security risks or to explore the behavior of people in different simulated environments.

FIG.: ISTOCK / PHOTOTECHNO; FLORIAN ALT

Project Voice of Wisdom

Secure Human-Centered Technology

In the context of the Voice of Wisdom project, an environment to study human behavior and physiological responses in security-critical contexts will be designed and developed. Furthermore, novel, secure user interfaces will be designed.

Certain behavioral patterns and physiological reactions of users can indicate safety-critical situations.

Human Behavior and Physiology in Risky Situations

The Voice of Wisdom project is exploring new approaches to preventing human-centric cyberattacks. The goal is to use an analysis of human behavior and physiological responses to identify signs that people are at risk and thus better protect them when interacting with technology. By better understanding human behavior and physiological states, whether at work, whilst communicating with others, or interacting in a group, signs and precursors to behavior implying high risk can be identified.

Usage of Everyday Devices and Modern Technologies

To this end, the team leverages the fact that sensors in everyday devices, for example, a keyboard, mouse, or smartwatch, allow (subtle) changes in the user's behavior or physiological state to be detected – even if users are unaware of them. Modern technologies such as thermal imaging cameras, depth cameras, and eye trackers further contribute to obtaining an in-depth understanding. With the knowledge gained, novel security mechanisms can be developed, which, for example, support the user with hints and instructions for action (e.g., pop-ups, notifications on a smartwatch, indicators for video conferencing software) or are executed automatically in the background.

Objectives of the Project

The Voice of Wisdom project aims to build a research environment for observing human behavior and physiological states in safety-critical situations. This will enable a detailed analysis of safety-critical situations and their influence on users. Based on this, novel human-centered safety mechanisms will be developed in a next step and the long-term impact of the developed technologies as well as the user's perspective will be investigated.

Project Progress in 2021

In the first year of the project, the technical and conceptual foundations for the project were laid. A central question is which sensor is best suited to detect changes in the user's physiology. At the same time, it must be ensured that this sensor is accepted and actively used by the user. Due to COVID-19, many employees began working from home. The question here is whether sensor technology that restricts the user's privacy (such as depth cameras) is viewed more critically when set up in the user's home.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

https://go.unibw.de/vow

Funded by:
dtec.bw – Digitalization and Technology Research Center of the Bundeswehr

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

FIG.: ISTOCK / METAMORWORKS

Project PrEvoke

Supporting Users in Informed Privacy Permission Revocation

PrEvoke investigates the consequences of revoking privacy decisions. In particular, users are generally unaware of how such decisions affect an app's functionality, behavior, or content.

PERSONALIZING DIGITAL services or apps requires access to sensitive data, such as the users' location, calendar, or stored personal content, among others. At the same time, the influence of (not) granting access to this data is generally unclear to users. Today's prevailing approach for privacy permissions is that users decide only once, upon setup or first use, whether or not to grant the requested permissions. This cognitive process is commonly known as "privacy calculus", i.e., users decide whether they consider the expected benefit from using the service/app to match the value of the provided data. The challenge is that in most cases, users never reconsider and/or revoke those decisions.

App personalization requires access to sensitive data, such as the users' location or calendar.

FIG.: ISTOCK / IPOPBA

Understanding Users' Concerns and Expectations

With this project, the research group aims at understanding users' concerns regarding the consequences of revoking privacy decisions, i.e., whether this will affect the core functionality of an app or a service and/or how the quality or appropriateness of content selection and behavior will be affected. To this end, the team will assess the expected consequences and concerns of revoking privacy permissions with regard to whether these match reality and how concepts can be created to address misconceptions and concerns.

Determining Service and App Behavior

Moreover, the project will assess how revoking particular permissions influences the actual functionality of a set of web services and mobile apps. The researchers will compare the findings from this assessment (i.e., actual behavior of services and applications) with users' expectations. This will allow them to identify misconceptions as well as information that needs to be conveyed through a privacy permission revocation assistant to address these.

Application Areas: Web Services and Smartphone Apps

The project will focus on privacy permissions in two application areas: web services and smartphone apps. This allows for investigating a broad range of privacy permissions. Examples include, but are not limited to, body sensors, calendar, call logs, camera, contacts, files and media, location, microphone, payment information, physical activity, SMS, device name, and ad identifier. The researchers expect the findings to be applicable beyond these application areas, in particular to Smart Home / Internet of Things and Augmented Reality devices.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

Funded by:
Google Munich

Prof. Dr. Harald Baier

Digital Forensics

Due to increasing digitization and subsequent cybercriminal activities, the need for digital forensics competencies grows. The main research areas of the professorship of Digital Forensics address the handling of bulk data in IT forensic investigations, the generation of synthetic data sets 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 device 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 like drones or cars – can be secured and analyzed. The background to this is that often, these devices offer only unknown interfaces for access and that data storage is manufacturer-dependent 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 data sets are not sufficiently available to the community.

Throwing sand in the gears: The third important task is dealing with anti-forensics, i.e., all measures taken by the attacker 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; ADOBE STOCK / MICROGEN

Synthetic Generation of Data Sets

A fundamental problem in the field of Digital Forensics is that due to data protection and security aspects, the use of real data sets is often difficult or even impossible. However, realistic, individual and configurable data sets of persistent storage media, volatile main memory contents and associated network traffic are needed for testing IT forensic analysis software, evaluating novel tools and algorithms, for training in digital forensics, and for training machine learning methods. Data sets from additional IT systems such as smartphones or drones are also of increasing importance. Such data sets each need to contain the forensically relevant traces, to ensure that forensic experts and their tools are prepared for later real-world use. Providing such data sets is extremely time-consuming.

Requirements

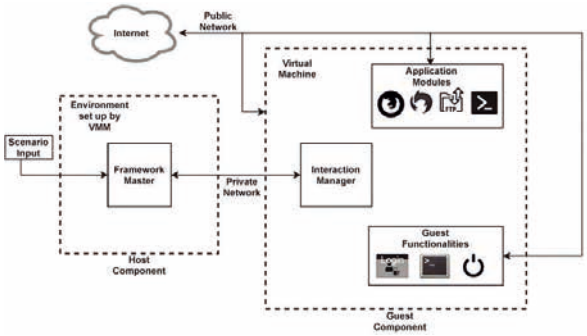
There are numerous requirements for high-quality data sets, such as the coherence – i.e., the respective digital traces must be generated together in the context of the same scenario to ensure that more complex forensic analyses based on multiple data sources are possible in the first place. In addition,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

hystck

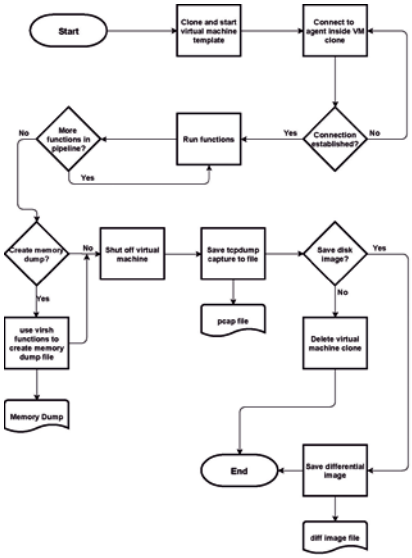
The team's hystck framework is used to generate synthetic data sets with a realistic ground truth. The framework supports the automatic generation of synthetic network traffic as well as operating system and application artifacts by simulating human-computer interactions.

ForTrace

"ForTrace" represents 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 that is as realistic as possible for IT forensic evaluation.



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

Prof. Dr. Harald Baier

harald.baier@unibw.de

+49 89 6004 7345

www.unibw.de/digfor

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

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

Handling large amounts of data

An IT forensic investigation is challenged by the sheer amount of data. Numerous data carriers from different devices such as computers, smartphones and tablets as well as removable media such as USB sticks, memory cards and DVDs have to be sifted through. The amount of data regularly reaches several terabytes. The task here is to separate important traces from unimportant ones as automatically as possible, i.e., to find the famous needle in a haystack.

Data Reduction

In order to screen the data as automatically as possible with regard to the legal questions after IT forensic imaging, the research group helped to develop, analyze and evaluate different approaches to data reduction. A first approach of this type searches for data that is known to be relevant to the case (such as files from the operating system or installed applications) and hides them for further investigation. However, analyses by the research group have shown that for typical data carriers with many individual files, the amount of data classified as irrelevant is in the mid-single-digit percentage range.

Approximate Matching

A second approach to data reduction uses approximate matching algorithms, i.e., change-robust compression functions ("fuzzy hashing methods"), to detect or recognize case-specific digital artifacts. For example, approximate matching can be used to find fragments of deleted child pornography files and match this fragment to the original image.

Artificial Intelligence

The concepts of Artificial Intelligence (AI) or Machine Learning (ML) are also intended to be used to detect case-related data structures using AI methods. However, compared to other cybersecurity disciplines, research here is still at an early stage. An important problem area of AI in the context of digital forensics is that many ML methods need to be sufficiently well trained, i.e., fed with data. This requires a critical mass of labeled data sets, which unfortunately are rare. Against this background, it is important that solutions such as ForTrace (see p. 38) also support AI-based procedures in digital forensics.

Prof. Dr. Harald Baier

harald.baier@unibw.de

+49 89 6004 7345

www.unibw.de/digfor

The large number of IT devices leads to bulk data.

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

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

The research group headed by Prof. Dr. 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.

THE MUNICH COMPUTER SYSTEMS Research Laboratory (µCSRL) directed by the Professorship of Secure Software Engineering conducts world-class research in computer security by coming up with novel defences that mitigate advanced attacks, primarily focusing on code-reuse attacks. By leveraging its expertise in programming languages, particularly in compiler technology, the team tackles challenging and important problems in programming languages, as well as security and privacy through its focus on language-based security.

Looking back at 2021, the µCSRL Research Group reports continuing success in the following areas: improved and novel defence against AOCR, a new technique to decompiling programs, bringing the team's fuzzing cluster online, and scaling up its operations through growth.

News and Updates

The researchers' efforts to mitigate Address-Oblivious Code Reuse (AOCR) saw multiple noteworthy achievements. First and foremost, through pushing the idea of booby traps into the domain of data objects, the team was able to demonstrate the first complete defence against AOCR. Second, through leveraging SSE and AVX instruction sets, the researchers' new implementation was able to achieve minimal performance impacts of about five percent on average. To the best of knowledge, no arbitrary code reuse attack not prevented by the established set of diversity-based defences exists at present.

µCSRL's endeavor to improve upon the state-of-the-art in decompilation of binary code into source code led to a pioneering new approach. The teams' new, self-developed decompiler – µDC, the Munich Feedback-Directed Decompiler – uses a feedback-loop to reconstruct source code that can be re-compiled to match the decompiled binary. As a result, a series of transformations can be applied to retroactively harden programs with state-of-the-art software defences.

The fuzzing cluster became operational in the final days of 2021. Now µCSRL has 1200+ CPUs to advance its research activities. The team has identified multiple interesting directions in which to progress regarding human knowledge in fuzzing and is confident that it will achieve promising results already in 2022, although fuzzing is to become a cornerstone of µCSRL's work for the upcoming years.

The past year allowed µCSRL to grow to six members: three new doctoral students, as well as a new Master's student ensure that the team can continue to tackle challenging problems, and in turn continue its growth trajectory.

Research Highlights

Prof. Dr. Brunthaler and his team have published over thirty Systems papers, with over half of them being published at top-ranked, highly competitive, international conferences, such as the IEEE Symposium on Security and Privacy, the Networked and Distributed Systems Security Symposium (NDSS), the ACM Conference on Computer and Communications Security (CCS), ACM SIGPLAN Conference on Object Oriented Programming: Systems, Languages, and Applications (OOPSLA), the IEEE / ACM International Symposium on Code Generation and Optimization (CGO), and the European Conference on Object-Oriented Programming (ECOOP).

In 2021, Prof. Brunthaler was elected a member of IFIP WG2.4 "Software Implementation Technology" and gave over thirty invited talks. Last but not least, the Python programming language adopted optimization technology pioneered by Prof. Brunthaler in 2010. As a result, the outcomes of his research are now applied by hundreds of millions of people daily.

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 and Space GmbH.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330

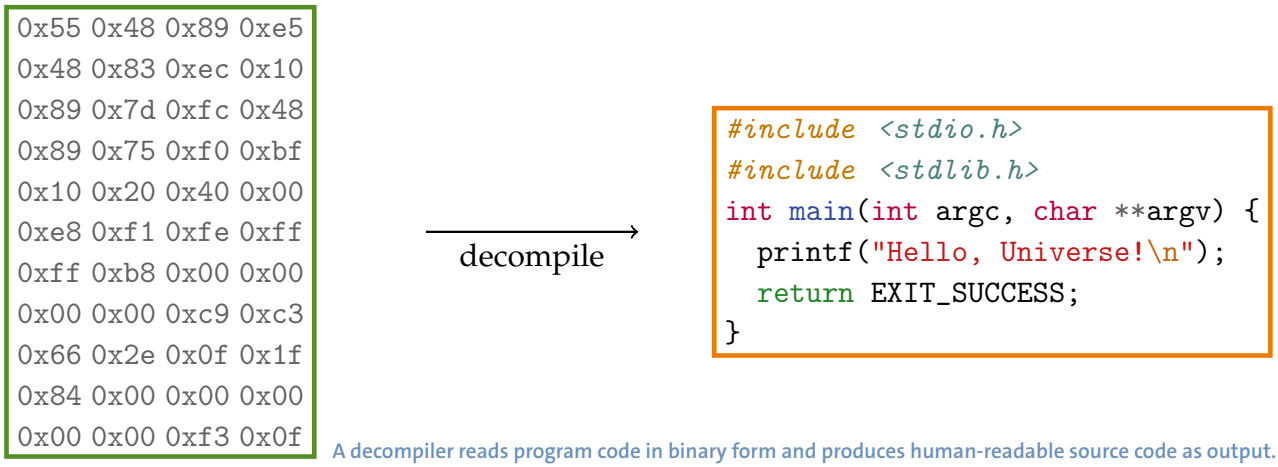
www.unibw.de/ucsrl-en

FIG.: ISTOCK / DE M10

Project µdc

Feedback-Driven Decompilation

While compilers compile the source code of a program to a binary, decompilers try to reverse the compilation process by restoring the original source code of a binary. Since compilers discard information during compilation, such a reverse compilation isn't always exact. The Munich Decompiler considers the feedback of the compiler during decompilation and can thus achieve a significantly higher precision when restoring source code from a binary.



A decompiler reads program code in binary form and produces human-readable source code as output.

Compiler versus Decompiler

To execute a program written in human-readable source code, the program must first be compiled to a binary by a compiler. In certain situations, a program is only available in its binary form without access to the original source code. A lack of source code is problematic because the source code is a prerequisite for tasks like maintenance or security audits. For that reason, decompilers try to reverse the compilation of a program and restore the original source code from a program in binary form. This reverse compilation is called decompilation.

Missing Information During Decompilation

After compiling a program, a compiler discards any information that is necessary only for the compilation, but not for the execution of the program. This loss of information significantly complicates decompilation. When decompiling a program, a decompiler must make assumptions about unavailable information to approximate the original source code as well as possible. However, as these assumptions can be incorrect, the restored source code typically does not resemble the original source code exactly.

The Munich Decompiler

An issue with existing decompilers is the lack of validation of the assumptions made during decompilation, leading to incorrectly restored source code if the assumptions turn out to be incorrect. In contrast, the Munich Decompiler validates assumptions by recompiling the restored source code with a compiler. Taking into account the compilers feedback during decompilation leads to an increased precision of the restored source code.

Broader Impact and Societal Merit

The Munich decompiler is an important improvement over state-of-the-art decompilation techniques and enables advances in several areas that critically hinge on decompilation. For example, security audits of proprietary software or the analysis of malware both depend on precise decompilation results.

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

FIG.: S. BRUNTHALER / RI CODE

Project Install-Time Diversity

Diversifying Programs at Install-Time

Frequently, malicious software successfully attacks a multitude of devices as they are running the exact same copy of a given program. Software diversity counteracts this danger through deploying a custom-diversified version of the program on every single computer. The project "Install-Time Diversity" investigates new methods to automatically diversify programs at the time of their installation.

Software Diversity

The essential idea of software diversity is to proactively transform programs to make them more resilient against attacks. The currently prevailing method of software distribution deploys identical copies of a program to many computers. A single bug thus affects all copies and can be used to mount a large-scale attack. Software diversity counteracts this danger through deploying a custom-diversified version of the program on every single computer. The attacker is now deprived of the economies of scale that enabled a single attack to target a multitude of devices.

Distribution of Diversified Programs

Diversified variants of a program can be created at various points in the software development process. Compilers can be augmented to diversify programs during compilation, for example. An alternative to compile-time diversification are self-diversifying programs that perform the diversification at run-time. Both approaches are ill-suited when it comes to the deployment of software diversity on resource-constrained devices. On the one hand, existing distribution channels in the form of app stores hinder the adoption of compiler-based diversity since each downloaded copy of a program needs to be diversified. On the other hand, performing the diversification at run-time can lead to performance problems on resource-constrained devices, such as smartphones.

At Install-Time

The project team is presently researching new methods that enable the deployment of software diversity, even on resource-constrained devices. The researchers distribute precompiled program building blocks to the device and assemble them on the device in a customized way, i.e., specific to the device. This allows re-using existing infrastructure for application delivery and eases adoption. Incurring run-time overhead during program execution is avoided by performing the diversification process at install-time. Hence, software diversity now is a viable even on resource-limited devices such as smartphones and routers.

Broader Impact and Societal Merit

Software diversity is the solution to problems caused by software monoculture, which are exemplified by the rapid spread of computer viruses and ransomware. The team's research enables variants to be created efficiently and thus paves the way for widespread deployment of software diversity.

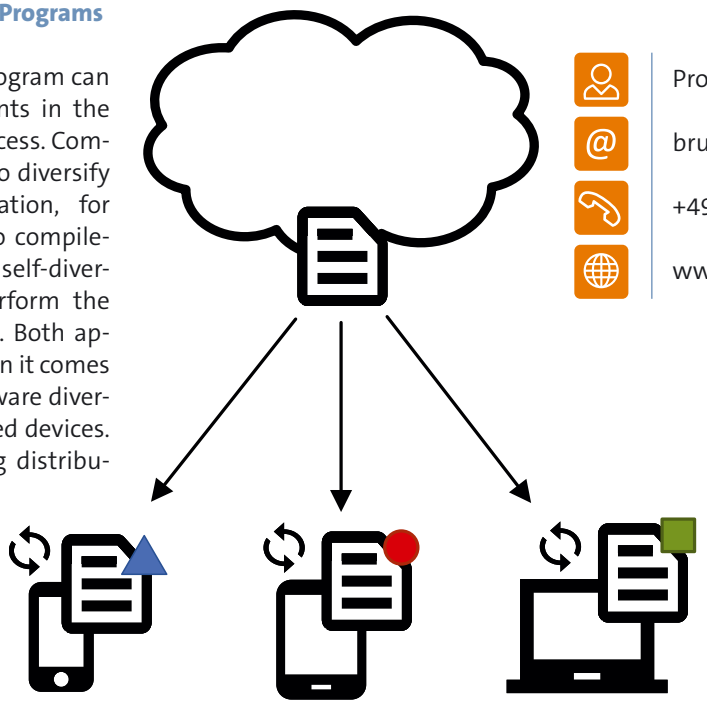


FIG.: S. BRUNTHALER / RI CODE

Moving software diversification from the cloud to the end user's devices simplifies software distribution.

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 and 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 during 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 Universität der Bundeswehr München.

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 like Twitter, etc., are in focus.

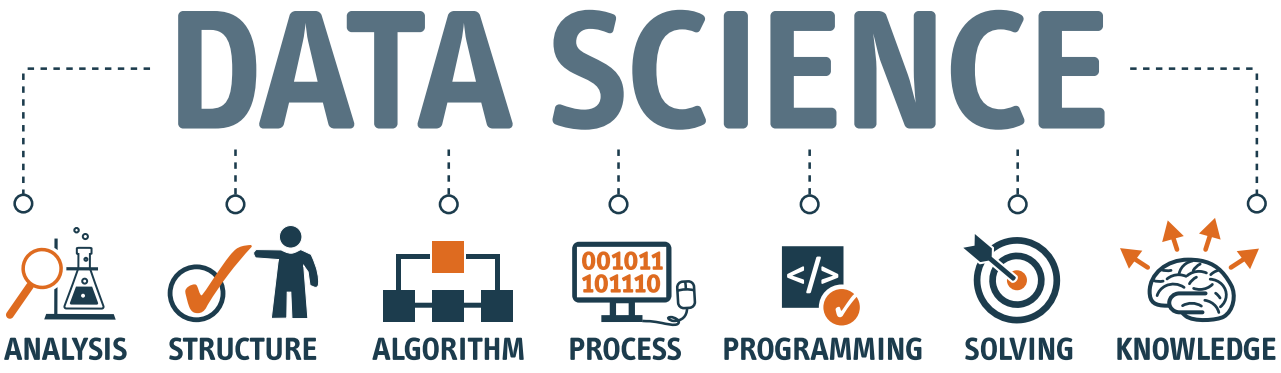
Recent technological advances and developments in the field of Artificial Intelligence (AI) have also given rise to so-called Deep Fakes. This refers to an audio-visual modification of a video generated by means of AI, in which the face and/or statements of the person depicted in the video have been 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



The range of tasks of tasks covered by the professorship of Data Science.

FIG.: SHUTTERSTOCK / RYZHI; SHUTTERSTOCK / TRUEFFELPIX

Project KIMONO

Detection and Modelling of Disinformation Campaigns in Social Media

The goal of the KIMONO project is the detection and modelling of short- and long-term disinformation and influencing campaigns in Social Media such as Twitter and Facebook. In particular, campaigns that are promoted by nation-state actors are in focus. In this context, the best technical approaches to detect such campaigns and narratives are gathered in order to propose the conceptualization of a prototype for an early warning system.

Disinformation campaigns in Social Media can take many forms and have many consequences.

FIG.: SHUTTERSTOCK / BUFFALOBOY

DISINFORMATION CAMPAIGNS can manipulate and influence people and thus lead to a massive weakening of trust in democracy, its rule-of-law principles and in freedom of speech. Furthermore, there is a risk that state actors will use influence campaigns in Social Media to destabilize enemy states (hybrid warfare). It is therefore essential to identify these campaigns as early as possible and to monitor their development and spread in order to be able to initiate suitable countermeasures.

In the KIMONO project, a Social Media pipeline is implemented that pulls respective data from various Social Media platforms such as Twitter, Facebook, and Instagram, and stores it in a database. Moreover, the researchers consult fact-checking websites (such as Volksverpetzer.de, Correctiv.org, PolitiFact, TheWhistle) in order to estimate a degree of truth of the gathered data. Various state-of-the-art Shallow and Deep Learning algorithms are examined and applied to the Social Media data. For the analysis and training of classification models, the following features are extracted:

1. **User-based:** They are extracted from the profile of the users in their respective Social Network (e.g., Twitter, Facebook). In this context, the team considers information such as how long does the account exist, how many posts were published or how many followers and followees does the user have as valuable for the task at hand. Those features are also useful for the detection of social bots.

2. **Post-based:** The researchers assume that the language of campaign-related posts differs from other posts. To this end, they rely on shallow syntactic and semantic analysis. Opinions, stances, sentiments and topics are extracted from the posts and ranked to retrieve the most valuable information. The team expects to find expressions of strong opinions, sensational and/or emotional wording as well as a characteristic use of certain words and phrases that are shared by campaign initiators.

Explainability is also of great importance. Classical Deep Learning models can be seen as black box systems and neither can provide the user with enough information to understand the classification, nor to recognize conclusive measures. However, by combining powerful neural networks with more traditional feature engineering, it seems possible to obtain results that are more transparent and explainable. At the end of the project, a list of requirements will be proposed to conceptualize the development of a Social Network audit and early warning system.

Dr. Olivier Blanc
olivier.blanc@unibw.de
+49 89 6004 7343
https://go.unibw.de/kimono

Funded by:
Federal Ministry of Defence

Project SMILE

A Scalable, Modular and Interactive Framework for Situation Picture Development

In the SMILE project, on the basis of various data and information sources, a system that uses Artificial Intelligence (AI) to create an overview of the situation is developed. For example, topic-specific data records from the last 24 hours will be visualized on a map to provide an overview of current local events. In addition, hotspots or anomalies can be prominently highlighted for further analysis.

Initial Situation in the Open Information Space

Sudden, dynamic events are captured by a variety of actors and disseminated through a variety of media and channels. Many of these sources are publicly available and could be used to obtain comprehensive information on political, economic, and social changes, both locally and globally. At the same time, however, this gigantic amount of data reveals a number of challenges in terms of data analysis and provision, which complicate the efficient use of the freely available information:

- Data extraction from different sources
- Ensuring information quality and validity
- Processing of inhomogeneous data sets
- Efficient information retrieval
- Data aggregation and correlation
- Data visualization
- Data interaction

However, a reliable knowledge base is essential for well-grounded decisions and strategic planning.

Objective of SMILE

Hence, the goal of SMILE is to develop a scalable, modular and interactive framework that extracts, processes and visualizes data from different sources. The data should ultimately be processed so that hotspots, anomalies or similar deviations from an expected normal state can be clearly identified. For further analysis, on the one hand, a spatial or temporal classification needs to be carried out and on the other hand, a specific event has to be examined in more detail with the help of supplementary data sources.

To achieve these goals, methods of information retrieval are combined with clustering and classification algorithms, as well as methods of human-computer interaction (HCI). For data retrieval, the focus is on publicly available data sources, such as press agencies, Social Media services, or structured event databases.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

FIG.: SHUTTERSTOCK / CONCEPTCAFE

Exemplary illustration of an AI-supported overview of the situation.

Prof. Dr. Wolfgang Hommel

Software and Data Security

Prof. Dr. Wolfgang Hommel's team researches technical and organizational security measures for complex IT infrastructures and environments 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, which 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 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 in the laboratory at least, but if possible, also in concrete pilot environments and ideally through individual embedding in scientifically accompanied projects. The role of the human factor in information security as well as economic and legal constraints is also taken into account.

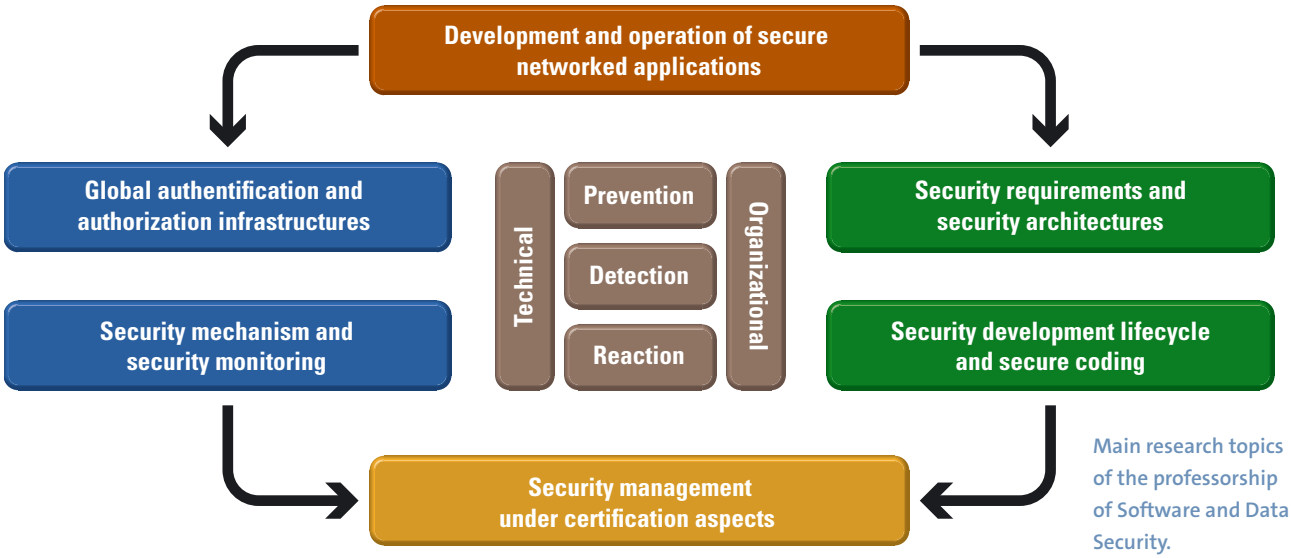
Current research and projects include, for example, the implementation of the self-sovereign identity paradigm for use in global authentication and authorization infrastructures as a data protection-friendly technological advancement of federated identity management that has proved itself in practice. Ongoing work on security monitoring components and policy-driven management platforms for federated software-defined networks is applied, for example, in the establishment and expansion of the 5G telecommunications infrastructure and in the dedicated cross-location networking of industrial control systems. Those lay the foundation for securing future 6G technologies and find their application, for example, in the protection of remote management infrastructures of modern power supply networks. In the area of the Internet of Things, research focuses 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

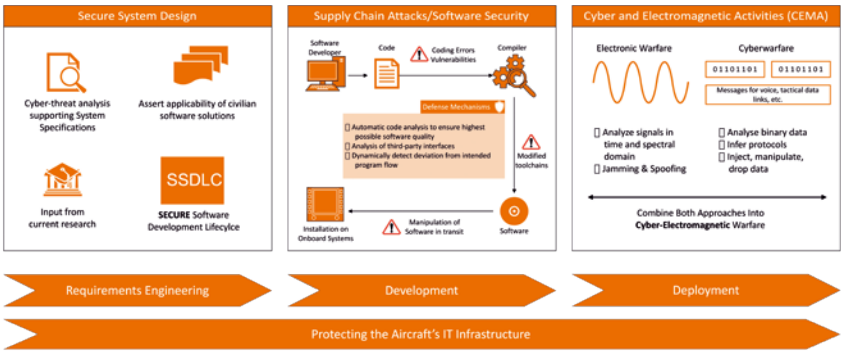
Project ACSE

Cybersecurity for Airborne Systems

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

Cybersecurity as Integral Part of Development: Raising Awareness on Cyber Threats

The RI CODE and Airbus Defence and Space pool their experience in the areas of IT Security and the development of airborne systems to improve current development processes, making them fit for the future. The team accompanies running projects within the industry and evaluates opportunities to enhance the development process with organizational and technical security mechanisms. To raise the awareness for threats to airborne systems originating from the cyber domain, the team developed relevant realistic scenarios that guide the project course.



ACSE contributions during the development lifecycle.

Hardening of Complex Interconnected Systems

Operational requirements demand increased connectivity between airborne and other systems, leading to the existence of a multitude of heterogenous internal and external interfaces on each system. One goal of ACSE is to research and implement methodologies and concepts for the (partially) automated analysis of and interaction with these interfaces. To this end, the team develops a framework that manages protocols and internal relations within a protocol in a generic and extensible way. Building on this foundation, new functionality can be realized in a modular manner. Specifically, the team evaluates the possibility to emulate interfaces of embedded hardware components to enable passive and active network analysis for these interfaces. Obtained data can be exported to established network analysis tools for further inspection. To ensure seamless integration into existing development cycles, the framework can automatically import process artifacts like interface specifications and make them available to developers.

Secure Software Development during the whole Development Cycle

Development and certification processes place high demands on software in avionics systems, especially for critical applications. A specific challenge in this environment is the heterogeneity of hardware and software caused by long project durations. The team inspects these development processes and develops organizational and technical measures to support secure software development in the long term. Concrete technical solutions are implemented for specific phases in the development process. One area of interest is the automation of process steps such as code review or the creation of supplementary documents, integrating tightly into existing processes.

Alexander Frank
alexander.frank@unibw.de
+49 89 6004 2745
www.unibw.de/software-security/forschung/acse-resources/acse

Funded by:
Airbus Defence and Space

FIG.: ALEXANDER FRANK

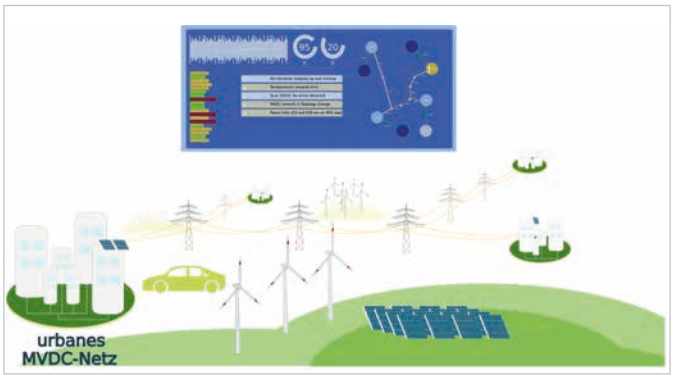
Project DEFINE

DC Networks for a Secure Energy Supply

In the dtec.bw project DEFINE, the professorship of Software and Data Security is researching into future secure power grid infrastructures in cooperation with the departments of Electrical Engineering and Information Technology, Mechanical Engineering, and Civil Engineering and Environmental Sciences at the Universität der Bundeswehr München.

Power Grids: Arteries of Modern Societies

Electricity is the basis of the modern information society. Power grids have grown historically and become widely adopted as alternating current (AC). However, aspects that became important in recent decades, such as resource efficiency and control in the power grid, can be realized much better in direct current (DC) grids, which can transport about 50 percent more energy for the same investment. The project therefore addresses the realization of medium-voltage direct current (MVDC) grids.



Centralized Network Management for MVDC Networks.

Secure Operation of MVDC Networks

MVDC networks, however, require highly dynamic monitoring and control in real time during operation: Converter stations located within must continuously coordinate with each other in update cycles of a few hundred microseconds. Since such concepts do not yet exist for conventional AC networks, secure control infrastructures, algorithms and protocols must be fundamentally researched for this purpose and designed from the ground up according to today's IT security standards. Key challenges relate to dealing with any potential disruptive factors such as component failure, as well as malicious attacks on the power grid and control infrastructures. Since the active control and configuration of the converter components in an MVDC network plays a crucial role, securing the communication and control infrastructure also becomes highly relevant. Control messages manipulated by attackers or replayed old control messages (so-called replay attacks) can lead to the inability to operate MVDC networks and must be prevented. However, the high update rates of a few hundred microseconds limit the "standard solutions" that can be used and cannot be applied directly in MVDC networks, which means that new solutions are also necessary here.

Multi-Tenancy-Capable Solutions for Power Grids

Another topic that has become indispensable in modern IT networks, at least since the advent of cloud computing, is multi-tenant management. Also in the power grid, there are different tenants – e.g., power generators, power grid operators and end customers – wanting to make increasingly better use of accruing real-time monitoring data. In the team, novel concepts and prototypes are developed. The figure illustrates the core vision: several subnetworks, connected via conventional network infrastructures, are centrally monitored, evaluated, and controlled to be able to handle fault cases quickly and automatically.

Michael Steinke

michael.steinke@unibw.de

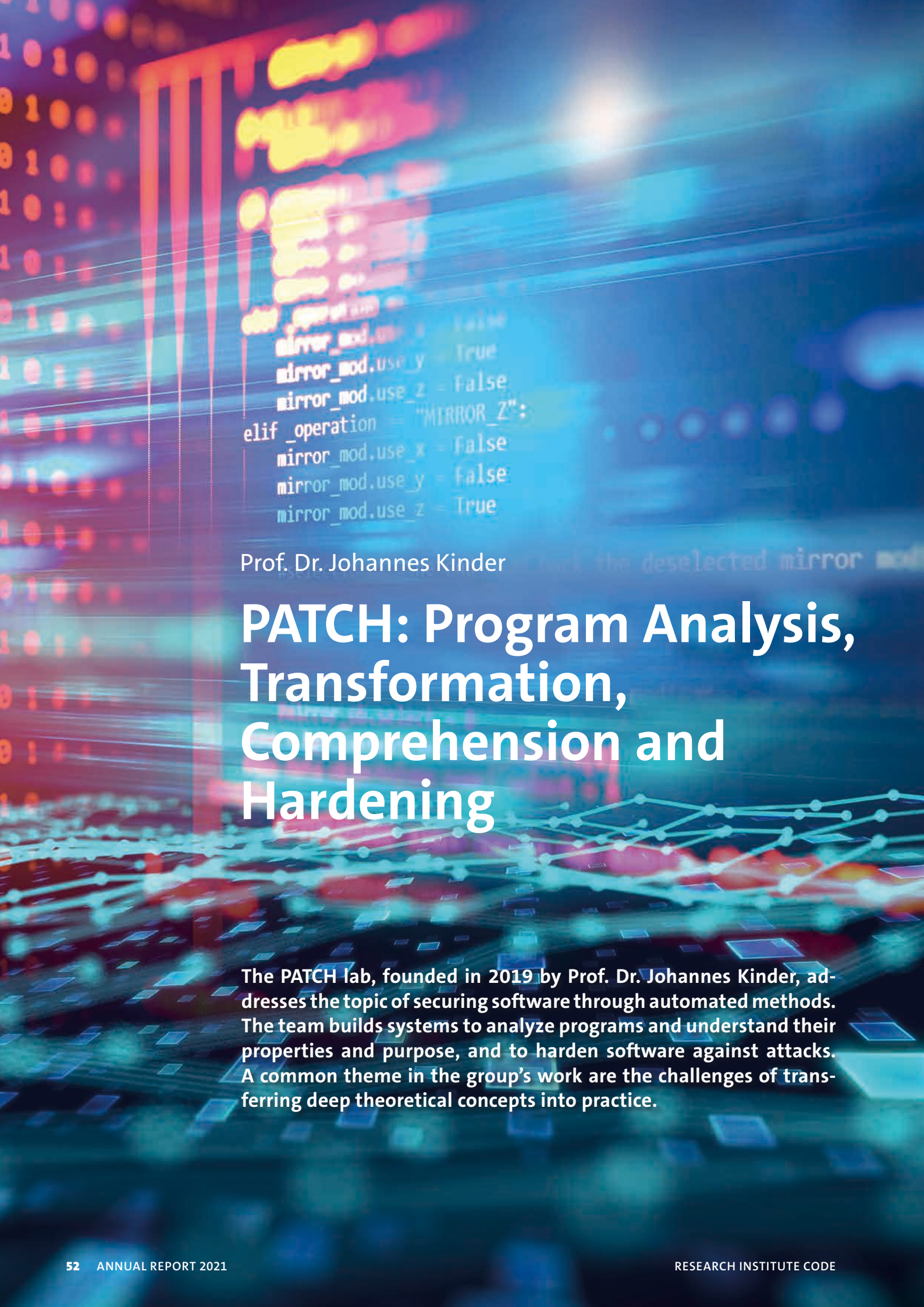
+ 49 89 6004 4825

https://go.unibw.de/inf24define

Funded by:
dtec.bw – Digitalization and technology Research Center of the Bundeswehr

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

FIG.: MICHAEL STEINKE



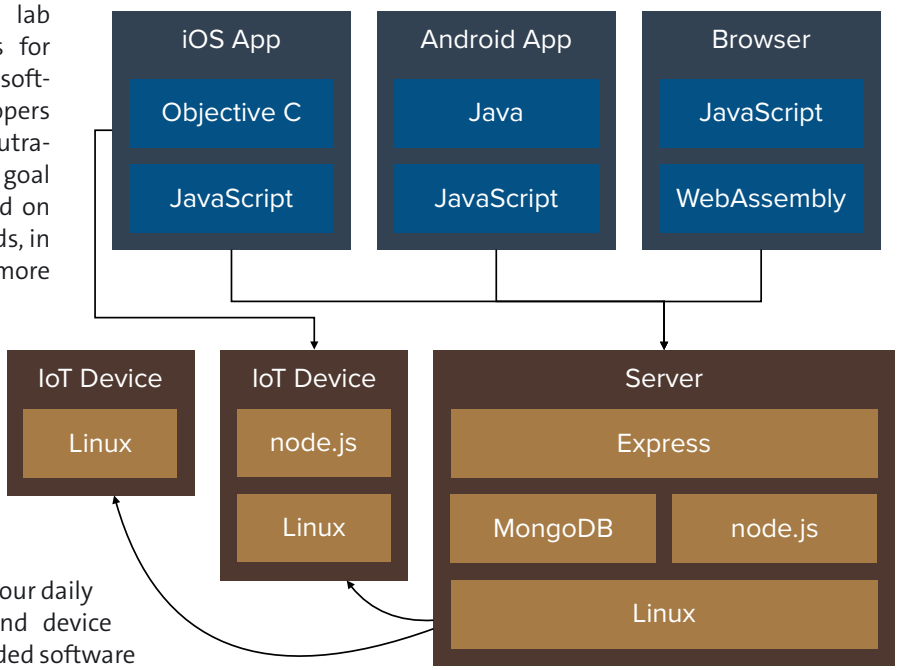
Prof. Dr. Johannes Kinder

PATCH: Program Analysis, Transformation, Comprehension and Hardening

The PATCH lab, founded in 2019 by Prof. Dr. Johannes Kinder, addresses the topic of 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 automated methods for securing computer systems and software. Designing tools for developers and organizations 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, more recently, 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.



Modern system stacks combine many different programming languages and platforms.

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 like 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 backdoors 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 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

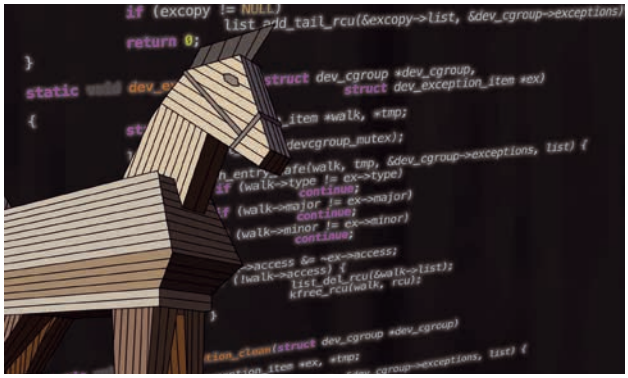
www.unibw.de/patch

FIG.: ISTOCK / MONSITJ; J. KINDER / RI CODE

Project DEMISEC – Detecting Malicious Implants in Source Code

Modern Software Supply Chains Must Be Protected from Internal and External Attacks

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.



Attackers can compromise software by injecting malicious code into otherwise benign source code.

THE REUSE OF SOFTWARE components is a fundamental element of software engineering. Today's developers can quickly implement complex projects by wiring together components and libraries, choosing from a vast range of open-source code. On the one hand, this eliminates repetition and therefore opportunities to accidentally introduce vulnerabilities, e.g., by relying verified and verifiable implementations of crypto libraries. On the other hand, it creates a potentially long software supply chain of transitive dependencies, where each element has to be trusted.

Protecting Open Source

Malicious code implanted at any point in the supply chain can propagate into critical systems. Already, there have been several cases of open-source developers stealing credentials to upload malicious code into popular libraries. With open-source repositories effectively becoming critical infrastructure, we need reliable methods to verify and validate source code. The goal of "DEMISEC – Detecting Malicious Implants in Source Code" is to develop techniques for the automatic vetting of open-source repositories, in particular for detecting implants of malicious code in source code.

The team will use a mix of static and dynamic techniques to achieve this goal: fuzzing or symbolic execution for differential testing of program versions, and modeling of implant code to detect dangerous patterns in code repositories using static analysis. In collaboration with Prof. Dr. Brunthaler's µCSRL lab, the researchers will investigate Quick-Vetting for the light-weight attestation of pre-vetted software components. Finally, they will conduct large scale studies on open-source code to evaluate the project outcomes.

Attack Categories

As part of the project, the team was able to divide previous attacks into four broad categories: Typosquatting, i.e., exploiting typos in the name of libraries; Dependency Confusion, i.e., unintentional import of external libraries; Malicious Commits, i.e., malicious code injected into legitimate projects; and Intrusions, i.e., targeted attacks against systems of software vendors.

The DEMISEC project is carried out as part of a German-Israeli research cooperation on behalf of the Federal Ministry of Defence (BMVg). On the Israeli side, the Defence Ministry, the Ben Gurion University of the Negev (BGU) and other research institutions are involved. The cooperation intends to strengthen the capabilities of both partners in the field of cyber defence, is purely defensive and has an open research character.

Prof. Dr. Johannes Kinder

Johannes.kinder@unibw.de

+49 89 6004 7335

www.unibw.de/patch

Funded by:
WTD81/BAAInBw

FIG.: FI CODE / 13SMOK@PIXABAY

Modeling Spectre Attacks

Axiomatic Semantics Can Capture the Speculative Executions Involved in Novel Micro-Architectural Attacks

The disclosure of the Spectre family of speculative execution attacks in 2018 shook the world of IT security with the news that most modern processors have inherent vulnerabilities. This project focuses on defining new types of semantics for speculative execution and building tools to verify software against Spectre and related attacks.

Micro-Architectural Semantics

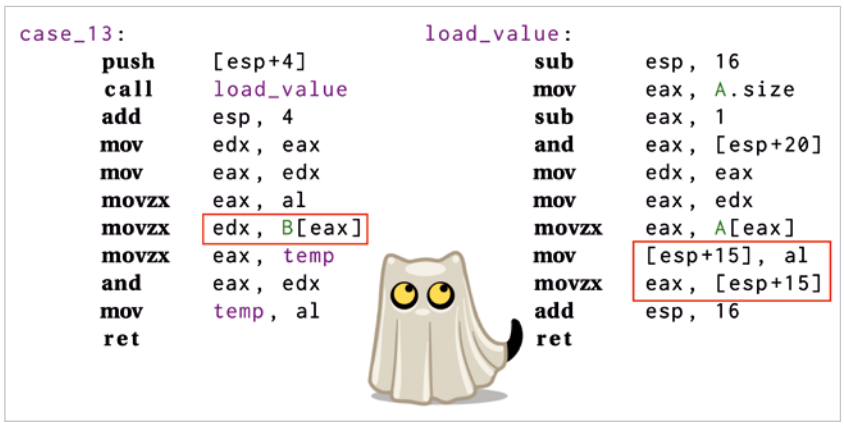
Despite several success stories of applying formal methods for security, speculative execution attacks went under the radar of verification techniques for many years because they ignored the role of the micro-architecture. Nowadays, there is ongoing work to incorporate micro-architectural effects into formal semantics. However, most approaches rely on operational semantics which require descriptions of the micro-architectural state, resulting in complex models. Newly discovered attacks can require a redesign of the entire semantics to account for the relevant micro-architectural effects. Because of this, verification techniques are having a hard time to keep up with the pace at which new attacks are being developed and countermeasures are being suggested.

The team proposes an alternative, lightweight and axiomatic approach to specifying speculative semantics that relies on insights from memory models for concurrency. It uses the CAT modeling language which was initially developed for memory consistency (and adopted by ARM for this purpose in 2017) to specify execution models. Its elegance lies in a modular style of reasoning. The team finds CAT to be ideally suited to capture a variety of attacks exploiting speculative control flow, store-to-load forwarding, predictive store forwarding, and memory ordering machine clears.

From Semantics to Tools

The use of the CAT language allows a natural way to model several kinds of speculative execution semantics using Bounded Model Checking (BMC). The researchers propose a unified analysis framework that is parametric in its micro-architectural model defined via CAT. They implement this framework in the prototype “Kaibyo”. The evaluation shows that the proposed models are precise enough to accurately detect several different vulnerabilities exploiting different micro-architectural features, and to prove that common countermeasures are effective. At the same time, CAT allows Kaibyo to be rapidly extended to new attacks.

This project is the first to establish a neat, systematic, and tool-supported framework to reason about speculative execution using axiomatic semantics. The team describes the proposed semantics and analysis framework together with an evaluation of their expressivity and precision in an article to appear at the 43rd IEEE Symposium on Security and Privacy (S&P), a premier forum for computer security research.



Kaibyo can detect speculative execution vulnerabilities due to (among others) instruction reordering.

FIG.: RI CODE

Dr. Hernán Ponce de León
hernan.ponce@unibw.de
+49 89 6004 7334
www.unibw.de/patch/ponce

Prof. Dr. Arno Wacker

Privacy and Compliance

Don’t just teach Data Privacy and Compliance, live it!

ONE OF THE MOST important goals of the professorship of Privacy and Compliance is not only to research and teach data privacy and IT security, but also to bring it into everyday life. Only in this way can complex topics be communicated in a persuasive and authentic way to the students. Additionally, the research group also wants to demonstrate to the public that technologies which support data privacy could be integrated into everyday life, be it private or business.

Teaching

Teaching in the professorship is divided into penetration testing, data privacy, privacy enhancing technologies, cryptology, and secure networks and protocols. Students learn what privacy is and why it is important, not only for the individual but also for democratic societies. Penetration testing deals with the examination of single systems, complex IT services and IT infrastructures, as well as real-world attacks based on well-established good practice documentation. Also, the fundamentals of cryptography and knowledge about methods for secure data communication in modern communication networks are taught.

Research

A special focus of the professorship is on methods and mechanisms supporting privacy and data privacy, and comprises three different research areas:

- Privacy-supporting mechanisms aim at strengthening the privacy of the individual as well as the communication rules for the age of the Internet.
- Increasing IT security awareness addresses, among other things, the area of personal data protection ("Selbstdatenschutz" in German). For this, the professorship develops and researches into, among other things, methods and tools for increasing security awareness in the development of software tools and in their use.
- Cryptoanalysis of classic ciphers examines the field of classic encryption methods with the help of modern (meta-) heuristic techniques. Thus, both the effectiveness of the analysis and the security of the algorithms are examined.

A special focus of the professorship is on privacy and privacy-supporting measures.

Knowledge Transfer

A special focus of our professorship is to upskill and enlighten interested citizens and to tutor and inform them on IT security-related questions. This task is achieved with the help of presentations and workshops that, for example, deal with the topics of penetration testing, secure email in everyday life, and the reconstruction of security breaches. Regarding the last point, the professorship offers, for instance, a heartbleed server on which those interested can try, in an isolated environment, to take advantage of such a bug.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

FIG.: ISTOCK / MATEJMO; ISTOCK / THITICHAYA YAJAMPA

Project Redundant Structures in Fully Distributed Overlay Networks

Network Resilience Through Redundancy

This research project deals with passive security measures in fully distributed overlay networks. The goals are to analyze and improve the resilience of such networks against attacks and technical failures by creating and exploiting redundancies in data storage and network connectivity, avoiding single points of failure and control.

Overlay networks withaout central node.

THE AVAILABILITY OF many services on the Internet depends on a central node and its reachability. To ensure high availability, the central node is often implemented as multiple load-balanced servers, a multitude of virtual server instances in a cloud infrastructure, or even one or more dedicated data centers. Still, even though its owner might take extensive measures, a sufficiently severe technical failure, a misconfiguration, or a successful attack can result in an unavailable central node and, thereby, an unavailable system. Apart from technical errors or attacks, the party controlling the central node might simply decide to shut it down, rendering the system unusable.

Problems in a centralized network can not just arise in terms of availability, but also in terms of privacy and censorship. A central node that is involved in the interactions between other nodes might be able to gather sensitive information. This ranges from metadata, such as who communicated with whom, to complete knowledge of all information exchanged in the system.

Beyond that, acting as proxy between other nodes allows the central node to apply censorship to any communication.

A different way of organizing a distributed networked system is the fully decentralized approach, e.g., in the form of an overlay network on the Internet. Here, no central node and, therefore, no single point of failure or control exists. The nodes of the system act as equals with regard to routing, communication, and other services or resources. The benefit of avoiding the single point of failure or control comes with a penalty in form of a higher effort for routing and resource location.

Whereas with the centralized approach, interaction with the central node is sufficient for participation, the fully distributed approach often requires interaction with multiple nodes for communication or resource location. The identity and number of these nodes can vary from interaction to interaction.

This project researches into the creation and exploitation of redundancies in data storage and network connectivity in fully distributed systems. The goal is to harden such systems against targeted attacks and technical failures by analyzing and improving the network resilience. Intended effects are the avoidance of single points of failure and control and, thereby, reducing the probability of unavailable services or of censorship.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

FIG.: ISTOCK / METAMORWORKS

Project DECRYPT: Decryption of Historical Manuscripts

Automatic Decryption of Historical Manuscripts

The aim of the project is to establish a new cross-disciplinary scientific field of historical cryptology by bringing the expertise of the different disciplines together for collecting data and exchanging methods for faster progress in decoding and contextualizing historical encrypted manuscripts, hitherto buried in archives and libraries.

HAND-WRITTEN HISTORICAL records constitute a key component of our collective memory, without which our understanding would be severely limited. A special type of hand-written historical records are encrypted manuscripts, so called ciphertexts. According to historians' estimates, one percent of the material in archives and libraries is encrypted or encoded, and many of these documents have still not been decrypted. Consequently, with a key aspect of our collective memory still hidden away, there is a need for a major research effort to make sure this missing knowledge is brought to light and used to further a deeper understanding of our shared history.

Many historians and linguists work individually and in an uncoordinated fashion on the identification and decryption of these documents. This is a time-consuming process, as they often work without access to automatic methods and processes that can help and accelerate the decipherment. At the same time, computer scientists, cryptologists, and computational linguists are developing automatic decryption algorithms to identify and decode various cipher types without having access to various kinds of real ciphertexts.

The aim of the project is to establish a new cross-disciplinary scientific field of historical cryptology by bringing the expertise of the different disciplines together for collecting data and exchanging methods for faster progress in decoding and contextualizing historical encrypted manuscripts, hitherto buried in archives and libraries.

Libraries and archives still contain many unsolved mysteries.

More concretely, the project will result in an openly accessible database with thousands of encrypted manuscripts and encryption keys, with information about their origin and other relevant documents.

By bringing the expertise of the various disciplines together, we will digitize, process, and decrypt the historical encrypted sources and provide tools for (semi-) automatic decryption of these manuscripts with hidden content through a web service.

One of the items to highlight this year is the featured attack on Schlüsselgerät 41 by George Lasry. The Schlüsselgerät 41 was a scrambling machine from World War II. It could not be broken by the Allies (British) at Bletchely Park at that time. The machine is considered cryptographically sophisticated, even by today's standards. This is also expressed in the fact that the solution approach used by Lasry requires a great deal of computing power.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

Funded by:
Swedish Research Council (SRC)

FIG.: ISTOCK / PASEVEN

Hon.-Prof. Dr. Udo Helmbrecht

Quantum Communication

Within the framework of dtec.bw, project MuQuaNet constructs a quantum internet in the Munich metropolitan area in cooperation with partners in academia and industry. Goals are the test and research operations of a quantum communication network with selected civil and military applications.

Project MuQuaNet

Munich's Quantum Network

With the help of Quantum Key Distribution (QKD) and Post Quantum Cryptography (PQC), MuQuaNet constructs the first quantum-safe network in the Munich area. It analyzes the gain in IT security and investigates the integration into existing secure network architectures. Furthermore, the project demonstrates the utility of the QKD and PQC technologies by implementing both civil and military use cases.

THE DEVELOPMENT OF increasingly powerful quantum computers not only represents great progress for science but also a serious threat for current encryption methods. There are two main possibilities to counteract this threat: Post Quantum Cryptography (PQC) and Quantum Key Distribution (QKD). PQC is based on special mathematical problems which are believed not to be efficiently solvable, even by quantum computers. QKD, on the other hand, employs single light quanta (photons) to create identical keys at two different locations. Here, the security against potential eavesdroppers rests on the physical laws of quantum mechanics.

Quantum Communication Infrastructure

The project MuQuaNet has begun to construct the first quantum-safe network in the wider Munich area and began to analyze it with regard to the potential gain in security and the practicability of the novel QKD and PQC technologies. Partner organizations such as ZITiS, LMU, Airbus, BWI and DLR as well as several institutes of UniBw M (RI CODE, INF3, ETTI, dtec.bw) constitute the network nodes. They will be connected by dedicated dark fiber links and free space QKD links. The resulting network will employ a variety of different QKD devices using a range of protocols. In this way, different technologies can be compared and their usefulness for future applications can be evaluated.

Key Management and Security Analyses

IT security is an important topic beyond QKD and PQC. MuQuaNet researches the question in which way they can be integrated into existing secure network architectures.

For this, encryption devices on both layer 2 and layer 3 of the famous OSI layer model are employed. All questions related to this topic as well as to the question how to use QKD keys in the higher layers up to the application layer are the content of the key management work package.

In the security analysis work package, the network will be put to the test by conducting pentests as well as through investigating possible side channels. Thereby, weaknesses of the network can be identified. Moreover, theoretical security proofs of the used protocols will be critically investigated and improved.

Use Cases

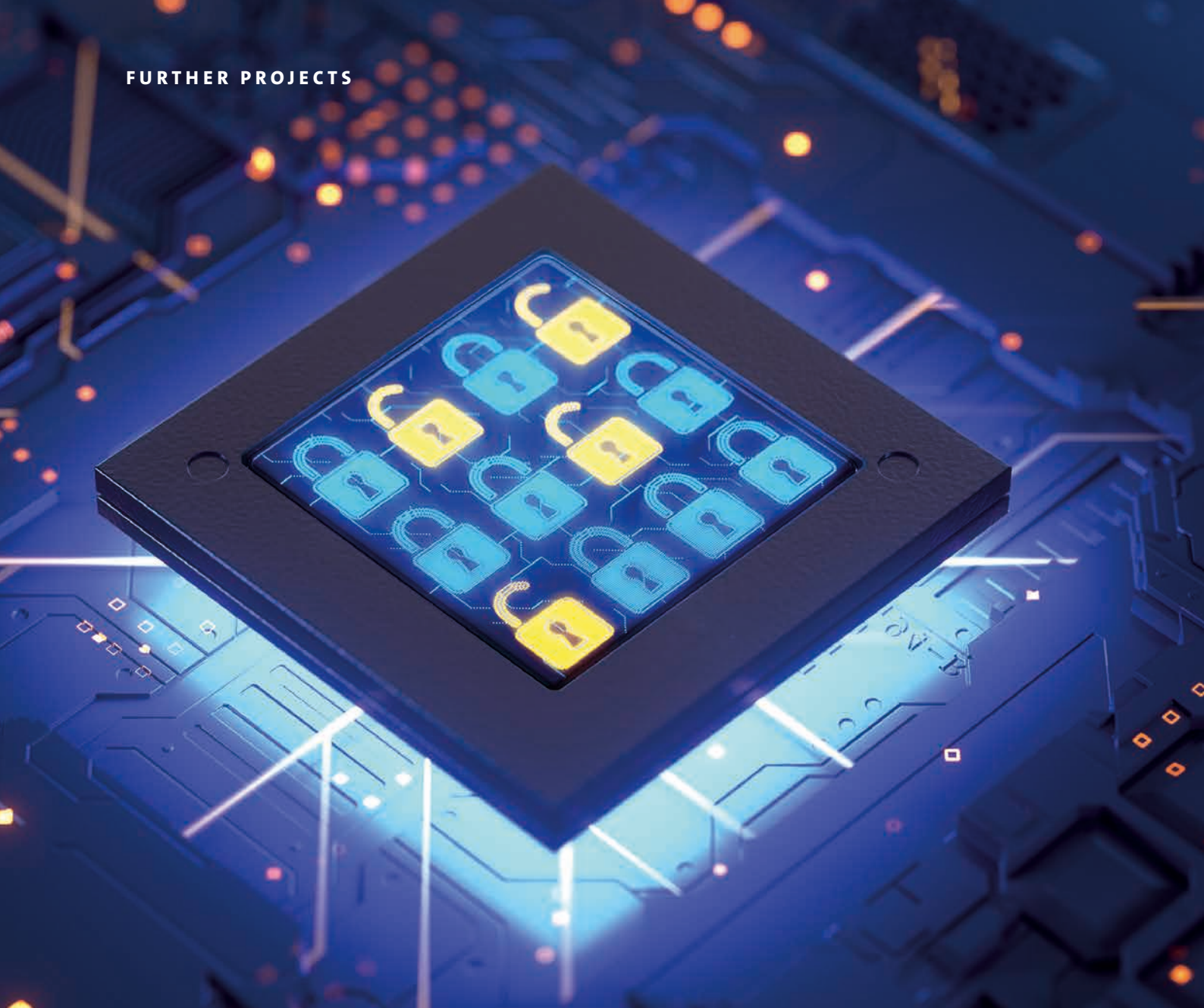
Civil and military use cases constitute a core area of the project. These include the quantum-safe remote maintenance of critical infrastructures, such as of a Bundeswehr naval ship. In MuQuaNet, this will be demonstrated as a proof of concept by remote-controlling a robot. In order to support the real-time transmission of video and control data, the network has to feature low latencies and high data rates. The data rate requirements are even higher for the second use case, the database application ADRIAN, for which several terabytes of sensitive personal data have to be transmitted in a secure way. The use cases are completed by implementing concepts of usable security as well as science communication and education in the context of QKD.

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

Funded by:
dtec.bw –Digitalization and technology Research Center of the Bundeswehr

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

FIG.: TAUSENDBLAUWERK.DE / MARKUS KRÄMER



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. Examples are the formal software verification of operating systems and graph theoretical modelling of IoT networks. The research is conducted in PhD projects and in cooperation with industry partners.

Project SW_GruVe: Mathematical Proofs Lead to Secure Software

Applying Formal Software Verification to Real-World Software Development

For decades already, the security of software based systems has been hampered by programming errors, despite sophisticated methods for error detection. Formal software verification has the potential of changing this, however, it requires an extreme effort for real-world programs. In the project SW_GruVe, together with an industry partner, the team of the research group increases the level of automation of formal verification to bring it closer to its practical application.

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 like Isabelle or Coq.

The Tools

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. In the predecessor project HoBIT the team investigated the Cogent language, developed by Data61 and the University of New South Wales, as an interesting candidate. It compiles abstract functional style specifications to executable C code and automates the verification process by generating a refinement proof which proves that the resulting code behaves as specified.

The verification target in the project is C code for operating system components, provided by the project partner HENSOLDT Cyber, from its TRENTOS system. In the HoBIT project, the researchers developed the tool Gencot for a semiautomatic translation from C code to Cogent. In SW_GruVe, they extend Gencot to a fully automatic translation of C statements with the exception of jumps. Translating the existing C code makes it accessible for verification.

Uniqueness Types

The code generated by Cogent uses pointers in a common memory to support efficient data manipulation. To be able to automatically prove its equivalence with a functional program, where all values are immutable, Cogent employs a uniqueness type system. Similar as in the language Rust it supports compile time checks that values compiled to pointers are never shared between different parts of the program, to ensure that no unexpected modification can occur for the referenced data values.

Gencot is not able to guarantee the uniqueness properties when it translates an arbitrary C program to Cogent, instead, however, the Cogent compiler can check the program for all places where the guarantees are violated. Only these parts need manual work to resolve the issues.

Data Abstraction

Although the translation by Gencot automates reasoning between functional specifications and executable code, it does not translate C data structures like arrays to more abstract data types such as mappings. In SW_GruVe, the team also develops a reasoning framework for abstracting the translated C data structures in Isabelle. Together with Gencot, it supports a relatively easy way of turning existing C programs into abstract specifications used to formally verify executable code.

As a proof of concept Gencot has been successfully applied to TRENTOS components. Gencot is open-source and available on GitHub.

Prof. Dr. Gunnar Teege

gunnar.teege@unibw.de

+49 89 6004 3353

www.unibw.de/fomset

Funded by:
Bavarian Ministry of Economic Affairs, Regional Development and Energy (StMWi)

FIG.: [M] SHUTTERSTOCK / BLUE ANDY, ISTOCK / MATEJMO

Cooperations

Germany and the World

FIG.: ADOBE STOCK / BAIVECTOR / TAUSENDBLAUWERK.DE

National Partners

The RI CODE is working with 47 partners in 34 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 the implementation of 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 Universität der Bundeswehr München, we work with 47 institutions in 34 cities and municipalities nationwide. A focus is on Bavaria and the Munich area, North Rhine-Westphalia and Hessia. ■

Institution	Location
Universität Bayreuth	Bayreuth
govdigital eG	Berlin
Bielefeld University of Applied Sciences	Bielefeld
Ruhr-Universität Bochum (RUB)	Bochum
Technische Universität Braunschweig	Braunschweig
University of Bremen	Bremen
Chemnitz University of Technology	Chemnitz
SoSafe GmbH	Cologne
Hochschule Darmstadt	Darmstadt
Technical University of Darmstadt	Darmstadt
ATHENE National Research Center for Applied Cybersecurity	Darmstadt
Technische Universität Dresden	Dresden
University of Duisburg-Essen	Duisburg-Essen
secunet Security Networks AG	Essen
Frankfurt University of Applied Sciences	Frankfurt am Main
IDunion, Main Incubator GmbH	Frankfurt am Main
Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities	Garching
Helmut Schmidt University Hamburg	Hamburg

Institution	Location
Technische Universität Ilmenau	Ilmenau
Leipzig University	Leipzig
Airbus Defence and Space	Manching
GESIS – Leibniz Institute for the Social Sciences	Mannheim
BWI GmbH	Meckenheim
Google Munich	Munich
LMU Munich	Munich
Central Office for Information Technology in the Security Sector (ZITiS)	Munich
FAST-DETECT GmbH	Munich
Rohde & Schwarz GmbH & Co. KG	Munich
Bavarian State Ministry for Digital Affairs (BayStMD)	Munich
Bavarian State Ministry for Health and Care (BayStMGP)	Munich
H & D GmbH	Munich
Technical University of Munich	Munich
Bavarian State Office for Taxes (BayLfSt)	Munich/Nuremberg/Zwiesel
Friedrich-Alexander-Universität Erlangen-Nürnberg	Nuremberg
Bavarian State Office for IT Security (BayLSI)	Nuremberg
IABG Industrieanlagen-Betriebsgesellschaft mbH	Ottobrunn
Paderborn University	Paderborn
WeFrame AG	Planegg
Max Planck Institute for Informatics, Saarland Informatics Campus	Saarbrücken
Fraunhofer Institute for Applied Information Technology (FIT)	Sankt Augustin
University of Siegen	Siegen
University of Stuttgart	Stuttgart
HENSOLDT Cyber GmbH	Taufkirchen
Airbus CyberSecurity	Taufkirchen
Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE)	Wachtberg/Bonn-Bad Godesberg
Hessian State Criminal Police Office	Wiesbaden
Bundeskriminalamt	Wiesbaden/Berlin


1 Hamburg
1 Bremen
2 Berlin
1 Braunschweig
1 Bielefeld
1 Paderborn
1 Duisburg
Bochum 1
Essen 1
1 Leipzig
1 Dresden
1 Chemnitz
1 Cologne
1 Siegen
Sankt Augustin 1
1 Meckenheim
Bonn 1
1 Wachtberg
1 Ilmenau
2 Wiesbaden
Frankfurt/Main 2
Darmstadt 3
1 Bayreuth
3 Nuremberg
1 Mannheim
1 Saarbrücken
1 Zwiesel
1 Manching
1 Stuttgart
Garching 1
10 Munich
Ottobrunn 1
1 Planegg
Taufkirchen 2
Map legend
1 Location with one partner
2 Location with several partners
Partner locations

Internationality

The RI CODE maintains a large international network. In 2021, employees came from 15 countries. We cooperated with 70 partners in 25 countries.

Employees

Nationality	Total
Argentine	2
Austrian	6
Bangladeshi	1
Bosnian	1
Brasilian/Argentine	1
British	1
Bulgarian	1
Croatian	1
Egyptian	2
Finnish	1
French	1
German	100
Slowenian/German	1
South Korean	1
Spanish	1

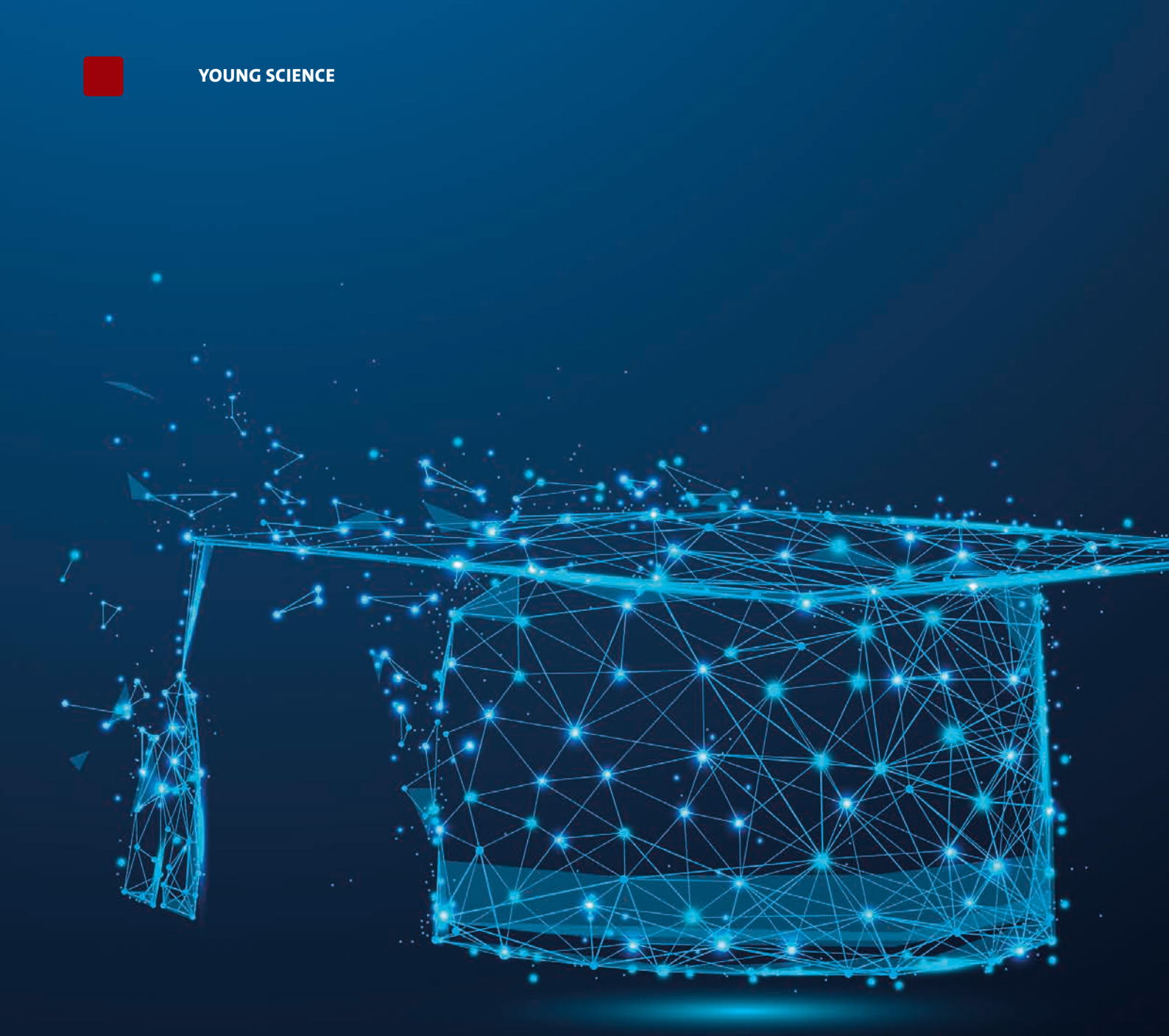
International Cooperation Partners

Country	Partner
Australia	The University of Melbourne
	University of New South Wales
Austria	Austrian Armed Forces
	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

FIG.: ISTOCK / BLUE PLANET STUDIO

Country	Partner
Denmark	Aarhus University
Egypt	German University in Cairo
France	Centre de Recherche de l'École de l'Air (CREA)
	Cyber-Detect
	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 Ministry of Digital Governance
Hungary	Budapesti Műszaki és Gazdaságtudományi Egyetem
	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
	Telenor Group
	University University of Oslo
Portugal	Efacec Electric Mobility
	University of Lisbon

Country	Partner
Romania	Babeș-Bolyai University
	Bitdefender
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
	Telefónica I+D
	Universitat Autònoma de Barcelona
Sweden	Chalmers University of Technology
	Ericsson
	RISE Research Institutes of Sweden
	University of Gothenburg
	Uppsala University
Switzerland	Ecole Polytechnique Fédérale de Lausanne
	ID Quantique SA
	RUAG
	University of Lausanne
	University of St. Gallen
	University of Zurich
United Kingdom	Imperial College London
	Lancaster University
	University College London
	University of Glasgow
U.S.A.	Auburn University, Samuel Ginn College of Engineering
	Davidson College
	George C. Marshall European Center for Security Studies
	The University of Arizona, College of Engineering
	The University of North Carolina at Charlotte



Young Science

Offers and Opportunities

FIG.: ADOBE STOCK / PICKUP

Study Award of the Research Institute CODE 2021

Realistic data sets for IT forensics

Martin Lukner, graduate of the Master's program in cybersecurity, received the study award of the Research Institute CODE 2021. In his thesis, he worked on generating configurable and realistic data sets for IT forensics.

MALWARE, or malicious software, plays a major role in today's IT security incidents. Reliable tools and up-to-date expert knowledge are required to handle these incidents. In order to evaluate the tools on a solid basis and to train experts in IT forensics in a realistic way, case-specific data sets are essential. Martin Lukner's work entitled „Synthesis and evaluation of malware traces on Windows systems" addresses this need.

Individual design of malware traces

In most cases, existing data sets are too small, outdated or can only be used in certain cases. For this reason, so-called „synthesis frameworks" have been developed in recent years to automatically generate the required malware traces. However, in none of these frameworks it is possible to configure the traces according to certain specifications. In his research, Martin Lukner therefore designed an extension of a framework already existing at the Professorship of Digital Forensics of Prof. Dr. Harald Baier, which allows exactly that: The new component for malware makes it possible to design traces according to individual wishes and thus contributes to creating diverse scenarios on different levels of difficulty. This is achieved by using different network protocols and encryption types. Traces on the network as well as on hard disks and in the working memory are taken into account.

Research published at relevant conference

With his thesis, which was supervised at the CODE professorship of Digital Forensics, Martin Lukner significantly contributes to generating configurable, case-specific, real-world datasets for IT forensics. Concept, implementation and evaluation of his thesis are excellent. It was successfully presented as a publication in January 2022 at a relevant conference for digital forensics (Eighteenth IFIP WG 11.9 International Conference on Digital Forensics) under the title „On Realistic and Configurable Synthesis of Malware Traces on Windows Systems". ■

> "This thesis has given me the opportunity to work on a scientific project that is not only highly relevant, but also brings together several of my areas of interest."
>
> *Award winner Martin Lukner*

Reliable tools are needed to deal with IT security incidents caused by malware.

FIG.: SMOLAW11 / ADOBE STOCK; SITTHIPHONG / ADOBE STOCK

Study Awards of the Universität der Bundeswehr München

Every year, the Universität der Bundeswehr München 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

Studying at the Research Institute CODE

The Master's program in Cyber Security at the RI CODE of the Universität der Bundeswehr München 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 skills are taught – such as those needed for 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's 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 support by the teaching staff, 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 round out the advantages.

Further Information

Master's program Cyber Security:
https://go.unibw.de/8o
(in German)

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

DOCTORATES 2021

Tanja Hanauer

"Visualization-based Enhancement of IT Security Management and Operations"

THE THESIS "Visualization-based Enhancement of IT Security Management and Operations" introduces a process framework for security visualization that supports the generation of an overview and the manageability of an organization's IT, its processes, selected security-specific tasks, and the data they rely on. It also supports the generation of organizational knowledge, knowledge generation through knowledge transfer amongst stakeholders, and the transformation from individual into organizational knowledge. In general, it is expected that applying the framework enhances the security of organizations.

Tanja Hanauer received her doctorate with Prof. Dr. Wolfgang Hommel as primary advisor in February 2021. During her PhD, she was employed at the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities. Currently, she works as a consultant for information security. ■

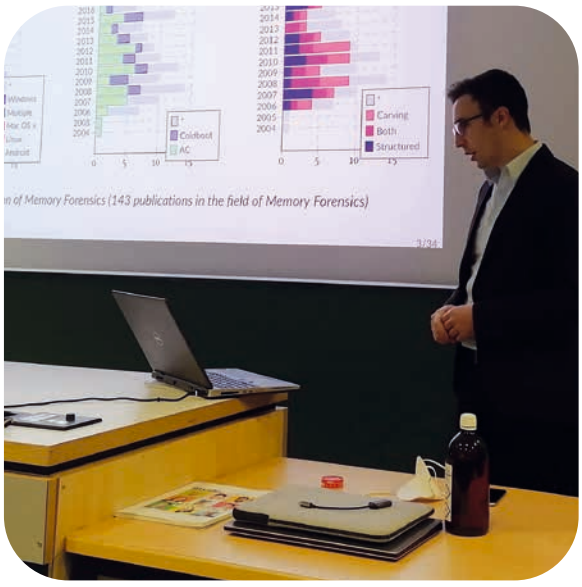
FIG.: PRIVATE (2)

Lorenz Liebler

"Towards Carving-Based Post-Mortem Memory Forensics and the Applicability of Approximate Matching"

THE FIELD OF memory forensics is an important branch of digital forensics. Various concepts enable practical experts to perform detailed analyses of potentially compromised systems by evaluating the volatile memory of a target. Lorenz Liebler's dissertation deals with the (re)detection of digital artifacts in a secured main memory image. He investigates and further develops the approach of memory carving, i.e., the classification of digital artifacts without interpreting structural data of the main memory (i.e., without using information of the operating system, e.g., about processes, handles, sockets). The central topic of the thesis is the conceptual design, implementation, and evaluation of the transferability of approximate matching functions to the field of memory forensics.

Lorenz Liebler defended his dissertation on December 7, 2021. The thesis was supervised by Prof. Dr. Harald Baier. Liebler completed his Master's degree at the Department of Computer Science at the Darmstadt University of Applied Sciences in October 2016, subsequently was a research assistant there, and has been working for a private cybersecurity service provider since the end of 2020. ■



Hacking Contest Full of Fun and Action

“Game of Trons”: Capture the Flag 2021

In the fall of 2021, the 7th “Capture the Flag” hacking competition (CTF) of the Research Institute CODE took place both on the campus of the Universität der Bundeswehr München as well as online – supported by ITIS e.V. and Team localos.

AT THE END OF NOVEMBER, a total of 14 teams that had passed the online qualifying as the best of 60 came together on the Neubiberg campus – in accordance with the applicable COVID-19 protection measures, of course – to compete in various areas of cybersecurity. Another 15 groups battled for victory in the online competition with a slightly different range of tasks. For 18 hours, the participants – among them several student teams – solved demanding challenges.

From Forensics to Virtual Reality: A Wide Variety of Tasks

As usual, RI CODE's CTF was held under a motto that determined the storyline and the design of the challenges: in accordance with the event title "Game of Trons" – a reference to the successful fantasy series "Game of Thrones" and the sci-fi epic "Tron" – the goal was to populate continents and gain dominance over them.

The total of 49 tasks this year came from the categories crypto, web, forensics, misc and reversing/pwning. In addition to the classic challenges, most of which were based on real exploits, there were also unusual tasks awaiting the teams: for example, the participants were confronted with a hardware challenge involving an oscilloscope or a virtual reality challenge from Team localos. A total of 36 tasks were successfully completed.

In the virtual reality challenge, a correct command sequence had to be entered to fight off dragons and save a threatened castle.

FIG.: RI CODE (3)

In the virtual reality challenge, a correct command sequence had to be entered to fight off dragons and save a threatened castle.

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

CTFS PROVIDE an opportunity to develop cybersecurity skills in a fun way, contributing to hands-on education. The Research Institute CODE's "Capture the Flag" is a hacking competition focused on the acquisition of knowledge, team building and fun. Since 2015, it is held once a year on the campus of the Universität der Bundeswehr München in Neubiberg. Not only students can test their theoretical knowledge during the event by solving different practical challenges.

RI CODE's Managing Director Volker Eiseler (left) with the winning team "Nemesis", which earned the right to put their names on the so-called "Flag of Fame".

Right to the end the race was tight, but finally the result was clear: The four lucky winners belonged to the team "Nemesis". Second place went to "Team T5", third place to "Sabobatage". The online track was won by the "Careless Eagles" followed by "0x90" and "Ignorital". The event ended with a big surprise: The SANS Institute EMEA, a renowned provider of cybersecurity training and certification, donated a total of four vouchers for an on-demand course to the winning team of the on-site track. The Research Institute CODE would like to say Thank you for the generous prize as well as for the support of various other partners, who made the event possible in this form. ■

More Information

www.unibw.de/code/events/ctf

www.unibw.de/code/news/ctf-2021-game-of-trons (in German)

ctf@unibw.de

Addendum

Publications, Activities and Organizational Chart

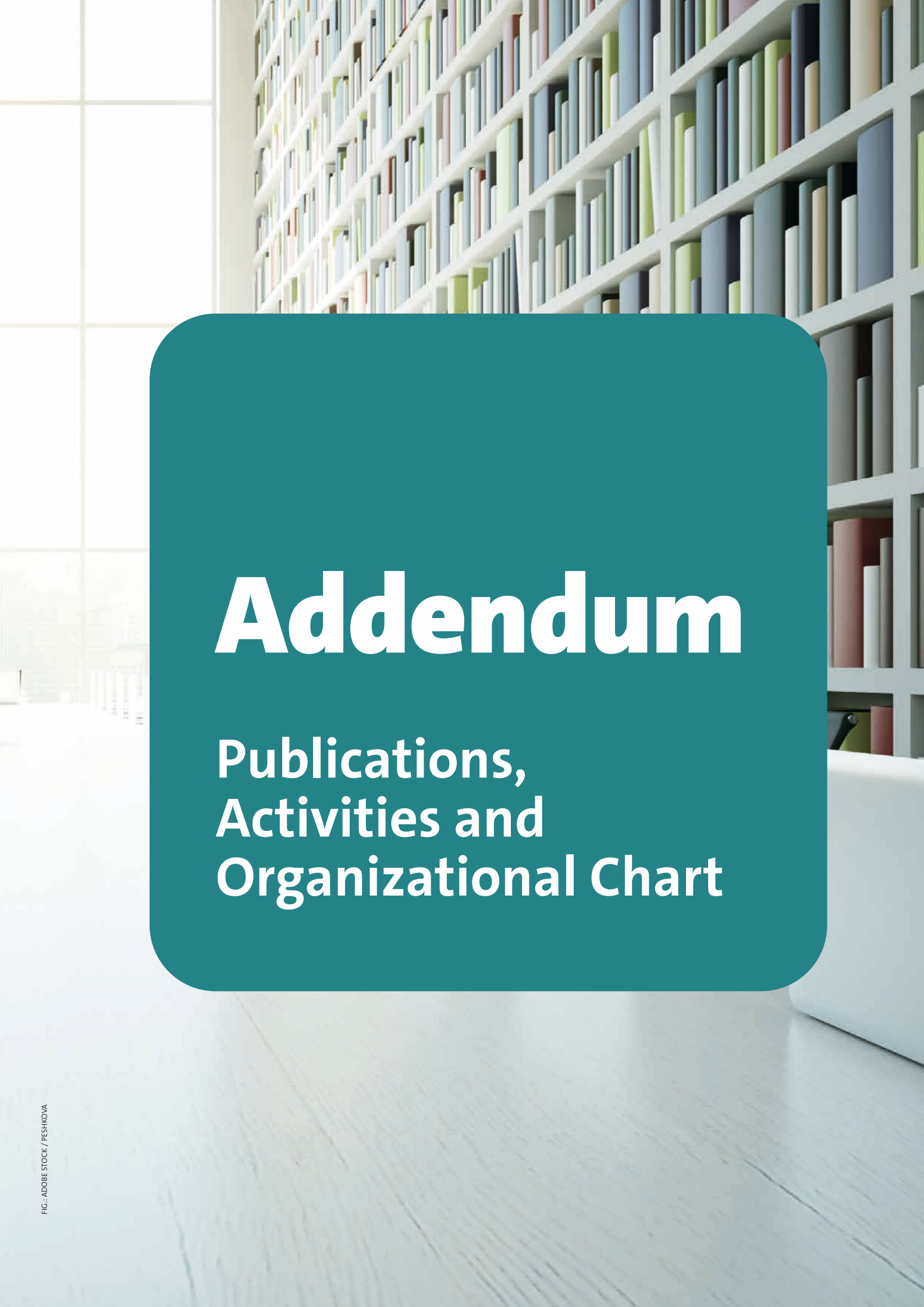


FIG.: ADOBE STOCK / PESHKOVA

Prof. Dr.
Florian Alt

Usable Security and Privacy

PUBLICATIONS

ABDRABOU, Y., ABDELRAHMAN, Y., KHAMIS, M., ALT, F.: Think about it! Investigating the Effect of Password Strength on Cognitive Load during Password Creation. CHI'21 Extended Abstracts, ACM.

ABDRABOU, Y., SHAMS, A., MANTAWY, M. O., KHAN, A. A., KHAMIS, M., ALT, F., ABDELRAHMAN, Y.: GazeMeter: Exploring the Usage of Gaze Behaviour to enhance Password Assessments. ETRA'21, ACM.

ABDRABOU, Y., HATEM, R., ABDELRAHMAN, Y., ELMOUGY, A., KHAMIS, M.: Passphrases Beat Thermal Attacks: Evaluating Text Input Characteristics Against Thermal Attacks on Laptops and Smartphones. INTERACT'21', Springer.

ALT, F.: Out of the Lab Research in Usable Security and Privacy. UMAP'2021 Adjunct Proceedings, ACM.

ALT, F.: Pervasive Security and Privacy — A brief reflection on challenges and opportunities. IEEE Pervasive Computing, vol. 20, iss. 4, 2021.

ALT, F., BUSCHEK, D., HEUSS, D., MÜLLER, J.: Orbuculum – Predicting When Users Intend To Leave Large Public Displays. IMWUT, ACM.

ALT, F., SCHNEEGASS, S.: Beyond Passwords – Challenges and Opportunities of Future Authentication. IEEE Security & Privacy (to appear).

BRAUN, M., WEBER, F., ALT, F.: Affective Automotive User Interfaces – Reviewing the State of Driver Affect Research & Emotion Regulation in the Car. ACM Computing Surveys.

BUSCHEK, D., ALT, F.: Intelligent Computing for Interactive System Design, ACM, Chapter: Building Adaptive Touch Interfaces.

DELGADO RODRIGUEZ, S., PRANGE, S., MECKE, L., ALT, F.: ActPad – A Smart Desk Platform to Enable User Interaction with IoT Devices. CHI'21 Extended Abstracts, ACM.

DELGADO RODRIGUEZ, S., PRANGE, S., ALT, F.: Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible. In 'Mensch und Computer 2021 - Workshopband', Gesellschaft für Informatik e.V.

FALTAOUS, S., ABDULMAKSOUD, A., KEMPE, M., ALT, F., SCHNEEGASS, S.: GeniePutt: Augmenting human motor skills through electrical muscle stimulation. it – Information Technology.

FROEHLICH, M., WAGENHAUS, M., SCHMIDT, A., ALT, F.: Don't Stop Me Now! Exploring Challenges Of First-Time Cryptocurrency Users. DIS'21, ACM.

FROEHLICH, M., KOBIELLA, C., SCHMIDT, A., ALT, F.: Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences. DIS'21, ACM.

KHAMIS, M., ALT, F.: Technology-Augmented Perception and Cognition, Springer International Publishing, Cham, Chapter: Privacy and Security in Augmentation Technologies, pp. 257 – 279.

LIEBERS, J., GRUENEFELD, U., MECKE, L., SAAD, A., AUDA, J., ALT, F., ABDELAZIZ, M., SCHNEEGASS, S.: Understanding User Identification in Virtual Reality through Behavioral Biometrics and the Effect of Body Normalization. CHI'21, ACM.

MARKY, K., PRANGE, S., MÜHLHÄUSER, M., ALT, F.: Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents. MUM'21, ACM.

MÄEKELÄ, V., KLEINE, J., HOOD, M., ALT, F., SCHMIDT, A.: Hidden Interaction Techniques: Concealed Information Acquisition and Texting on Smartphones and Wearables. CHI'21, ACM.

MÜLLER, L., PFEUFFER, K., GUGENHEIMER, J., PRANGE, S., PFLEGING, B., ALT, F.: SpatialProto: Using Real-World Captures for Rapid Prototyping of Mixed Reality Experiences. CHI'21, ACM.

NUSSBAUM, A., SCHUETTE, J., HAO, L, SCHULZRINNE, H., ALT, F.: Tremble: TRansparent Emission Monitoring with BLockchain Endorsement. iThings'21, IEEE.

PFEUFFER, K., ABDRABOU, Y., ESTEVES, A., RIVU, R., ABDELRAHMAN, Y., MEITNER, S., SAADI, A., ALT, F.: ARtention: A Design Space for Gaze-adaptive User Interfaces in Augmented Reality. Computers & Graphics.

PFEUFFER, K., DINC, A., OBERNOLTE, J., RIVU, R., ABDRABOU, Y., SCHELTER, F., ABDELRAHMAN, Y., ALT, F.: Bi-3D: Bi-Manual Pen-and-Touch Interaction for 3D Manipulation on Tablets. UIST '21, ACM.

PIENING, R., PFEUFFER, K., ESTEVES, A., MITTERMEIER, T., PRANGE, S., SCHROEDER, P., ALT, F.: Gaze-adaptive Information Access in AR: Empirical Study and Field-Deployment. INTERACT'21, Springer.

PRANGE, S., SHAMS, A., PIENING, R., ABDELRAHMAN, Y., ALT, F.: PriView – Exploring Visualisations Supporting Users' Privacy Awareness. CHI'21, ACM.

PRANGE, S., MAYER, S., BITTL, M.-L., HASSIB, M., ALT, F.: Investigating User Perceptions Towards Wearable Mobile Electromyography. INTERACT'21, Springer.

PRANGE, S., GEORGE, C., ALT, F.: Design Considerations for Usable Authentication in Smart Homes. Mensch Und Computer 2021, ACM.

PRANGE, S., MARKY, K., ALT, F.: Usable Authentication in Multi-Device Ecosystems. CHI'21 Workshop on User Experience for Multi-Device Ecosystems: Challenges and Opportunities.

RIVU, S. R. R., ABDRABOU, Y., ABDELRAHMAN, Y., PFEUFFER, K., KERN, D., NEUERT, C., BUSCHEK, D., ALT, F.: Did you Understand this? Leveraging Gaze Behavior to Assess Questionnaire Comprehension. ETRA'21, ACM.

RIVU, R., JIANG, R., MKELÄ, V., HASSIB, M., ALT, F.: Exploring Emotions and Emotion Elicitation Techniques in Virtual Reality. INTERACT'21, Springer.

RIVU, R., ZHOU, Y., WELSCH, R., MÄKELÄ, V., ALT, F.: When Friends become Strangers: Understanding the Influence of Avatar Gender On Interpersonal Distance Between Friends in Virtual Reality. INTERACT'21, Springer.

RIVU, R., MÄKELÄ, V., HASSIB, M., ABDELRAHMAN, Y., ALT, F.: Exploring how Saliency Affects Attention in Virtual Reality. INTERACT'21, Springer.

RIVU, R., MÄKELÄ, V., PRANGE, S., RODRIGUEZ, S. D., PIENING, R., ZHOU, Y., KÖHLE, K., PFEUFFER, K., ABDELRAHMAN, Y., HOPPE, M., SCHMIDT, A., ALT, F.: Remote VR Studies – A Framework for Running Virtual Reality Studies Remotely Via Participant-Owned HMDs. ACM Transactions on Computer-Human Interaction (ToCHI).

SAAD, A., LIEBERS, J., GRUENEFELD, U., ALT, F., SCHNEEGASS, S.: Understanding Bystanders' Tendency to Shoulder Surf Smartphones Using 360-degree Videos in Virtual Reality. MobileHCI'21, ACM.

SCHMIDT, A., ALT, F., MÄKELÄ, V.: Evaluation in human-computer interaction – beyond lab studies. CHI'21 Extended Abstracts, ACM.

RESEARCH PROJECTS

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: 1/2019–7/2021

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, containing multiple users with changing behavior, different physicalities, and changing sensing and interaction capabilities.

Funded by: DFG
Duration: 4/2020–3/2023

TEACHING

3665-V1 **Secure human-computer interfaces**

36651 **Usable Security**

36653 **Design of Usable and Secure Systems**

FAIRS, CONFERENCES, SEMINARS

- CHI 2021 Course: Evaluation in Human-Computer Interaction – Beyond Lab Studies
- SOUPS 2021: VR4Sec – Workshop on Security for XR and XR for Security
- ETRA 2021: EyeSec – Workshop on Eye-Gaze for Security Applications

PRIZES AND AWARDS

- Google Faculty Research Award 2021
- Designing Interactive Systems (DIS 2021) – Honorable Mention Award for the paper: M. Froehlich, C. Kobiella, A. Schmidt, and F. Alt. Is It Better With Onboarding? Improving First-Time Cryptocurrency App Experiences.
- Mobile and Ubiquitous Multimedia (MUM'21) – Honorable Mention Award for the paper: K. Marky, S. Prange, M. Mühlhäuser, and F. Alt. Roles Matter! Understanding Differences in the Privacy Mental Models of Smart Home Visitors and Residents.

ADDITIONAL FUNCTIONS

- Subcommittee Chair for CHI 2021
- Associate Chair for Interact 2021
- Program Committee Member for SOUPS 2021
- Program Committee Member for EuroUSEC 2021
- Program Committee Member for IEEE AIVR 2021
- Demo Chair for MobileHCI 2021
- Workshop Chair for ETRA 2021
- Associate Editor for Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT)
- Editorial Board Member for IEEE Pervasive Computing
- Department Chair for Security and Privacy for IEEE Pervasive Computing Magazine

Prof. Dr. Harald Baier

Digital Forensics

PUBLICATIONS

GÖBEL, TH.; UHLIG, F.; BAIER, H.: Empirical Evaluation of Network Traffic Analysis using Approximate Matching Algorithms, in Proceedings of the 12th EAI International Conference on Digital Forensics & Cyber Crime (ICDF2C), Singapore, December 2021.

GÖBEL, TH.; UHLIG, F.; BAIER, H.: Empirical Evaluation of Network Traffic Analysis using Approximate Matching Algorithms, in Proceedings of 19th Annual IFIP WG 11.9 International Conference on Digital Forensics, p.89-108, Springer, online, January 2021.

MUNDT, M.; BAIER, H.: Towards Mitigation of Data Exfiltration Techniques using the MITRE ATT&CK Framework, in Proceedings of the 12th EAI International Conference on Digital Forensics & Cyber Crime (ICDF2C), Singapore, December 2021.

TEACHING

1162 **Digital Forensics (WT)**

3824 **Digital Forensics (AT)**

5501/1009 **Seminar Digital Forensics (AT + WT)**

5501/1009 **Seminar Forensic Methods in Computer Science (HT)**

5505 **IT Forensics (ST)**

FAIRS, CONFERENCES, SEMINARS

Preparation and moderation of the CAST Forensics/Cybercrime workshop on 12/16/2021, URL: https://cast-forum.de/workshops/infos/302

ADDITIONAL FUNCTIONS

- Reviewer for "Journal of Digital Investigation" and "Computers & Security"
- Membership in program committees: Digital Forensics Research Workshop (DFRWS) EU 2021, CAST Grant Award 2021, CAST-GI Doctoral Award 2021
- 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

PUBLICATIONS

DESHARNAIS, M., AND BRUNTHALER, S.: Towards efficient and verified virtual machines for dynamic languages, in Proceedings of the 10th ACM SIGPLAN International Conference on Certified Programs and Proofs, Virtual Event, Denmark, January 17-19, 2021.

WIESINGER, M., DORFMEISTER, D., AND BRUNTHALER, S.: MAD: Memory Allocation Diversity, In Proceedings of the 1st Workshop on DRAM Security, co-located with ISCA 2021, Virtual Event, June 17, 2021.

RESEARCH PROJECTS

ACSE (Airborne Cyber Security Enhancement)

The Research Institute CODE collaborates with Airbus DS on comprehensive research understanding and addressing 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, Manching
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 Pilot (Dependable Production Systems Pilot Project)

Within the DEPS Pilot project, the research group analyzed the feasibility of combining two hitherto separate research areas to devise an efficient method of binding hardware to software.

Funded by: Government of Upper Austria, Software Competence Center Hagenberg
Duration: 2020–2021

DEPS (Dependable Production Systems)

Leveraging the positive feasibility results of the DEPS Pilot project, 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 regular, known ways to attack software systems will 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: 2021–2025

TEACHING

1009 **Seminar Language-based Security (WT)**

1009 **Seminar Optimization of Programming Languages (AT)**

1010 **Machine-oriented Programming (WT)**

3647 **Compiler Construction (WT + AT)**

55071 **Language-based Security (ST)**

FAIRS, CONFERENCES, SEMINARS

- CPP'21
- ISCA'21
- IFIP WG 2.4

PRIZES AND AWARDS

Elected Member of IFIP Working Group 2.4 "Software Implementation Technology"

ADDITIONAL FUNCTIONS

- PC Member of IEEE Security & Privacy, 2022
- PC Member of AvioSE'22
- Vice-Dean
- Faculty-Council Member

Prof. Dr. Michaela Geierhos

Data Science

PUBLICATIONS

ADLER, A.; GEIERHOS, M.; HOBLEY, E. (2021): Influence of Training Data on the Invertability of Neural Networks for Handwritten Digit Recognition. 20th IEEE Intl. Conf. on Machine Learning and Applications (ICMLA). Piscataway, NJ: IEEE. 2021. pp. 731-738.

BÄUMER, F. S.; KERSTING, J.; DENISOV, S.; GEIERHOS, M. (2021): In Other Words: A Naive Approach to Text Spinning. 18th Intl. Conf. on Applied Computing 2021. pp. 221–225.

BÄUMER, F. S.; DENISOV, S.; GEIERHOS, M.; LEE, Y. S. (2021): Towards Authority-Dependent Risk Identification and Analysis in Online Networks. STO-MP-IST-190: NATO Science and Technology Organization. 2021.

HÖLLIG, J.; DUFTER, P.; GEIERHOS, M.; ZIEGLER, W.; SCHÜTZE, H. (2021): Semantic Text Segment Classification of Structured Technical Content. In: Métais, E.; Meziane, F.; Horacek, H.; Kapetanios, E. (Eds.): Natural Language Processing and Information Systems (NLDB), Saarbrücken, Germany, June 23–25, 2021. Cham: Springer. pp. 165–177. LNCS 12801.

HÖLLIG, J.; LEE, Y. S.; SEEMANN, N.; GEIERHOS, M. (2021): Effective Detection of Hate Speech Spreaders on Twitter. In: Faggioli, G.; Ferro, N.; Joly, A.; Maistro, A.; Piroi, F. (Eds.). Working Notes of CLEF 2021: Conference and Labs of the Evaluation Forum. 2021. pp. 1976–1986. CEUR Workshop Proceedings 2936.

KAUFF, M.; ANSLINGER, J.; CHRIST, O.; NIEMANN, M.; GEIERHOS, M.; HUSTER, L. (2021): Ethnic and gender-based prejudice towards medical doctors? The relationship between physicians' ethnicity, gender, and ratings on a physician rating website. The Journal of Social Psychology. 2021.

KERSTING, J.; GEIERHOS, M. (2021): Towards Aspect Extraction and Classification for Opinion Mining with Deep Sequence Networks. In: Loukanova, R. (Ed.): Natural Language Processing in Artificial Intelligence – NLPinAI 2020. Cham: Springer. 2021. pp. 163–189. SCI 939.

KERSTING, J.; GEIERHOS, M. (2021): Human Language Comprehension in Aspect Phrase Extraction with Importance Weighting. In: Métais, E.; Meziane, F.; Horacek, H.; Kapetanios, E. (Eds.): Natural Language Processing and Information Systems (NLDB), Saarbrücken, Germany, June 23–25, 2021. Cham: Springer. pp. 231–242. LNCS 12801.

KERSTING, J.; GEIERHOS, M. (2021): Well-Being in Plastic Surgery: Deep Learning Reveals Patients' Evaluations. 10th Intl. Conf. on Data Science, Technology and Applications (DATA 2021): SCITEPRESS. 2021. pp. 275–284.

MERTEN, M.-L.; WEVER, M.; GEIERHOS, M.; TOPHINKE, D.; HÜLLERMEIER, E. (2021): Annotation Uncertainty in the Context of Grammatical Change. 2021. pp. 1–18. https://arxiv.org/pdf/2105.07270

MITTERMEIER, T.; FRANK, M.; ULLRICH, S.; DREO RODOSEK, G.; GEIERHOS, M. (2021): A Multimodal Mixed Reality Data Exploration Framework for Tactical Decision Making. 21st Intl. Conf. on Military Communications and Information Systems (ICMCIS). Piscataway, NJ: IEEE. 2021. pp. 1-8.

ULLRICH, S.; GEIERHOS, M. (2021): Towards Constructing Multi-Hop Reasoning Chains Using Local Cohesion. The CODE 2021. www.unibw.de/code-events/05_ullrich.pdf

ULLRICH, S.; GEIERHOS, M. (2021): Using Bloom's Taxonomy to Classify Question Complexity. Proc. of the Intl. Conf. on Natural Language and Speech Processing (ICNLSP). Nov. 12 –13, 2021, Trento, Italy.

RESEARCH PROJECTS

CRC 901 "On-the-Fly Computing" "Parameterized Service Specifications"

In terms of agile, participative software development, end users will be more involved in the interactive composition process of software services to be created on-the-fly. For this purpose, it is necessary to transparently clarify which requirements were taken into account during the creation and which had to be dropped.

Funded by: German Research Foundation (DFG)
Duration: 7/2019–6/2023

Greater Munich Quantum Internet (MuQuaNet) "Authority-Dependent Risk Identification and Analysis in online Networks"

The aim is to automatically monitor selected apps and analyze the data they collect, correlate it with social media profiles, and form networks of people in order to identify potential targets and classify their risk potential on the basis of the given data.

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr
Duration: 10/2020–12/2024

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: 9/2021–12/2024

News Articles and Knowledge (NAWI)

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

Duration: 12/2021–11/2024

TEACHING

1009 **Knowledge Management**
1144 **Knowledge Discovery in Big Data**
3850 **Natural Language Processing**
3851 **Information Retrieval**
3852 **Data Science Applications**
3853 **Analysis of Unstructured Data**

PRIZES AND AWARDS

AI4HMO Best Paper Award

F. S. Bäumer and S. Denisov presented an approach for monitoring and analyzing fitness apps to identify targets of cyberattacks and assess their risk of exposure.

ADDITIONAL FUNCTIONS

- Member of the advisory board "German Biography" of the Historical Commission at the Bavarian Academy of Sciences and Humanities
- Expert for the Alexander von Humboldt Foundation

Program Committee

- AAAI 2021 – 35th AAAI Conf. on Artificial Intelligence
- ACL-IJCNLP 2021 – Joint Conf. of the 59th Annual Meeting of the Association for Computational Linguistics and the 11th Intl. Joint Conf. on Natural Language Processing
- EACL 2021 – Conf. of the European Chapter of the Association for Computational Linguistics
- EMNLP 2021 – Conf. on Empirical Methods in Natural Language Processing
- IoTBDS 2021 – 6th Intl. Conf. on Internet of Things, Big Data and Security
- NAACL-HLT 2021 – Conf. of the North American Chapter of the Association for Computational Linguistics – Human Language Technologies
- NLPCC 2021 – 10th CCF Intl. Conf. on Natural Language Processing and Chinese Computing
- PATTERNS 2021 – 13th Intl. Conf. on Pervasive Patterns and Applications
- SEMANTICS 2021 – 17th Intl. Conf. on Semantic Systems

Hon.-Prof. Dr. Udo Helmbrecht

Quantum Communication

PUBLICATIONS

AUER, M.: A portable and compact decoy-state QKD sender, in: 2021 Conference on Lasers and Electro-Optics Europe and European Quantum Electronics Conference, in: 2021 Conference on Lasers and Electro-Optics Europe and European Quantum Electronics Conference, 2021, Optica Publishing Group.

BÄUMER, F. S., DENISOV, S., GEIERHOS, M., LEE, Y. S.: Towards Authority-Dependent Risk Identification and Analysis in Online Networks, in: IST-190 Symposium on Artificial Intelligence, Machine Learning and Big Data for Hybrid Military Operations (2021, Koblenz), 2021, NATO Science and Technology Organization.

BÄUMER, F. S., KERSTING, J., DENISOV, S., GEIERHOS, M.: In other words: A naive approach to text spinning, in: Proceedings of the International Conferences on WWW/Internet 2021 and Applied Computing 2021, 2021, International Association for Development of the Information Society.

DELGADO RODRIGUEZ, S., PRANGE, S., ALT, F.: Take Your Security and Privacy Into Your Own Hands! Why Security and Privacy Assistants Should be Tangible, in: Wienrich, C., Wintersberger, P. & Weyers, B. (Hrsg.), Mensch und Computer 2021 – Workshopband, 2021, Gesellschaft für Informatik e.V.

HÖLLIG, J., LEE, Y. S., SEEMANN, N., GEIERHOS, M.: Effective Detection of Hate Speech Spreaders on Twitter, in: Proceedings of the Working Notes of CLEF 2021, 2021, CEUR Workshop Proceedings.

MÜLLER, L., PFEUFFER, K., GUGENHEIMER, J., PFLEGING, B., PRANGE, S., ALT, F.: Spatial-Proto: Exploring Real-World Motion Captures for Rapid Prototyping of Interactive Mixed Reality, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, Association for Computing Machinery.

PIENING, R., PFEUFFER, K., ESTEVES, A., MITTERMEIER, T., PRANGE, S., SCHRÖDER, P., ALT, F.: Looking for Info: Evaluation of Gaze Based Information Retrieval in Augmented Reality,in: Human-Computer Interaction – INTERACT 2021, 2021, Springer International Publishing.

PRANGE, S., SHAMS, A., PIENING, R., ABDELRAHMAN, Y., ALT, F.: PriView – Exploring Visualisations to Support Users' Privacy Awareness, in: Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, 2021, Association for Computing Machinery.

EVENTS

Invited Talk "MuQuaNet – The quantum network in the Munich area", Dr. Matthias Lienert, European Quantum Leadership Session 2: Quantum Communication, for recording see www.youtube.com/watch?v=oLSxPuqt6-o, Quantum Business Network, February 2021.

Prof. Dr. Wolfgang Hommel

Software and Data Security

PUBLICATIONS

FIETKAU, J., STOJKO, L.: Activity Support for Seniors Using Public Displays: A Proof of Concept. In: Schneegass, S.; Pfleging, B.; Kern, D. (Ed.). Tagungsband Mensch & Computer 2021. ACM 2021

GRABATIN, M., HOMMEL, W.: Self-sovereign Identity Management in Wireless Ad Hoc Mesh Networks. In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE 2021

GRABATIN, M., STEINKE, M., PÖHN, D., HOMMEL, W.: A Matrix for Systematic Selection of Authentication Mechanisms in Challenging Healthcare Related Environments. Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. ACM 2021

HANAUER, T.: Visualization-based Enhancement of IT Security Management and Operations. Dissertation, UniBw M 2021. 287 S.

KOCH, M., FIETKAU, J., STOJKO, L., BUCK, A.: Designing Smart Urban Objects – Adaptation, Multi-user Usage, Walk-up-and-use and Joy of Use. UniBw M, Schriften zur soziotechnischen Integration 2021

PHAM, S., SCHOPP, M., STIEMERT, L., SEEBER, S., PÖHN, D., HOMMEL, W.: Field Studies on the Impact of Cryptographic Signatures and Encryption on Phishing Emails. In Proceedings of the 7th International Conference on Information Systems Security and Privacy, Vol. 1: ICISSP 2021

PÖHN, D., HILLMANN, P.: Reference Service Model for Federated Identity Management. In: Augusto, A.; Gill, A.; Nurcan, S.; Reinhartz-Berger, I.; Schmidt, R.; Zdravkovic, J. (Ed.). Enterprise Business-Process and Information Systems Modeling. Springer LNBIP 2021

PÖHN, D., GRABATIN, M., HOMMEL, W.: eID and Self-Sovereign Identity Usage: An Overview. Electronics. Vol. 10. 2021. No. 22

PÖHN, D., HOMMEL, W.: Universal Identity and Access Management Framework for Future Ecosystems. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA). Vol. 12. 2021. No. 1.

PÖHN, D., HOMMEL, W.: Proven and Modern Approaches to Identity Management. In: Daimi, K.; Peoples, C. (Ed.). Advances in Cybersecurity Management. Springer International Publishing 2021

PÖHN, D., SEEBER, S., HANAUER, T., ZIEGLER, J., SCHMITZ, D.: Towards Improving Identity and Access Management with the IdMSecMan Process Framework. The 16th International Conference on Availability, Reliability and Security. ACM ARES 2021

STEINKE, M., HOMMEL, W.: FEDCON: An embeddable Framework for Managing MOC Functions and Interfaces in Federated Software Networks. In 2021 IFIP/IEEE International Symposium on Integrated Network Management (IM). IEEE 2021

STEINKE, M., STOJKO, L., BRUNNER, S., EISELER, V., HOFMANN, J., HOFMANN, M., HOMMEL, W., LANGER, U., RIEDL, J.: Smart Hospitals: Maßnahmenkatalog zur Verbesserung der IT-Sicherheit in Bayerischen Krankenhäusern. Ausgabe 2021/2022. Universität der Bundeswehr, Forschungsinstitut Cyber Defence (CODE). 2021. 133 S.

RESEARCH PROJECTS

Digital Identities with Self-Sovereign Identity Management: Processes and Technologies (DISPUT)

This project continues the work started in DISKURS by scientifically accompanying the establishment and operation of the national identity federation FINK.

In addition, the technological development of eID solutions based on Self-Sovereign Identity (SSI) management is analyzed. This involves the design of secure handling of highly sensitive personal data and a clear migration path.

Funded by: Bavarian State Ministry of Digital Affairs (StMD)
Duration: 4/2021–12/2022

Ledger Innovation and Operation Network for Sovereignty (LIONS)

The project LIONS builds a research platform for enhancing the resilience and digital sovereignty in digitalization using distributed ledger technologies.

As part of the interdisciplinary 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
Duration: 1/2021–12/2023

Smart Hospitals – Secure Digitization of Bavarian Hospitals

About 400 hospitals form a mainstay of healthcare provision in Bavaria. The project recorded the status quo of their technical and organizational IT security measures, especially in the context of current digitization projects. The findings have been incorporated into a catalog of measures to further increase the security level, which is currently available in the 2021/22 edition.

Funded by: Bavarian Ministry of Health and Care (StMGP)
Duration: 10/2018–11/2021

ROLORAN – Resilient Operation of LoRa Networks

As a far-reaching, energy-efficient wireless technology, LoRaWAN offers a promising foundation for persistent long-range communications. This project therefore investigates the robustness and limitations of LoRaWAN through experimental and theoretical analysis, supports protocol security through software hardening, and demonstrates applicability through the development of selected prototypes.

Funded by: dtec.bw – Digitalization and Technology Research Center of the Bundeswehr
Duration: 1/2021–12/2024

TEACHING

1006 **Introduction to Computer Science 1 (AT)**

1007 **Introduction to Computer Science 2 (WT)**

3459 **Selected Chapters of IT Security (WT+ST)**

5501 **Seminar Information Security in the Health Domain (WT, AT)**

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

5507 **Secure Networked Applications (ST)**

5508 **Information Security Management (ST)**

FAIRS, CONFERENCES, SEMINARS

Digitales Ich: Selbstbestimmte Identitäten im Netz. Event of Blockchain Bayern e.V. and the Bavarian State Ministry for Digital Affairs on 27.4.2021.

ADDITIONAL FUNCTIONS

- Dean of Studies of the computer science department (up to January 2021)
- Faculty council member
- Board of examiners for Master of Intelligence & Security Studies
- Member of the Operating Committee of the German Research and Education Network
- Reviewer in the Austrian research program Sparkling Science 2.0
- Technical Program Committee member:
  - IEEE Integrated Management (IM 2021)
  - IEEE International Conference on Communications (ICC 2021)
  - DFN Conference Security in Networked Systems 2021

Prof. Dr. Johannes Kinder

PATCH: Program Analysis, Transformation, Comprehension and Hardening

PUBLICATIONS

LORING, B., KINDER, J.: Systematic Generation of Conformance Tests for JavaScript. arXiv:2108.07075, 2021.

PATRICK-EVANS, J., DANNEHL, M., KINDER, J.: XFL: eXtreme Function Labeling. arXiv:2107.13404, 2021.

PONCE DE LEÓN, H., HASS, T., MEYER, R. DARTAGNAN: Leveraging Compiler Optimizations and the Price of Precision (Competition Contribution). In Proc. Tools and Algorithms for the Construction and Analysis of Systems (TACAS), pp. 428–432, Springer, 2021.

PONCE DE LEÓN, H., KINDER, J.: Cats vs. Spectre: An Axiomatic Approach to Modeling Speculative Execution Attacks. arXiv:2108.13818, 2021.

TEACHING

38191 **Reverse Engineering (ST)**

38192 **Reverse Engineering Lab (ST)**

55011 **Software Hardening Seminar (AT)**

55011 **Seminar Machine Learning in Reverse Engineering & Malware Detection (ST)**

55102 **Static Program Analysis (WT)**

55103 **Fuzzing Lab (WT)**

38491 **Dynamic Program Analysis (HT)**

38492 **Fuzzing Lab (HT)**

PROGRAM COMMITTEES

- ACM Conference on Computer and Communications Security (CCS)
- IEEE Symposium on Security & Privacy
- Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA)
- 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)

ADDITIONAL FUNCTIONS

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

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: 1/2021–12/2023

TEACHING

1016 **Introduction to Operation Systems**

5505 **Operating Systems Security**

Prof. Dr. Arno Wacker

Privacy and Compliance

PUBLICATIONS

HECK, H., WACKER, A.: Applying Harary Graph Structures to the Overlay Network Kademlia. 2021 International Conference on Computer Communications and Networks (ICCCN). DOI: 10.1109/ICCCN52240.2021.9522261, IEEE, pp. 1-8 (2021) [URL https://ieeexplore.ieee.org/document/9522261]

TEACHING

3480 **Secure Networks and Protocols**

55011 **Vulnerabilities and Attack Vectors Seminar**

55041 **Data Privacy**

55042 **Privacy Enhancing Technologies**

55061 **Introduction to Cryptography**

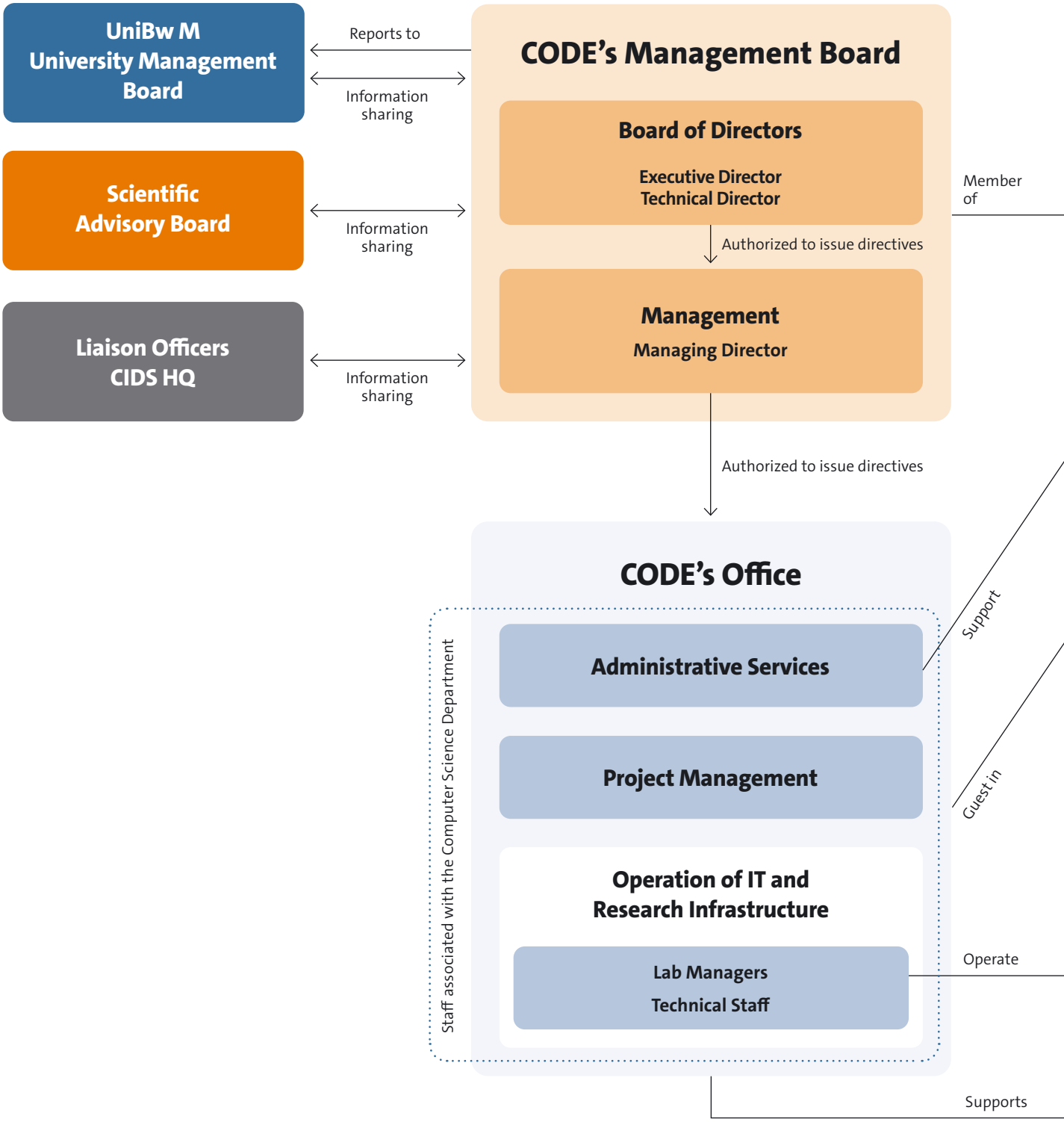
55091 **Penetration Testing**

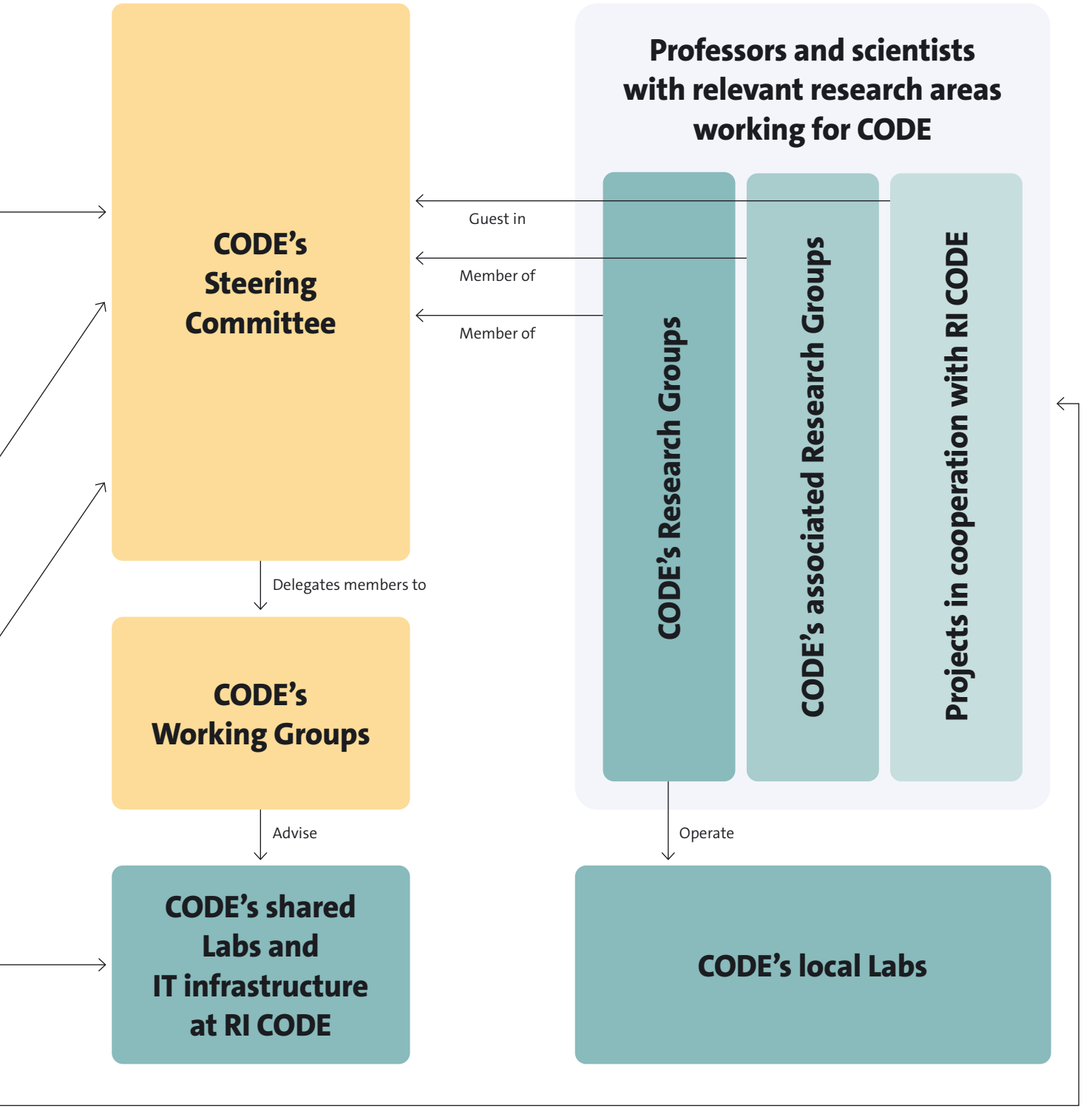
55093 **Penetration Testing Lab**

ADDITIONAL EVENTS

- Invited (online) talk at Gymnasium Ulricianum Aurich, 23.11.2021
  - o Title: "Insights into Cryptology and IT-Security"
- Invited (online) talk within the framework of the project "School & Newspaper", 23.11.2021
  - o Title: "You're Being Watched – Tricks and Tools of the Hackers"
    The Project "School & Newspaper" aims to promote students' media and reading skills by engaging them with the medium of the daily newspaper. The young people are to learn how to deal critically with media content.
- Invited talk on the real estate day IVD Mitte, Frankfurt/M, 30.9.2021
  - o Title: "You're Being Watched – Tricks and Tools of the Hackers"
- ARD-alpha: "Elections targeted by hackers", TV show, 22.6.2021
  - o Prof. Dr. Arno Wacker as a guest at alpha-demokratie

Organizational Chart 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)
Universität der Bundeswehr München
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
Universität der Bundeswehr München
Carl-Wery-Str. 22
81739 Munich
Germany

MANAGEMENT OF RI CODE

Prof. Dr. Wolfgang Hommel,
Executive Director (since 11/2021);
Technical Director (2/2021–10/2021);
Acting Executive Director (10/2021)

Prof. Dr. Gabi Dreo Rodosek,
Executive Director (until 9/2021)

Prof. Dr. Michaela Geierhos,
Technical Director (since 11/2021)

Prof. Dr. Udo Helmbrecht,
Technical Director (until 1/2021)

Dipl.-Inf. Volker Eiseler,
Managing Director (until 12/2021)

Marcus Knüpfer M. Sc.,
Acting Managing Director (since 1/2022)

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. Helmut Mayer,
Professor for Visual Computing

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 Privacy and Compliance

MEMBERS OF THE ADVISORY BOARD (IN 2021)

From the Department for Computer Science at the Universität der Bundeswehr München:

Prof. Dr. Uwe Borghoff (until 8/2021)

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Ulrike Lechner (since 8/2021)

Prof. Dr.-Ing. Helmut Mayer (since 8/2021)

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

Other Members

Prof. Dr. Aiko Pras,
University of Twente (NL)

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

Dr. Norbert Gaus,
Executive Vice President of Siemens AG

Ralf Wintergerst,
Chairman of the Management Board of Giesecke+Devrient GmbH

EDITING AND COORDINATION

Lisa Scherbaum M.A.,
Public Relations Officer

ART DIRECTION

Tausendblauwerk Design Agency
Michael Berwanger
www.tausendblauwerk.de

PROOFREADING

Nina Göringer,
Technical Translator M.A.
https://goeringer-fachuebersetzungen.de

PRINTED BY

Holzer Druck und Medien
www.druckerei-holzer.de

REGULATIONS

Editorial deadline: March 2022

Title illustration: Adobe Stock / Digital art

ISBN: 978-3-943207-63-7 | ISSN: 2748-9485

Also published as an electronic publication
(ISBN: 978-3-943207-64-4 | ISSN: 2748-9507)
as well as in German language
(ISBN: 978-3-943207-61-3 | ISSN: 2748-8780).


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