Universität der Bundeswehr München

CODE RI

ANNUAL REPORT 2020

Research Institute
Cyber Defence
Universität der Bundeswehr München

The Institute in Figures ▶▶▶

Universität der Bundeswehr München

RI CODE

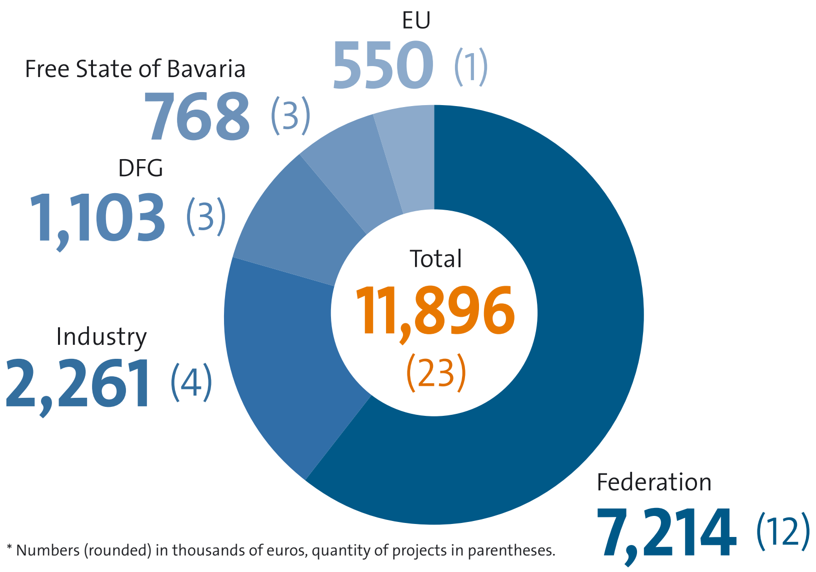
ANNUAL REPORT 2020

Research Institute
Cyber Defence
Universität der Bundeswehr München

Project Funding

In 2020, a total of 23 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 thousands of euros, quantity of projects in parentheses.

dtec.bw Project**

MuQuaNet – The greater
Munich area Quantum Internet

Participating Professorships

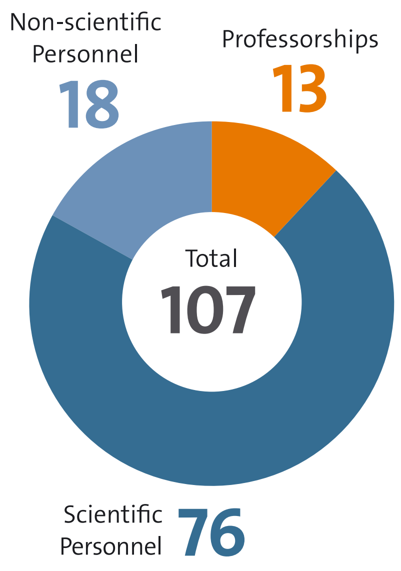
Prof. Dr. Udo Helmbrecht
Prof. Dr. Michaela Geierhos
Prof. Dr. Florian Alt

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

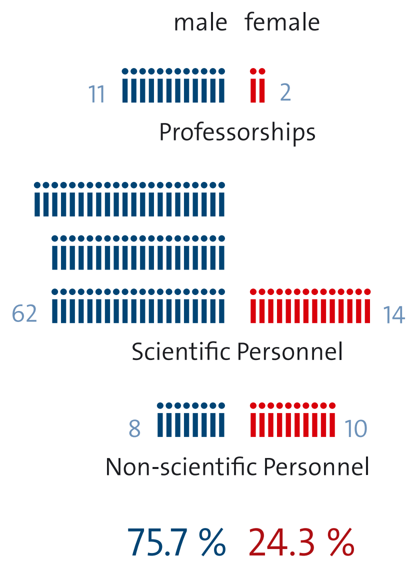
Staff Structure

RI CODE had a total of 107 employees in 2020.
The percentage of women was 24.3.

Employees



Gender Share



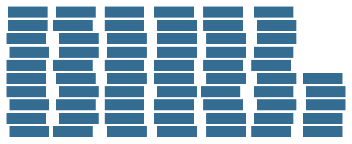
Research Work

Overview of doctorates and publications at RI CODE 2020

Doctorates

4

Publications



65

Internationality

RI CODE maintains a large international network.

Employees***

In 2020, the employees came from 14 countries.

Cooperation Partners***

In 2020, RI CODE cooperated with 79 partners in 28 countries.

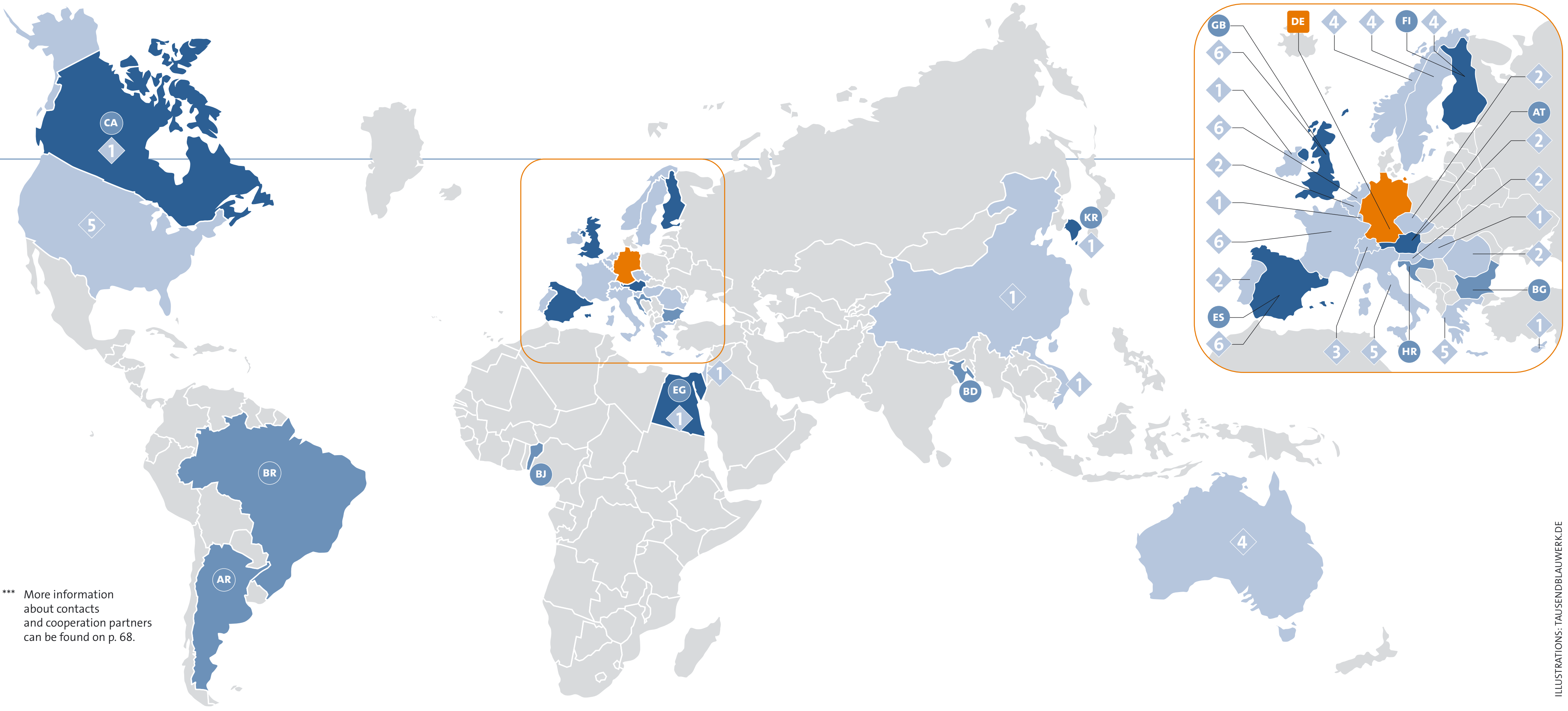
Legend

🟧 Location of RI CODE

AT Country of origin of CODE employees

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 on p. 68.

ILLUSTRATIONS: TAUSENDBLAUWERK.DE

Foreword by the President

We live in uncertain times. The range of threat scenarios is expanding more and more, as the COVID-19 pandemic clearly shows us. With its research centers, the Universität der Bundeswehr München concentrates decidedly on topics of security in society and technology. This involves both technical aspects, such as the problem of digital attacks on computer systems, and society's approach to the new challenges.

Our Research Institute CODE (RI CODE) for Cyber Defence and Smart Data is thematically located in the middle of the focus of these university priorities and can look back on a successful development in recent years. It was founded in 2013 as a research center and expanded in 2017 to become a research institute of the German Federal Government and the Bundeswehr. CODE is one of the leading research institutes in Germany and Europe, conducting both basic and applied research in the fields of cyber security, smart data and quantum technology. RI CODE's central task is to build a European ecosystem that enables and facilitates collaboration between national and international stakeholders from research, industry, public institutions, start-ups and venture capitalists.

I am therefore extremely pleased that the positive development of CODE can be mapped and documented for the first time in a comprehensive annual report, which is now available to you.

The growing importance of RI CODE is also reflected in an increasing number of professorships, research groups and employees, to whom I wish continued success in their exciting work!

With best regards

Prof. Dr. Merith Niehuss
President UniBw München

FIG.: PRIVATE, RI CODE

Dear Readers,

This first Annual Report is a small but important milestone on the growth path of the Research Institute CODE. It provides a fascinating insight into our extensive research areas as well as into selected projects of the professors involved. Furthermore, it gives highlights from the year 2020.

We are particularly happy about our new members: Prof. Dr. Michaela Geierhos has held the professorship for Data Science since April 2020, Prof. Dr. Harald Baier the professorship for Digital Forensics since September 2020. The excellence and visibility of Research Institute CODE is reflected in the significantly increasing numbers of scientific publications, third-party funded projects and collaborations, completed PhDs in our still emerging but internationally successful research groups, as well as the growth of our third major research area of quantum technologies.

In the pandemic year 2020, our Annual Conference entitled "Europe's Digital Sovereignty — Road to Success?" with more than 500 prominent guests was held for the first time completely digitally and as a contribution by the Federal Ministry of Defence to the German EU Council Presidency. Speakers included the Federal Minister of Defence Annegret Kramp-Karrenbauer and the Minister of Defence of the Netherlands Ank Bijleveld-Schouten, to both of whom we would like to express our sincere thanks. Overall, the preparation and smooth execution of our Annual Meeting under difficult conditions was a great effort, which could only be successful thanks to the commitment of all members of the CODE office and the colleagues who contributed to it.

We also take this opportunity to express our heartfelt thanks to all supporters and cooperation partners, who all contribute to the Research Institute CODE achieving its full potential. Special thanks go to the Federal Minister of Defence Annegret Kramp-Karrenbauer, the Head of Department CIT Lieutenant General Vetter, the Inspector CIR Vice Admiral Dr. Daum, our direct contacts at the Federal Ministry of Defence as well as the management of UniBw M, whose support forms the basis of our activities.

We wish you an entertaining and interesting read and look forward to further cooperation!

Wolfgang Hommel

Prof. Dr. Gabi Dreo Rodosek *Prof. Dr. Wolfgang Hommel* *Volker Eiseler*
Management of the Research Institute CODE

Contents

FIG.: ISTOCK / ARCHY13

Highlights
From the Institute

Research
Portraits and Projects

Addendum
Publications and Activities

Cooperations and Partners

Categories

Highlights

From the Institute

FIG.: FORSCHUNGSZENTRUM JÜLICH / RALF-UWE LIMBACH

Quote from the Program of the German EU Council Presidency: “Europe must become digitally sovereign, in order to remain capable of acting on its own in the future”.

FIG.: ISTOCK / NICOELNINO

Report on the Annual CODE 2020 Conference

European Digital Sovereignty: Road to Success?

Prof. Dr. Gabi Dreo Rodosek, Volker Eiseler,
Dr. Nils gentschen Felde, Dr. Wolfgang Gehrke,
Prof. Dr. Udo Helmbrecht,
Prof. Dr. Wolfgang Hommel, Julius Zahn

The annual CODE 2020 conference, which took place from November 10 to 12, focused on the German EU Council Presidency and was held under the motto “Europe’s Digital Sovereignty — Road to Success?”. Against the background of the COVID 19 pandemic, the conference was held completely virtual for the first time. The Research Institute CODE welcomed over 540 virtually participating guests.

Europe: Digitally Sovereign or Digital Colony?

All future globally dominant products and services will be located in the digital world, in cyberspace, or at least interact strongly with it. Examples include robotics, industrial automation, autonomous driving, intelligent power grids, smart cities and smart homes. The world is becoming “smarter” and IT is the basis of our digital society. Digital technologies such as Big Data, Artificial Intelligence, autonomous systems and cyber-physical systems generate and process the huge amounts of data generated in the process. Today, Europe stands for a high level of data security and data protection, and the EU is probably the most trusted region in the world when it comes to these issues. Economically, this can be seen as a significant competitive advantage that must be maintained and expanded. But how digitally sovereign is Europe? What is the European path to digital sovereignty? These questions must also be considered in the context of data security and data protection.

The discussions and contributions at the annual conference of the Research Institute CODE (RI CODE) of the Universität der Bundeswehr München (UniBw M), CODE 2020, which was held as a digital conference from November 10 to 12, 2020, highlighted different aspects of this topic.

The first day of CODE 2020 with high-level discussion panels was a contribution by the Federal Ministry of Defence (BMVg) to the German EU Council Presidency. Quote from the program of the German EU Presidency[1]: “Europe must become digitally sovereign to remain capable of acting on its own in the future.” But what is the European way?

Today, data and digital services are dominated almost exclusively by U.S. and, increasingly, Chinese global companies. If security authorities in Europe become increasingly dependent on the products and services of non-European players to fulfill their missions, it will threaten the state’s ability to act in the future, and not just in the event of a crisis.

In an increasingly globalized world, Europe presents itself as a pioneer of ethical values; however, this cannot guarantee the digital sovereignty of its citizens or its companies. Current challenges in the areas of climate protection and health, especially regarding the COVID-19 pandemic, can also only be solved with the help of trustworthy IT. There is no alternative to digitization. A strategic focus on maintaining and building essential capabilities for the ability of the state and its institutions to act is important to ensure the protection and security of all its citizens in the future. This does not necessarily mean the need for self-sufficiency in all areas of society. However, it should be pushed more strongly in those areas that pose high risks to the state, society, and the economy. It is precisely in those areas where we have to or want to rely on others that our own competence is imperative in order to be able to check and regulate the use of these methods or goods.

1) Federal Foreign Office (2020): Together for Europe’s recovery. Programme for Germany’s Presidency of the Council of the European Union, 1 July to 31 December 2020, https://www.eu2020.de/blob/2362036/e0312c50f910931819ab67f630d15b2f/07-02-pdf-programm-en-data.pdf

eu2020.de
CODE 2020"
RI CODE Research Institute Cyber Defence Bundeswehr University Munich
A leading European Research Institute for Cyber Security, boosting technology and innovation for the digital society.
Connecting experts in a Cyber Cluster - an ecosystem for politics, research, industry, military and public authorities
Conferenc

Prof. Dr. Gabi Dreo Rodosek, Executive Director of RI CODE, and Prof. Dr. Merith Niehuss, President of the UniBw M.

Key Technologies and Strategic Perspectives of Digitization

Lieutenant General Michael Vetter, Head of Cyber/Information Technology (CIT) and Chief Information Officer at the German Federal Ministry of Defence, opened the conference and emphasized the importance of a strong Europe that can protect its citizens. The focus is on strengthening European resilience with a focus on digital sovereignty. Digital sovereignty and cybersecurity can only be successfully implemented through the cooperation of different actors, from research, industry, and public institutions to start-ups.

The President of the Universität der Bundeswehr München, Prof. Dr. Merith Niehuss, welcomed the more than 500 participants connected online and gave a brief overview of the current developments in RI CODE.

In her keynote speech, the German Federal Minister of Defence, Annegret Kramp-Karrenbauer, addressed various aspects of European digital sovereignty. Among other things, she emphasized the importance of cooperation, networking, and the establishment of digital ecosystems, explicitly mentioning the EU project CONCORDIA with currently more than 55 partners, coordinated by RI CODE, as an important program for the establishment of such a European digital ecosystem. Using trusted IT, minimizing dependencies on non-European IT, strengthening digital resilience, and establishing European technological leadership are just some of the aspects the federal minister emphasized in her keynote.

The Minister of Defence of the Netherlands, Ank Bijleveld-Schouten, stressed the importance of a strong and independent Europe. Furthermore, the minister highlighted the close cooperation of the German and Dutch armed forces in the digital world.

In the discussion with the ministers, Prof. Dr. h. c. Wolfgang Ischinger, Chairman of the Munich Security Conference, addressed ways to strengthen European digital sovereignty and, in particular, highlighted the relevance of mutual trust using the example of the Charter of Trust initiative.

Cybersecurity as a prerequisite for digital sovereignty was the focus of the second panel, moderated by Prof. Dr. Manfred Broy from the Technical University of Munich. Here, Juhan Lepassaar, Executive Director of ENISA, Vice Admiral Dr. Thomas Daum, Inspector CIR, Ralf Wintergerst, CEO of Giesecke+Devrient, Dr. Annegret Bendiek of Stiftung Wissenschaft und Politik and Jeremy Jurgens of the World Economic Forum discussed the challenges of cybersecurity from different perspectives such as building a European data space, privacy, digital identities and data protection.

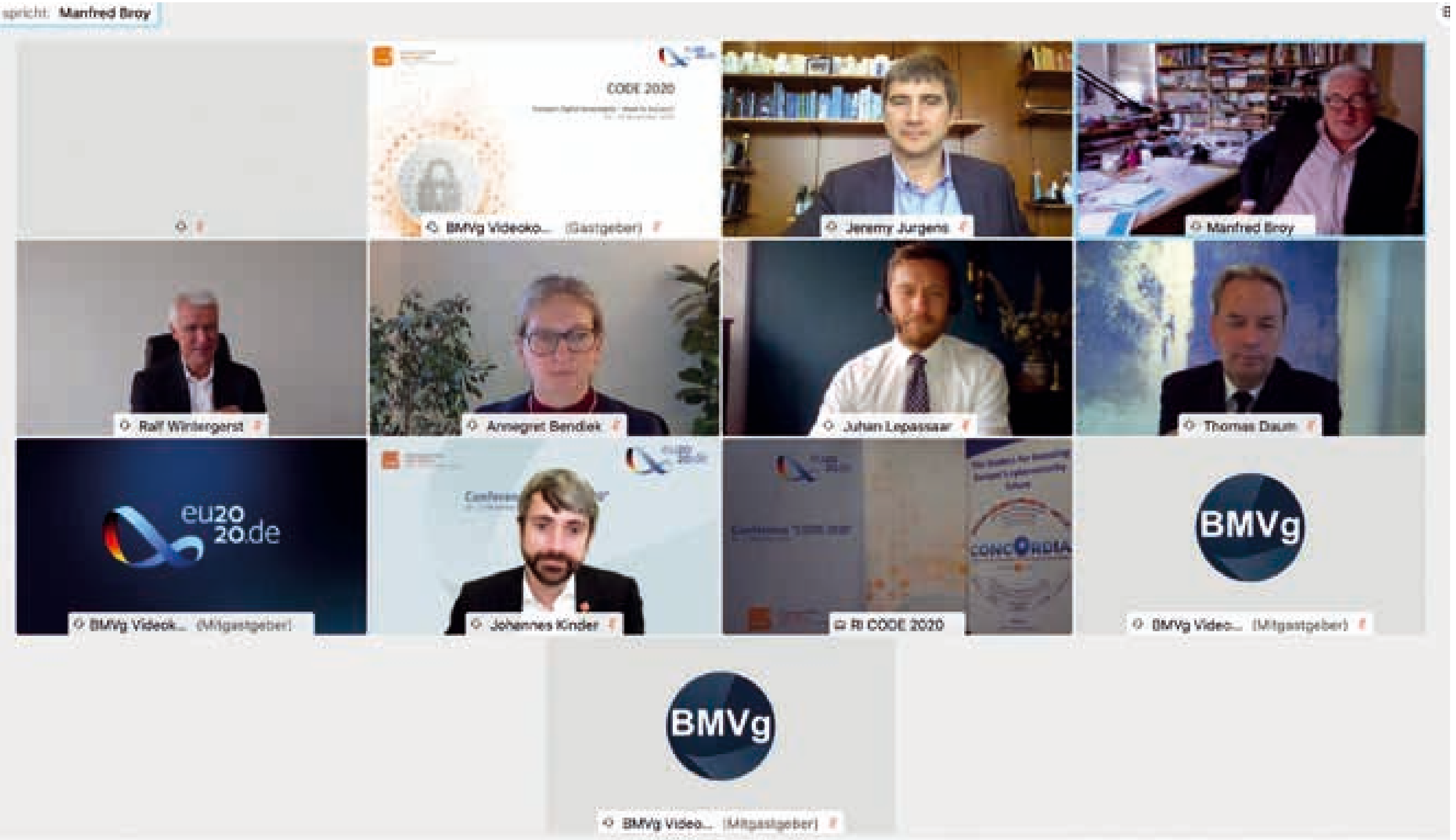
The first day of CODE 2020 ended with a panel discussion on future key technologies as the basis of digital sovereignty, moderated by Prof. Dr. Gabi Dreo Rodosek, Executive Director of RI CODE. Benedikt Zimmer, State Secretary of the German Ministry of Defence, emphasized how important the availability of trustworthy IT is for the armed forces' ability to act. Dr. Angelika Niebler, Member of the European Parliament, and Jiří Šedivý, Chief Executive of the European Defence Agency, presented their views regarding the development and promotion of European key technologies. Stefan Winners, consultant at Lakestar, a European venture capital company, explained his view on investments in key technologies and the main obstacles that lead to the fact that Europe does not have major IT champions. The final question to all discussants was, "What is the path, the roadmap, to build a digitally sovereign Europe?" — "Cooperation, collaboration and trust" was the unanimous answer.

Pioneering Digital Sovereignty

On the second day of CODE 2020, seven parallel workshops took place, which enabled an intensive, in-depth exchange between the experts on current topics. The various topics that were presented and discussed in depth in the expert workshops illustrate the numerous challenges that need to be overcome on the way to European digital sovereignty. A total of almost 300 participants from Europe took part in the virtual workshops — a new record. The highlights of two of the 2020 workshops are summarized hereafter.

BOTH FIG.: UNIBW M

In her keynote speech, German Defence Minister Annegret Kramp-Karrenbauer adressed various aspects of European Digital Sovereignty.



Cybersecurity as a prerequisite for digital sovereignty was the focus of the second panel of CODE 2020.

Cyber Resilience of Critical Infrastructures Workshop

The workshop addressed the resilience of critical infrastructures in the systemic interconnection of complex cyber-physical systems. A special focus was on the economic sector and on different company approaches to deal with new cyber security threat scenarios. The impact of attacks on institutions relevant to state security, in particular the Bundeswehr, was also discussed. Artificial intelligence in the area of the Internet of Things was mentioned as a possibility for improving cyber resilience, here in particular through prediction.

Participants estimated that the greatest challenges in the area of cyber resilience are:

a) sharing best practices with relevant stakeholders,
b) enabling the secure and rapid exchange of data.

Quantum Technology Workshop

The focus of this workshop was on quantum computing and post-quantum cryptography (PQC). On the one hand, quantum computing and the hardware used for it are a direct result of the application of quantum mechanical effects. On the other hand, PQC is an improvement of previous classical cryptographic methods, which now have to withstand potential attacks by quantum computers. The theory of quantum circuits forms the basis for understanding currently available hardware.

The algorithms of Lov Grover and Peter Shor from the 1990s still are the best examples of the effectiveness of a quantum approach. Both methods put both symmetric and asymmetric cryptography at risk, with the latter being more affected in the form of ECC[2] and RSA[3]. That is why a NIST[4] process is underway to standardize new methods to improve current digital signatures, key exchange protocols, and public key cryptography.

IBM recently laid out an ambitious roadmap for devices with more than 1,000 qubits by 2023. This milestone could finally open the door to better error handling and correction. Therefore, PQC will probably have to be applied sooner rather than later.

2) Elliptic Curve Cryptography
3) Asymmetric encryption algorithm
4) National Institute of Standards and Technology, USA

Innovation as a Requirement for Digital Sovereignty

The afternoon of the second day of CODE 2020 was dedicated to the innovation conference on the topic of cyber and information technology. Following its launch in 2018, it was held for the third time. Bernd Schlömer from BMVg Department CIT I 2, which is responsible for research and technology as well as innovation management in cyber/IT, explained, in his role as chairman of the jury, the objective of identifying technical innovations relevant for the Bundeswehr from academic and industrial research and development in a competitive process, and of networking innovators and users with each other.

From more than 30 submissions to the Innovation Conference, the organizational team selected twelve for presentation pitches, i.e. short presentations limited to a maximum duration of seven minutes. Based on these pitches and the ensuing discussions, the best three of the twelve contributions, all of which demonstrated their relevance, were selected.

Despite the individuality of each contribution, it was clear that the main focus of the innovations presented in 2020 was on the use of machine learning — for identifying fake news and supporting decisionmaking, among other things — the finely granulated segmentation of data networks for placing technical security measures, and the evaluation of data freely accessible on the Internet in the sense of Open Source Intelligence.

Tobias Appel from the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities was awarded third place for his contribution to automated success testing in the use of exploits as part of penetration tests of the company's own IT infrastructure. Second place went to Michael Grytz of HENSOLDT Sensors GmbH for presenting I-unHYDE, an AI-based tool for detecting and analyzing disinformation campaigns. First place went to Ingmar Heinrich and Ulf Schröter of Rheinmetall Electronics GmbH, who presented an approach for moving target defense in micro-segmented zero-trust networks. All participants were given the opportunity to present their innovations in more detail to selected target groups after the conference.

Digital Sovereignty Requires Digital Skills

In 2020, the Science Track was held for the first time as part of the CODE annual conference, providing young PhD students with a forum for scientific exchange and networking. The event was divided into two parts, the Early Stage PhD Forum and the Last Stage PhD Forum. The first part of the program provided a platform for prospective PhD students to present their PhD projects at an early stage, while the second part of the program allowed for an exchange of experiences between more advanced PhD students and their younger counterparts.

The Logo of the German EU Presidency.

FIG.: UNIBW M; EU

A total of seven speakers were selected during a scientific review process. Thematically, the program offered a variety of content from the field of IT security and ranged from very technical lectures on the level of machine instructions to semantic analyses of social networks or aspects of visualization in the context of education.

Prof. Dr. Aiko Pras from the University of Twente, Prof. Dr. Gabi Dreo Rodosek and Prof. Dr. Florian Alt from RI CODE provided scientific support for the discussion. The event was very popular right from the start and, despite the purely virtual form of presentation, achieved a good initial success with more than 80 listeners. In 2021, the Science Track of the CODE Annual Conference will again contribute to building the scientific community and supporting young scientists on their career paths. ■

More Information:

🌐 www.unibw.de/code/events/jahrestagungen

🌐 www.eu2020.de

🌐 www.youtube.com/c/FZcodeDeubw

Quantum Technologies

Get Quantum ready

Prof. Dr. Udo Helmbrecht, Dr. Sabine Tornow,
Dr. Wolfgang Gehrke, Volker Eiseler

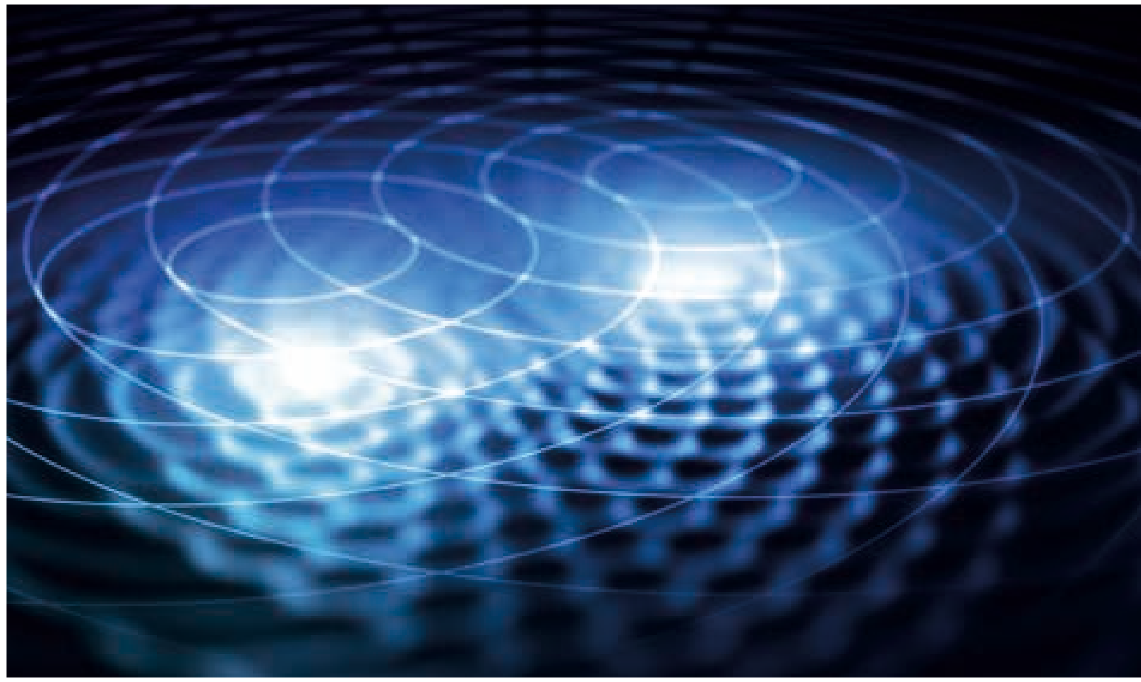
Quantum technologies form the basis for modern technologies such as microchips, broadband internet, or satellite navigation. Effects such as quantum interference or quantum entanglement are now technologically usable and provide the potential for completely new technical solutions such as quantum computers, quantum sensors, quantum cryptography and communication as well as quantum simulation. At the Research Institute CODE, we conduct research in the fields of quantum computing and quantum communication. Post-quantum cryptography is also one specific topic we are looking into at the RI CODE in order to develop new methods to protect data and communications from threats posed by quantum computers.

Quantum Computing

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, or modeling of complex systems. These problems are intractable to any current or future conventional computer.

It has been shown in theoretical work that – compared to the best-known classical algorithms – certain structured problems can be computed exponentially faster with quantum algorithms. The arithmetic operations are performed with qubits. A qubit is the smallest unit of information in a quantum computer: it is a quantum

This page: The origin of quantum speed up is that quantum computers allow interference between computational paths.



Left: IBM Q at the Consumer Electronics Show 2020. The IBM Q Network has grown to include more than 100 organizations.

FIG.: IBM / ANDREW LINDEMANN; ISTOCK / PETROVICH9

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, the qubit does enter one of the two states (0, 1). The measurement result can then be stored in a classical bit.

Heuristic algorithms, which have been empirically shown to be effective, are now used for many practical computational problems. Analogously, heuristic quantum algorithms have also been proposed. Empirical testing, however, will not be possible before the appropriate quantum hardware is available. With recent remarkable technological advances in quantum computers, we now have the opportunity to test quantum algorithms and quantum heuristics on small devices.

While quantum hardware is constantly improving, it is still error- and noise-prone. Interaction with the environment or noise disturbs the superposition states. This leads to the loss of the interference effects.

An important goal is to maximize the time for which the superposition state is maintained, if possible, and thus minimize the error rates. If these are below a certain threshold, not only can longer quantum calculations be performed, but with the help of error correction even arbitrarily long calculations can be carried out with arbitrarily good accuracy.

Currently, error correction is still difficult to implement due to hardware requirements – but error mitigation to improve the signal-to-noise ratio is possible.

Central to further research and development, in addition to hardware improvement, is hardware-based programming with error mitigation techniques, development of new heuristics for optimization applications, and modeling and simulation of complex systems on quantum computers.

The Famous Double Slit Experiment.

IBM Q Hub at RI CODE

For several years, the Research Institute CODE has been working scientifically on applications that can be implemented with universal quantum computers. In addition, military situation awareness and scenario analyses will be use cases in future research in the field of quantum computing at RI CODE.

According to the Planning Instruction 2022 from the German Ministry of Defence, the areas of quantum technology, digitalization and innovation capability are key aspects for the implementation of a future-oriented personnel management. The military use of quantum technology is to be ensured, among other things, by the RI CODE combined with the medium-term procurement of a quantum computer and the administration of a quantum computing hub at CODE.

In 2018 the Research Institute CODE at the Universität der Bundeswehr München became one of 16 global IBM Q Hubs with exclusive access to the IBM quantum computer infrastructure. The current availability of small, noisy quantum computers (20–65 qubits) allows us to test quantum algorithms and heuristics, as well as error mitigation schemes.

In addition to machine learning, many-body physics and optimization with hybrid variational algorithms are the most promising initial applications. In the future, more quantum heuristics will be developed and tested in the framework of potential use cases. In addition, a collection of error mitigation methods will be developed for general availability.

The RI CODE also organizes Quantum Computing Hackathons for students from the Universität der Bundeswehr München, TUM and LMU Munich.

Contact Information IBM Q Hub:

Volker Eiseler
volker.eiseler@unibw.de
+49 89 6004 7304

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

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

FIG.: ISTOCK; IBM / ANDREW LINDEMANN

IBM Q Computation Center.

Quantum Communication

Secure communication via the internet is an essential requirement for trusted cooperation in all areas of our society. Applications, data, messages, telephone calls or e-mails must be protected from access by unauthorized third parties. Powerful, universal quantum computers, which are already available as initial test devices, would render virtually all public-key encryption and key exchange methods used today insecure. To be prepared in terms of appropriate risk management, preparations for the "post-quantum era" must begin today. Confidential services with a long-term need for protection, such as the exchange of personal messages, video conferencing or online banking, and digital signatures and certificates with long expiry dates are all affected. In order to maintain state sovereignty, sensitive and in some cases classified military communications must be specially secured.

Quantum key distribution (QKD) is a method that uses the physical properties of quantum mechanics to provide two or more parties with a common, secure key for communication. The advantage of quantum key exchange over classical key distribution methods is that the security it achieves is based on known physical laws, rather than assumptions about the performance of computers and algorithms or the reliability of trusted parties. The security of the various methods of quantum key exchange arises from the fact that an attacker who eavesdrops on the key transmission is noticed, and even the amount of information they tap can be measured.

For research and experimental proof of usable quantum key distribution, the research project MuQuaNet (The greater **Mu**nich area **Qua**ntum Inter**Net**), funded by the Digitalization and Technology Research Center of the Bundeswehr (dtec.bw), was set up with a duration of four years. Within the framework of MuQuaNet, a quantum communication infrastructure is being established in the greater Munich area. Researchers are implementing selected security-critical civil and military use cases and testing them for confidentiality, integrity, availability, and cost-effectiveness against attacks from quantum computers.

In addition to the development and integration of optical QKD components for fiber and outdoor links, a scalable quantum key distribution management system is the focus of the project. Furthermore, security analyses from the applications via the middleware to the QKD terminals are an essential part of the research project. ■

Contact Information
dtec.bw Research Project MuQuaNet:

Prof. Dr. Udo Helmbrecht
@ udo.helmbrecht@unibw.de
☎ +49 89 6004 7308

ICE&T Cyber Range Training Room at RI CODE.

The Cyber Range at Research Institute CODE

ICE&T – IT Competence Education & Training

The ICE&T (IT Competence Education & Training) Cyber Range is Research Institute CODE's central laboratory for realistic cybersecurity training and the evaluation of novel cybersecurity-products and approaches. It offers a platform for learning and deepening of Cyber Network Operations competences with a strong focus on teamwork.

Overview

ICE&T is a comprehensive and flexible Cyber-Training solution. Today it contains complex Cyber Incident and Response Management (CIRM) scenarios at three different difficulty levels. Furthermore, scenarios are implemented that address offensive security and Supervisory Control and Data Acquisition (SCADA). The content is complemented with a variety of self-learning modules and more than 80 individual exercises from nine different cybersecurity domains.

Architecture and Setup

Scenarios are played out on predefined virtualized network topologies. A learning-management system (LMS) and a software backend that allows training control and evaluation support the training. Teamwork is promoted by a sensible layout of training rooms and additional equipment, that allows collaboration and documentation. The modular architecture facilitates the design and implementation of new scenarios from different cybersecurity domains. Furthermore, it enables an integration of novel network topologies, hardware components or software solutions. This makes ICE&T subject to continuous extension and evolution and is the basis for evaluation of novel cybersecurity solutions and approaches.

Purpose and Aim of Training

Different training scopes and modalities allow a fine adjustment of the goals to be reached within a training session. A basic training for example, aims for teamwork-driven coping with cybersecurity incidents.

The collective analysis of compromised systems helps the understanding of attackers' intentions, tactics and procedures. It creates awareness and exemplifies possibilities for successful mitigation.

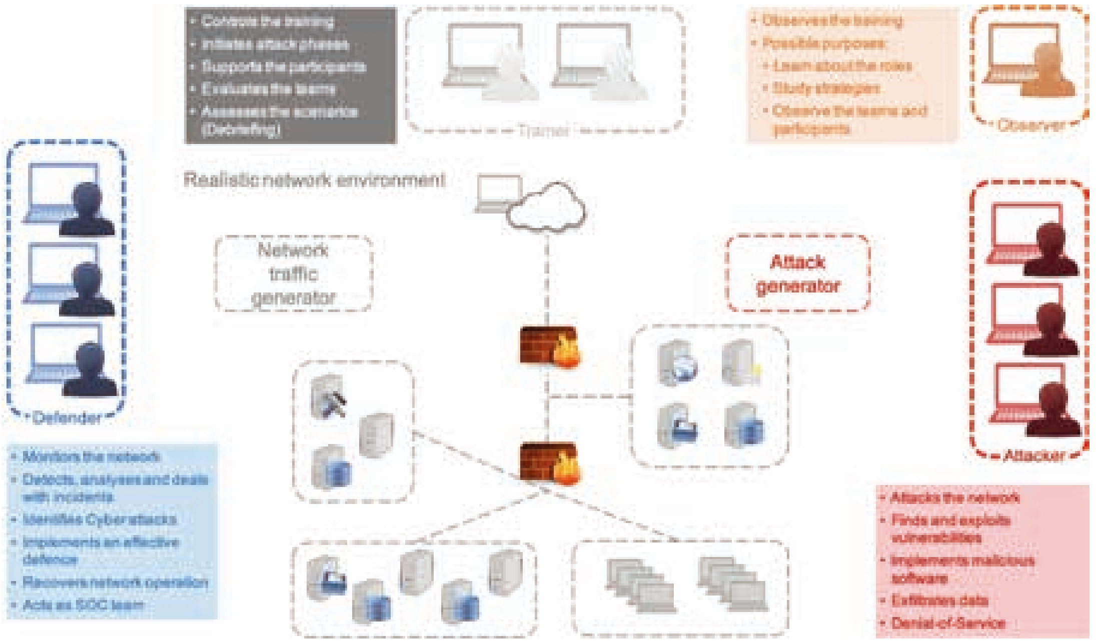
Advanced training aims to evolve existing competences and to increase efficiency of teamwork, processes and mitigation measures. More complex attack mechanisms have to be detected and analyzed, with a focus on enhancing teams' coordination and the creation of comprehensible documentation of incidents and countermeasures. Furthermore, design and implementation of customized training is possible, to cover more individual applications or to integrate customer's network topologies.

COMPETENCE EDUCATION & TRAINING
ICE&T
RI
CODE
Research Institute
Cyber Defence
Universität der Bundeswehr München

Brand Logo of the ICE&T Cyber Range at RI CODE.

Current Work

To ensure a realistic training experience in an up-to-date environment, the continuous evolution of existing scenarios and the development of new content is a crucial part of ongoing activities in the ICE&T Cyber Range. In this context, an expansion into further cybersecurity domains, namely IoT, 5G and SCADA is planned. Moreover, the system is part of a variety of RI CODE's research projects.


Controls the training
Initiates attack phases
Supports the participants
Evaluates the teams
Assesses the scenarios (Debriefing)
Trainer
Observes the training
Possible purposes:
Learn about the roles
Study strategies
Observe the teams and participants
Observer
Realistic network environment
Network traffic generator
Attack generator
Defender
Monitors the network
Detects, analyses and deals with incidents
Identifies Cyberattacks
Implements an effective defence
Recovers network operation
Acts as SOC team
Attacker
Attacks the network
Finds and exploits vulnerabilities
Implements malicious software
Exfiltrates data
Denial-of-Service

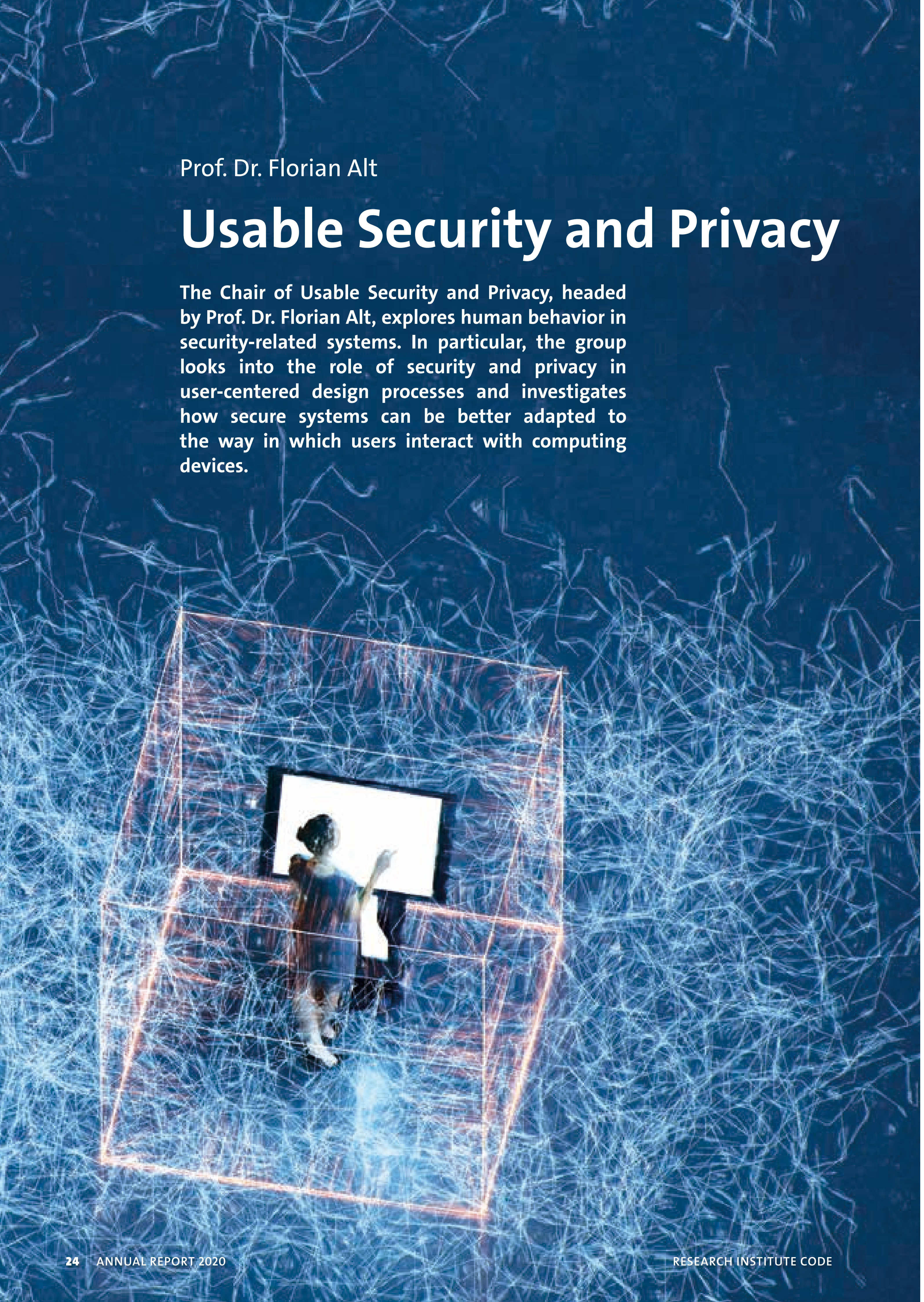
Roles and functions of the ICE&T Cyber Range at RI CODE.

BOTH FIG.: RI CODE

Research

Portraits and Projects

FIG.: SHUTTERSTOCK / EFMAN



Prof. Dr. Florian Alt

Usable Security and Privacy

The Chair of 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 Chair of Usable Security and Privacy was founded in 2018 and conducts research at the crossroads of Human-Computer Interaction and 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 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.

The group focuses on a variety of different research topics including, but not limited to, security and privacy mechanisms based on human behavior, leveraging users' physiological state to both enhance existing security approaches as well as to build novel security concepts, understanding and investigating threats that emerge from ubiquitous computing technologies, and the explainability of security and privacy. Specific application areas are smart homes, social engineering, behavioral biometrics, and mixed reality.

In the context of their research, the group employs and enhances research methods commonly known from human-computer interaction. These include, but are not limited to, user-centered design and iterative prototyping. The work is strongly centered around humans, making empirical approaches a fundamental part of the group's research. To understand behavior as well as to evaluate novel approaches, studies are conducted in the lab as well as in the field.

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

Together with his team, Prof. Dr. Florian Alt has published over 200 DBLP-listed scientific articles and won more than 10 awards in leading scientific venues of his field. The group's research received funding from the DFG, the Bavarian State Ministry of Education and Cultural Affairs, Science and the Arts, the Humboldt Foundation, the DAAD, Google, and the BMW Group.

Prof. Dr. Florian Alt

@ florian.alt@unibw.de

☎ +49 89 6004 7320

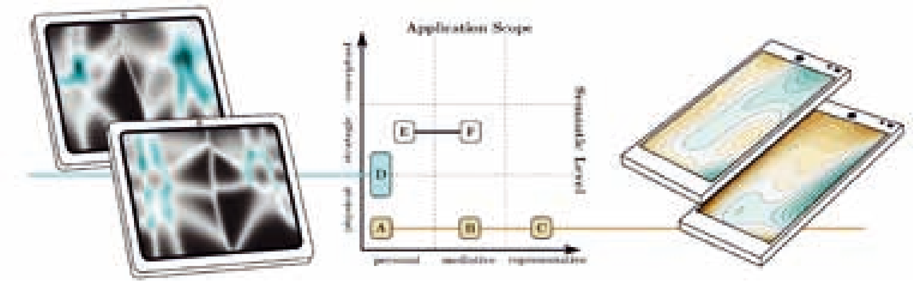
https://go.unibw.de/usec

Team of the Chair of Usable Security and Privacy.

FIG.: ISTOCK / GREMLIN; FLORIAN ALT

Project ubihave

The ubihave project investigates how ubiquitous computing devices can benefit from behavioral models. This research is motivated by computers permeating our life, as everyday companions and as sensors embedded in the environment. These devices provide rich streams of user-specific data, opening new avenues for applications using behavioral models, which appropriately adapt to individual users and contexts.



The ubihave project investigates how concepts based on behavioural biometrics can be realised for pervasive computing environments.

Sensors Provide Rich Behavioral Data

Computers are ubiquitous: as everyday companions (smartphones, tablets, wearables) or as sensors in embedded systems (NFC, (depth) cameras, eye trackers). These devices provide rich user-specific data opening new avenues for applications based on behavioral models. One example is the possibility of realizing the vision of intelligent user interfaces, smart devices and responsive environments.

Behavioral Biometrics as a Promising Alternative

Many current UIs and devices can react to simple sensor properties. However, interfaces and interactions are rarely adapted to the individual user and context since this requires dedicated inference tools to process uncertain user-specific sensor data. To render user-specific information more accessible and useful to applications and users, this project aims to build and apply models that can describe, analyze, and predict user behavior based on data from mobile devices and ubiquitous sensors. Particular application areas that we expect to strongly benefit from such models are usable privacy and security, touch interaction, text input, and context-aware adaptive interfaces.

Research Questions

This project integrates HCI and user modeling perspectives to address a number of guiding questions: in which applications and contexts can users benefit from behavioral models? How can models improve interactions? Do users notice and like adaptations and do they match their expectations to capture and utilize user behavior? How do we define performance metrics for user actions with behavior-aware interfaces? Which interactions provoke characteristic and consistent behavior?

Impact

The contribution of the project is threefold. Firstly, we chart a holistic design space to understand and investigate user modeling comprehensively across tasks and beyond the desktop. This reveals future opportunities and a goal unique to this project: we aim to identify common grounds for diverse applications based on the same user representation, leading to efficient data handling across applications. Secondly, we use deployment-based research to identify scenarios in which behavioral biometrics help to optimize, personalize, and secure interactions. Examples include novel usable security mechanisms, efficient and usable mobile text entry, activity-aware applications, and novel mobile services that can adapt to user behavior. Thirdly, to allow applications to consider user-specific interaction characteristics and behavior, this project also develops inference tools, which can process uncertain sensor data with respect to the targeted user contexts and goals.

Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

go.unibw.de/usec

Funded by:
German Research Foundation (DFG)

FIG.: DANIEL BUSCHEK; STEFAN SCHNEEGASS

Project Scalable Biometrics

In this project, we examine how pervasive computing environments can leverage behavioral biometrics for identifying and authenticating users. The main challenge this project is addressing is the question how behavioral biometrics approaches scale to environments containing multiple users with changing behaviors, different physicalities, and changing sensing and interaction capabilities.

The Problem with Traditional Authentication

Knowledge-based authentication mechanisms that require users to remember login and password are among the most popular means for authentication, despite the fact that they were never designed for today's requirements. For example password-based authentication originates in the mainframe era around 1960 where users would log onto a single device a few times a day at most. Today authentication happens much more frequently as well as in almost any situation and context. As a result, authentication creates a significant overhead (using state-of-the-art authentication mechanisms, people spend on average 90 minutes per month authenticating), which ultimately leads to many users using weak (but therefore faster) means to protect sensitive data, or no protection at all.

Behavioral Biometrics as a Promising Alternative

In recent years, behavioral biometrics, that is the ability to identify users implicitly from their behavior, received considerable attention in the research community. This approach does not require users to remember a secret but authentication can seamlessly slide into the background without the need for active user engagement. Suitable behavioral traits to identify users include, but are not limited to, users' gait, typing behavior, touch targeting behavior, gaze behavior, and mouse movements. At the same time, behavioral biometrics so far was mainly investigated in the lab for a single user at a time, since assessing different features requires precise measurements in controlled environments. Thus it remains unclear how these approaches scale to the novel challenges of pervasive computing environments.

Research Questions

In this project we address this new field by answering questions like how users' behavior is influenced both by people in the vicinity, characteristics of a space (either public or private), as well as by novel interaction techniques, how this influences the way in which we design and develop behavioral biometrics systems, and what this means for behavioral biometrics-based authentication concepts (e. g., how can we build user interfaces that foster a certain behavior; how can appropriate behavioral traits be identified based on the current context).

The scalable biometrics project investigates how concepts based on behavioral biometrics can be realized for pervasive computing environments.

Impact

We envision this project as enabling a significant leap forward towards behavioral biometrics becoming a powerful means for identification and authentication in future pervasive computing environments that combine high usability with strong security. Furthermore the outcomes of this project are valuable beyond security, e. g. the adaption of interfaces for individual users based on features like their body physique or current pose.

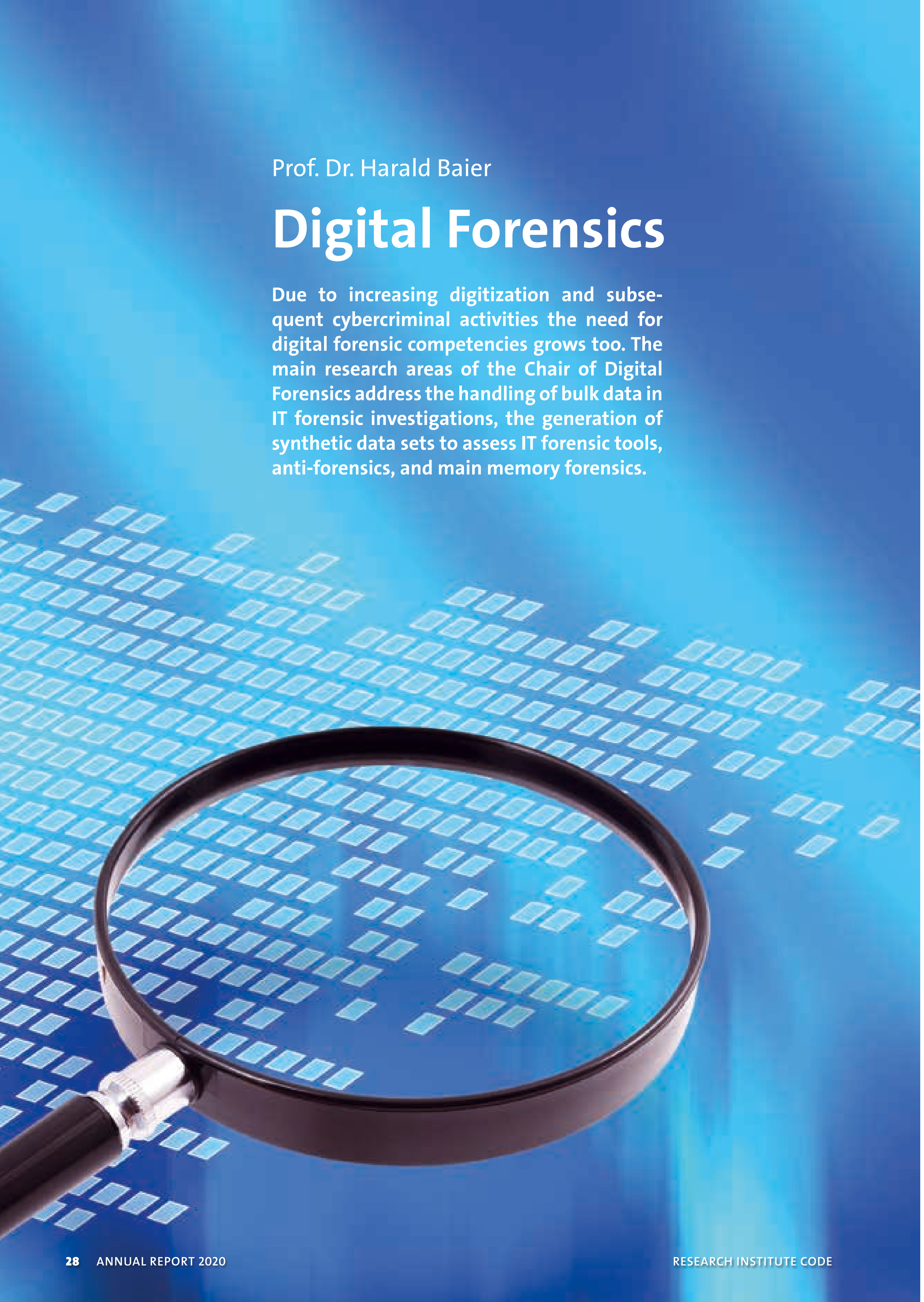
Prof. Dr. Florian Alt

florian.alt@unibw.de

+49 89 6004 7320

go.unibw.de/scalablebiometrics

Funded by:
German Research Foundation (DFG)



Prof. Dr. Harald Baier

Digital Forensics

Due to increasing digitization and subsequent cybercriminal activities the need for digital forensic competencies grows too. The main research areas of the Chair 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.

As the digital equivalent of the classic forensic disciplines, digital forensics always comes into play when an attack on an IT system is suspected. Imagine the following exemplary scenario: you come into the office on a Monday morning after a relaxing weekend and find a number of electronic messages in your e-mail inbox. Structured as you are, you first turn your attention to the obviously important e-mails. One message, presumably from your boss, immediately catches your eye. He wants to explain to you once again the updated planning for an important project in an attached Office document and asks you to take a close look at it and make comments. So you open the Office document attached to the email, but all you get is an error message. Actually nothing exciting, the computer often does what it wants. After a few minutes, your computer's fan starts up because the processor apparently has to process a lot of commands. Unfortunately, a program just encrypts all your stored data and then shows you a message on the screen: either you pay blackmail and then you can decrypt your data again, or the computer's data remains encrypted forever.

An IT forensic investigation is associated with numerous challenges, which the Chair of Digital Forensics deals with. A first important challenge is the sheer flood of data during an IT forensic investigation. Numerous storage media 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 the haystack.

A further important challenge is the accuracy of IT forensic tools, i. e., they should work exactly how they are supposed to. Standardized test data sets are needed for this, where the digital traces to be detected are known *a priori* and are matched against the detected traces by the respective tool.

A third important challenge is dealing with anti-forensics, i. e., all efforts by the attacker to cover up or destroy his traces. Anti-forensics has 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 the anti-forensic methods used by attackers.

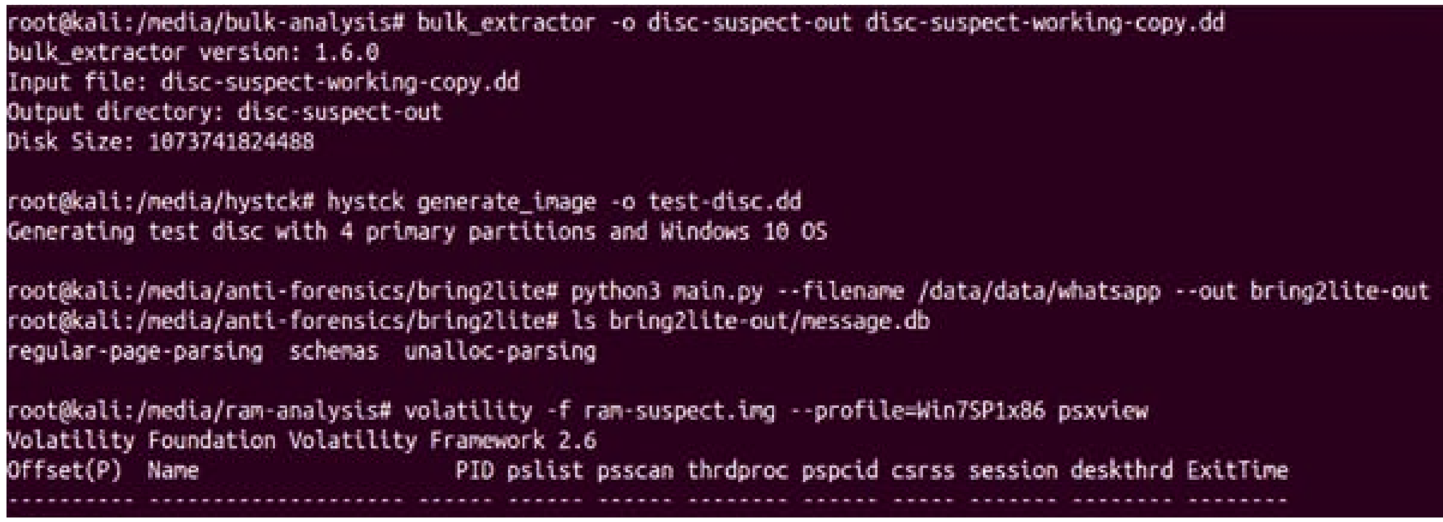
And finally, malware hides itself so well that it can only be found and analyzed on the "live" system — i. e., the main memory or its image. For this purpose, suitable methods of post-mortem storage media forensics must be transferred to main memory forensics.

Prof. Dr. Harald Baier

@ harald.baier@unibw.de

☎ +49 89 6004 7345

www.unibw.de/digfor



```
root@kali:/media/bulk-analysis# bulk_extractor -o disc-suspect-out disc-suspect-working-copy.dd
bulk_extractor version: 1.6.0
Input file: disc-suspect-working-copy.dd
Output directory: disc-suspect-out
Disk Size: 1073741824488

root@kali:/media/hystck# hystck generate_image -o test-disc.dd
Generating test disc with 4 primary partitions and Windows 10 OS

root@kali:/media/anti-forensics/bring2lite# python3 main.py --filename /data/data/whatsapp --out bring2lite-out
root@kali:/media/anti-forensics/bring2lite# ls bring2lite-out/message.db
regular-page-parsing  schemas  unalloc-parsing

root@kali:/media/ram-analysis# volatility -f ram-suspect.img --profile=Win7SP1x86 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
```

Key aspects of the Chair of Digital Forensics are the handling of bulk data, the generation of synthetic data sets, anti-forensics, and advanced methods for RAM analysis.

FIG.: ISTOCK / DEMIO; HARALD BAIER

"children": [
{
"uuid": "05B57416-1BE5-4A96-
"type": "Mesh",
"name": "Ground",
"matrix": [1,0,0,0,0,0.000796,-1,
"geometry": "E80D9EC5-D722-4812-8226
"material": "3A94490Z-62D8-4884-

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

The research group headed by Stefan Brunthaler focuses on language-based security, an area that investigates the use and applicability of language-based transformations to secure vast amounts of software in a way that is automated, transparent, and effective.

FIG.: iSTOCK / DEM10

The Munich Computer Systems Research Laboratory directed by the Chair of Secure Software Engineering conducts world-class research in defensive computer security by conceiving novel defenses that mitigate advanced, sophisticated, and current cyber-attacks. This class of attacks includes, among others, transient execution attacks (such as Spectre and Meltdown), Rowhammer, side channels, code injection and code reuse attacks (exemplified by return-oriented programming). From a strategic perspective, these tactical attack vectors are of utmost importance, since a clear and present danger emanates from these attacks, which are often used in a combined, multi-stage fashion. Such a combination is particularly relevant, as it enables supply-chain attacks that form bridgeheads for advanced-persistent threats (APTs).

µCSRL's research focuses primarily on transformative novel and groundbreaking research in software diversity. In 2020, we report two major milestones in this research area. First, we pioneered a new defense, called Decoy Return Addresses, that breaks two major attacks: Speculative Probing and Address Oblivious Code Reuse (AOCR). Our defense breaks the new Speculative Probing attack (published in August of 2020) by using so-called "speculation aware booby traps". Decoy Return Addresses breaks the AOCR attack by invalidating core attacker assumptions on stack frame layout and information leaks through indirect code pointers, exemplified by return addresses. Second, our research in formalization and verification of software systems laid the foundation for upcoming research in verifying the correctness of diversification transformations. At present, the successful principles of software diversity cannot be used in high-assurance and high-availability contexts, since there is no proof that the applied random experiments do not break some software properties. To account for this downside, we formalize and mechanically verify that the applied diversifying transformations preserve program semantics, thereby enabling the beneficial use of diversity in safety-critical contexts.

Along with the growth of µCSRL, we plant to extend our research agenda to include groundbreaking research in the following areas:

(i) automatic vulnerability analysis by fuzzing;
(ii) energy- & space-efficient datacenter architectures; and
(iii) 21st century systems software.

Our objectives in the first new research direction "fuzzing" will receive extensive support through our own new cluster infrastructure and through extensive cooperation with Prof. Dr. Kinder. By strategic cooperation and collaboration with leading European researchers, we intend to become the leading European research institution in the domain of fuzzing. This expertise will, furthermore, be of major importance for the Bundeswehr, as it will drive automatic vulnerability analysis and detection in new gear and thus be vital to detect supply-chain attacks as soon as possible. Our key objective in the second new research direction "datacenter architecture" is to enable Germany to close the knowledge gap required to build and operate leading datacenters, an area where the US and China are, at present, the undisputed leaders. Without this new capability it will be impossible for Germany to counter moves by these two superpowers, either in the military or in the industrial domain. Our objectives in the third new research direction "21st century systems software" focuses on the needed foundational research to supply Germany and its European parents with essential systems software, such as compilers and browsers.

The common thread among these new research areas is that they are indispensable prerequisites for European and German digital sovereignty. By way of the original, ambitious and highly competitive research plans, we hope to establish Research Institute CODE as the internationally leading research institution.

Prof. Dr. Stefan Brunthaler

@ brunthaler@unibw.de

☎ +49 89 6004 7330

www.unibw.de/ucsrl

Project µRAD

Return Address Decoys + Speculation-Aware Booby Traps

Software diversity is a potent defense against advanced, sophisticated attack vectors, such as code-reuse techniques (e. g., just-in-time return-oriented programming). Its most potent variant — leakage-resilient software diversity — suffers from two attacks: address-oblivious code reuse and the recently discovered BlindSide attack. µRAD overcomes these obstacles and thereby re-establishes diversity's reign among software defenses.

Software Diversity

The idea of software diversity is to replicate the effect of biodiversity in software. At present, the software "ecosystem" is organized as a monoculture, where programs are identical across vast numbers of computers. What follows from this monoculture is a fundamental advantage leveraged by attackers, namely that a single attack affects all computers simultaneously. This direct effect from the monoculture gives attackers huge economies of scale. By changing the programs, we break this fundamental advantage favoring attackers over defenders.

Address-Oblivious Code Reuse

In 2017, researchers presented a new code-reuse attack, called Address-Oblivious Code Reuse (AOCR). In theory, the AOCR attack breaks even advanced leakage-resilient software diversification techniques, such as Readactor (coauthored by the chair Prof. Dr. Brunthaler). Based on their results, researchers conclude that AOCR presents an important roadblock to software diversity, which can only be overcome by focusing on integrity-based defenses instead.

BlindSide

In 2020, researchers from the leading systems security research group — VUsec from VU Amsterdam — presented a novel attack called BlindSide. BlindSide is an important upgrade from a prior attack, namely Blind-ROP, an attack that uses brute-force techniques to bypass defense-based software diversity. BlindSide extends Blind-ROP by using a speculation-based side channel that does not signal an alarm to the operating system when its brute-force approach fails. BlindSide thus allows for covert, stealth brute-force operation to identify functions belonging to a program. Using these discovered functions, BlindSide can break a pillar of leakage-resilient software diversification techniques: execute-only memory (XOM).

Return Address Decoys

µRAD pioneers an entirely new diversification technique that randomizes return addresses of function calls. This diversification technique breaks the predictability of return addresses required by the AOCR attack.

Speculation-Aware Booby Traps

To mitigate BlindSide-style attacks, µRAD breaks new ground by using speculation-aware booby traps. When compiling a program, cyber booby traps can be weaved into a program to provide an active defense against code-reuse attacks. These booby traps are, however, susceptible to a BlindSide attack, as they cannot distinguish speculative from non-speculative execution. µRAD presents new booby traps that are speculation-aware, allowing them to mislead a BlindSide attack. A subsequent offensive use of the misled attacker results in triggering the booby trap, thus aiding detection and response.

Broader Impact & Societal Merit

µRAD is not only the first known defense against the Blind-Side attack, thus putting the CODE research institute at the center stage of the international security community. It also provides important evidence contradicting the conclusion by prior work claiming that no diversity-based defense can overcome AOCR.

👤 Prof. Dr. Stefan Brunthaler

@ stefan.brunthaler@unibw.de

☎ +49 89 6004 7330

Funded by:
Federal Ministry of Defence (BMVg)

Project µFoCUS

Verified and Secure Execution of Dynamic Languages

µFoCUS formalizes and mechanically verifies the optimized interpretation of dynamic languages. Since just-in-time compilers are often riddled with complex and severe bugs, µFoCUS provides an excellent alternative with formal correctness guarantees.

The Prevalence of Dynamic Languages

Dynamic languages, such as Python and JavaScript have become ubiquitous. Dropbox, for example, uses Python to implement their client, and JavaScript has become the dominant language on the web. Dynamic languages are often associated with offering higher productivity than other languages, but suffer from unacceptable performance penalties.

Dangers Emanating from the Execution of Dynamic Languages

To address the performance penalties, dynamic languages use a so-called just-in-time compiler, that is a compiler that runs parallel to the program to generate optimized native machine code. It turns out, however, that writing a just-in-time compiler for such complicated languages as JavaScript is non-trivial and thus often riddled with complicated but severe bugs. Google's Project Zero information security research group has authored a three-part blog post series detailing exploits to their own JavaScript JIT compiler (V8). The underlying problem of the status quo is that just-in-time compiler architecture predates insights derived from modern cyber security research. Many of the vulnerabilities and exploits documented by researchers pinpoint that the crux of the matter is the native-machine code is emitted by the JIT compilers. Interpreters sidestep this issue, but at the same time also suffer from the original performance problem.

µFoCUS

The "Verified and Secure Execution of Dynamic Languages" project builds on prior work by the chair Prof. Dr. Brunthaler on optimizing interpreters. His prior work builds on optimization of interpreting dynamic languages, which resulted in massive and important speedups of up to 6x. Since the interpreters do not emit native machine code, vulnerabilities and exploits as seen for JIT compilers are ruled out by construction. We formalized the essence of common dynamic language semantics in Isabelle and mechanically verified that it preserves semantics across a variety of aggressive optimizations similar to those applied by JIT compilers. Our results of formalizing and verifying optimized interpretation of dynamic languages have been published at the international conference on certified programming and proofs, CPP 2021

Broader Impact & Societal merit

Our project unites performance within reach of JIT compilers with guaranteed, mechanically verified correctness, thus eliminating an entire class of implementation errors plaguing commercial JavaScript JIT compilers. In consequence, society is presented with an alternative execution model of optimized dynamic languages, finally giving way to secure, verified execution of dynamic languages.

👤 Prof. Dr. Stefan Brunthaler

@ stefan.brunthaler@unibw.de

☎ +49 89 6004 7330

Funded by:
Federal Ministry of Defence (BMVg)

Prof. Dr. Gabi Dreo Rodosek

Communication Systems and Network Security

The chair deals with the detection and mitigation of so-called advanced persistent threats, the development of novel network-based moving target defence approaches, the use of AI/ML in the area of situational awareness and social analytics, among others, as well as software defined networking, 5G/6G, Internet of Things and quantum communication.

FIG.: ADOBE STOCK / DENIS PUTILOV, TAUSENDBLAUWERK; QUELLE: G. DREO RODOSEK

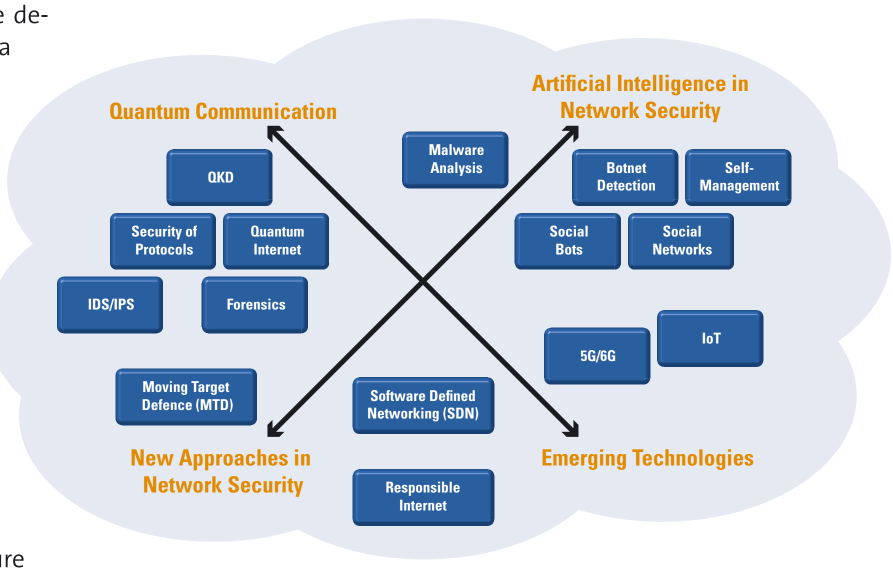
All future global dominant products and services will be located in the digital world or at least interact strongly with it. Examples are robotics, industrial automation, autonomous driving, smart grids, smart city and smart home. The digital transformation and the increasing networking of a wide variety of systems and objects are already changing our social, societal and professional lives. The increasing complexity and interdependencies of IT systems, and especially their interconnectivity, also cause a high cyber threat level.

It is nothing new that both the attacker and the defender challenge each other, but nowadays on a significantly higher and more qualified level than a few years ago. For example, the cyberattack on SolarWinds, which affected over 250 government agencies, thousands of companies and over 18,000 networks, represents a new dimension and quality of a threat that particularly targeted the IT management of computer networks. Therefore, the issue of cyber security of IT infrastructures in particular plays a key role. A trustworthy IT infrastructure, based on trustworthy, secure communication systems, is the basic prerequisite for functioning in our digital society.

The chair therefore pursues the goal of developing and prototyping solutions for the design and secure operation of modern, complex communication infrastructures within the framework of research projects. In doing so, different research areas are considered.

In a current research project, for example, a paradigm shift in network defense is being researched using Moving Target Defense (MTD) methods. The static approach to securing IT systems and computer networks grew out of the beginnings of cyber security, in which the system complexity and also the number of found or possible vulnerabilities were significantly lower than today. In order to break up conventional cyber defense concepts and, in particular, to change the asymmetry of the attack in favor of the defender, capabilities are needed that make it possible to dynamically change the attack surface of an IT system or network. This permanent dynamic change of the attack surface increases the complexity and thus the effort as well as the costs for attackers and limits the risk of security vulnerabilities and attack opportunities.

Another field of research is the use of AI/ML for the development of innovative cyber defense approaches at the level of network security. The fields of application are diverse and range from anomaly detection in the field of IDS/IPS, botnet detection, detection of cyberattacks such as DDoS in different network infrastructures such as Software Defined Networks, 5G/6G, or Internet of Things (IoT) networks. It also explores the use of AI/ML based on arbitrary data sources (e. g. social networks) to create cyber situational awareness, visualize the data resp. information and interact with it using mixed reality technologies.



Research Map of the Chair of Communication Systems and Network Security.

Further research deals with the use of quantum communication and the construction of a Quantum Internet in which quantum computers are connected by means of quantum communication links. In particular, research questions in the area of post-quantum cryptography and quantum key distribution are considered.

Prof. Dr. Gabi Dreo Rodosek

gabi.dreo@unibw.de

+49 89 6004 7300

www.unibw.de/network-security

CONCORDIA

A European ecosystem with leading competences from research, industry, SMEs and public organizations

The objective of CONCORDIA is to build the European Secure, Resilient and Trusted Ecosystem to develop next-generation cybersecurity solutions by taking a holistic end-to-end data-driven approach. In addition, building the European Education Ecosystem, identifying marketable solutions, growing pioneering techniques, building incubators are among other objectives.

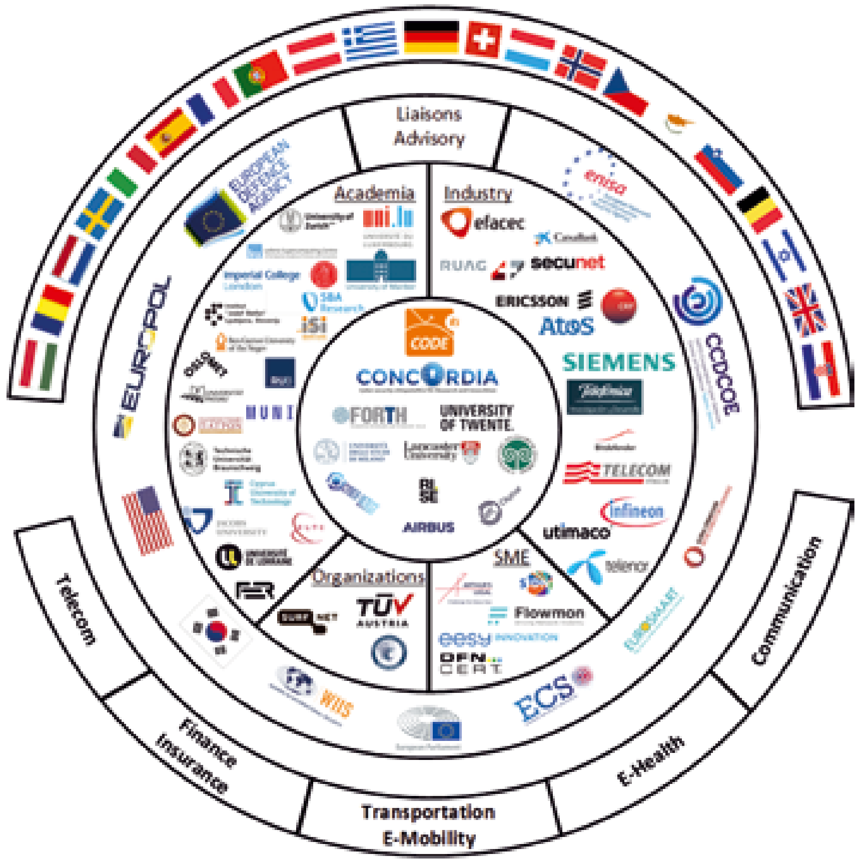
The pervasiveness of ICT technologies is increasing at an immense rate along with the complex interconnected environment of billions of Internet of Things (IoT) devices, services and users. The future ICT environment, likely cloud-assisted and IoT-based, is built of complex interconnected systems, highly heterogeneous and pervasive. The increasing heterogeneity, complexity and diversity of devices, computing systems, technologies, software and services along with the changing user interactions with technology are challenging for cybersecurity.

The threat landscape is evolving with tremendous speed. We are facing an extremely fast-growing attack surface with a diversity of attack vectors, a clear asymmetry between attackers and defenders, billions of connected IoT devices, mostly reactive detection and mitigation approaches, and finally Big Data challenges. The clear asymmetry of attacks (i. e., attackers need to find one weak spot only, the defenders needs to protect everything) and the enormous amounts of data are additional arguments making it necessary to re-think cybersecurity approaches in terms of reducing the attack surface, to make the attack surface dynamic, to automate detection, risk assessment and mitigation, and to investigate the prediction and prevention of attacks, utilizing artificial intelligence and machine learning.

Building a strong European Cybersecurity Competence Network

CONCORDIA is one of four winning pilot projects in the 2018 Horizon 2020 cybersecurity call "Establishing and Operating a Pilot for a European Cybersecurity Competence Network and Developing a Common European Cybersecurity Research & Innovation Roadmap."

Since cybersecurity is of vital importance for Europe's digital sovereignty, and following a Horizon 2020 (H2020) call, the Research Institute CODE as the coordinator has submitted a proposal in cooperation with 42 partners which has been accepted in the first place. CONCORDIA started in January 2019 with a funding of 16 million euros from the EU and comprises 53 partners and an additional funding of 7.1 million euros from industry and member states. The European security landscape does not suffer from a lack of ideas, but from fragmentation across its national borders, posing a key problem. Sometimes it is the lack of understanding of industrial constraints and major developments in secure hard- and software systems being out of the sphere of influence of the European Union that causes concern. CONCORDIA addresses this issue by building a European cybersecurity ecosystem, bringing different stakeholders (industry, research, SMEs, start-ups, public bodies) together in the development of European IT services and IT products.

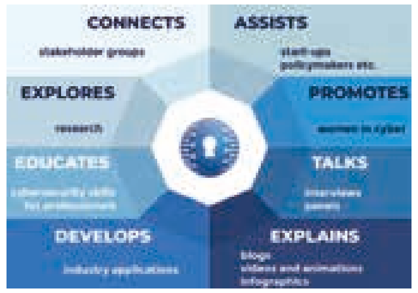


CONCORDIA Consortium, Still Growing.

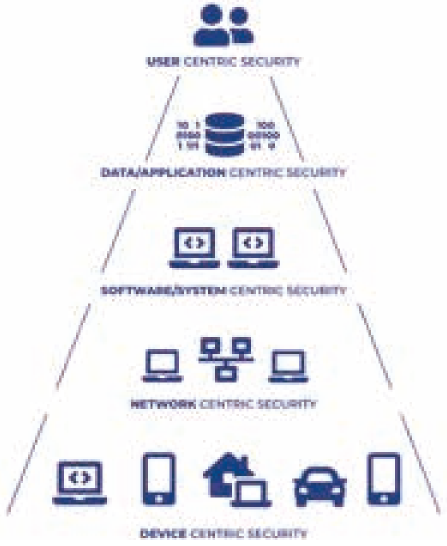
FIG.: © CONCORDIA CONSORTIUM PARTNERS

Service Catalog

CONCORDIA offers various services for the community. The "Assists" service, for example, aims to support young researchers and investors in establishing a startup company. At the same time, CONCORDIA supports women in their cybersecurity careers with "Women in Cyber". Since humans are still the biggest security threat in the system, CONCORDIA focuses on raising awareness for threats (including blogs, videos, and through infographics) combined with simultaneous training at a wide range of levels (including professionals, school, university, faculty) with the "Educates" service. Research and development are strongly related and interdependent, therefore CONCORDIA fosters collaboration and diversity in this area. Another goal is to connect the different stakeholders.



CONCORDIA's Service Board.



Layers of Research: Complex, Dynamic, Fast-growing, Highly Connected "Internet of Everything" from IoT to Cloud.

CONCORDIA Explores

A broad and evolvable data-driven and cognitive end-to- end (E2E) security approach for the highly complex and interconnected compositions of emerging cloud, IoT and edge-assisted ICT ecosystem is a must.

CONCORDIA addresses five layers of research and technology, from user-, application-, system-, network- to device-centric security, taking a holistic end-to-end security approach, especially as all cloud, IoT, and edge systems evolve in complex, interconnected ways to link multiple systems and services.

CONCORDIA Develops

The development of IT products and services will be performed in seven industrial pilot projects within CONCORDIA — five sector-specific and two cross-sector pilots.

Two sector-specific pilots, namely the telecom and financial sectors have established a customized threat intelligence platform for their application domains in order to properly share indicators of compromise (IoC). Both pilots are instantiating the more general threat intelligence platform for Europe (one of the cross-sector pilots) for their very sector-specific needs. Beyond the threat intelligence domain, a focus is put on e-health, e-mobility, security of unmanned aerial vehicles (UAV) and the creation of a DDoS clearing house for Europe.

Prof. Dr. Gabi Dreo Rodosek

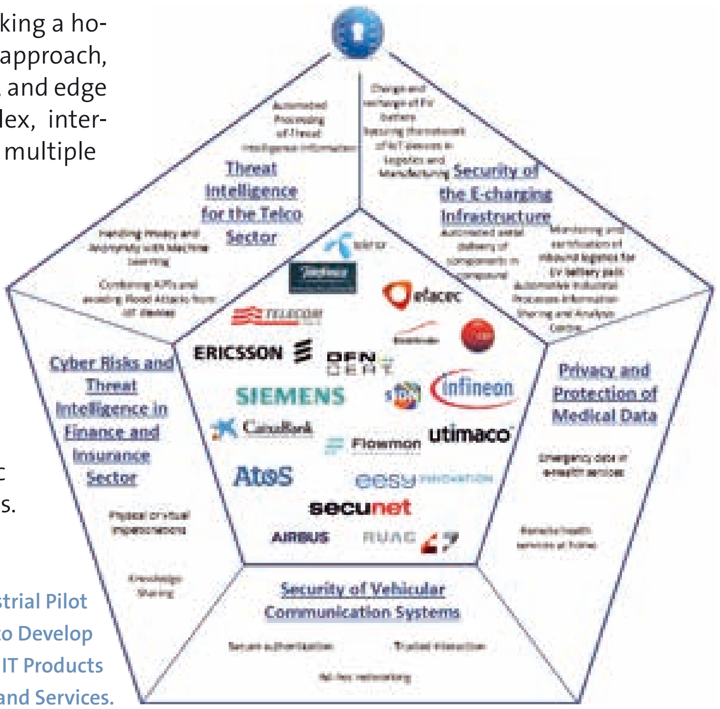
gabi.dreo@unibw.de

+49 89 6004 7300

www.unibw.de/network-security

Funded by: European Comission (EC)

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No. 830927.

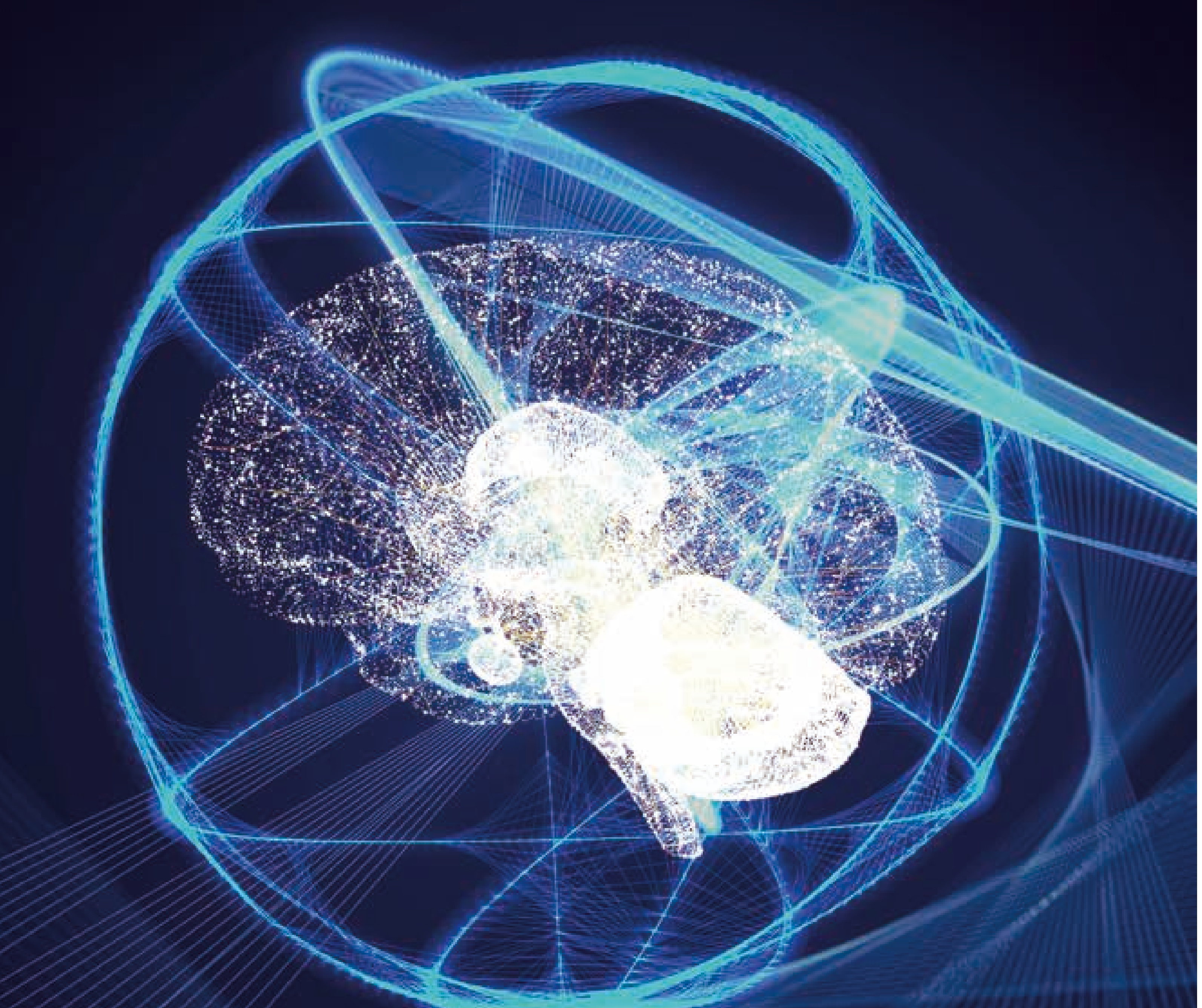

Threat Intelligence for the Telco Sector
Security of the E-charging Infrastructure
Cyber Risks and Threat Intelligence in Finance and Insurance Sector
Privacy and Protection of Medical Data
Security of Vehicular Communication Systems
ERICSSON
SIEMENS
infineon
utimaco
Flowmon
Atos
secunet
AIRBUS
RUAG
efacec

Seven Industrial Pilot Projects to Develop Platforms and IT Products and Services.

Prof. Dr. Michaela Geierhos

Data Science

The interdisciplinary team of the Chair of Data Science combines expertise from the fields of computer science, computational linguistics, and economics to address current and future-oriented research questions in the areas of semantic information processing and knowledge & data engineering.



Applied Research

Data Science is an applied, interdisciplinary science. Its goal is to generate knowledge from data in order to, for example, support decision-making processes. Approaches and knowledge from different fields such as mathematics, statistics, stochastics, computer science, and computational linguistics are used. The Chair 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). We focus 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, we maintain 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, we follow Alan Kay's guiding principle from 1970: "The best way to predict the future is to invent it".

Practice-oriented Training

In our courses, we particularly focus on a concept that combines theory and practice. From the very beginning, students benefit from the opportunity to directly apply the theoretical knowledge gained in the lectures in varied exercises and diverse practical projects. In this way, we contribute 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 our 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, we focus on the identification and modeling of short- and long-term disinformation campaigns in social media like Twitter, etc.

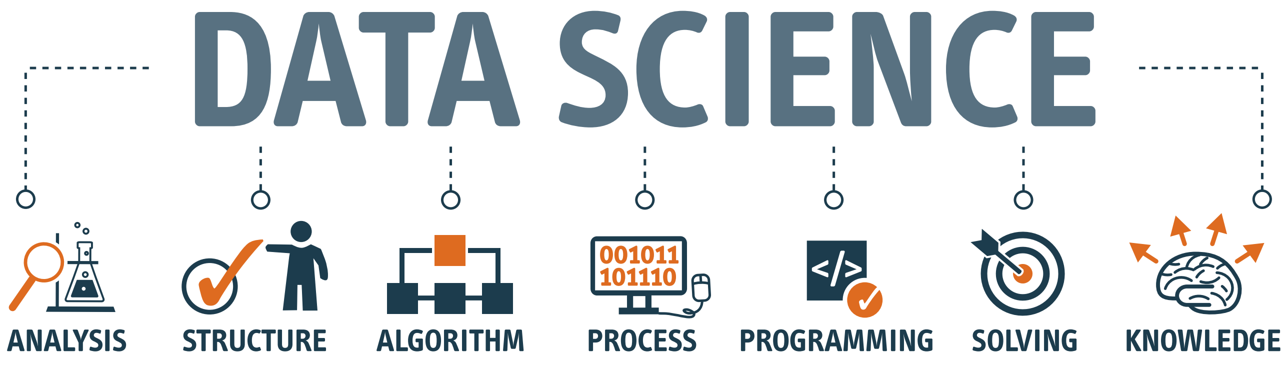
Recent technological advances and developments in the field of artificial intelligence (AI) have also given rise to so-called deep fakes. This refers to an audio-visual modification of a video generated by means of AI, in which the face and/or statements of the person depicted in the video have been changed. Our aim is to uncover these manipulations.

Prof. Dr. Michaela Geierhos

@ michaela.geierhos@unibw.de

☎ +49 89 6004 7340

www.unibw.de/datascience



Range of Tasks Covered by the Chair of Data Science.

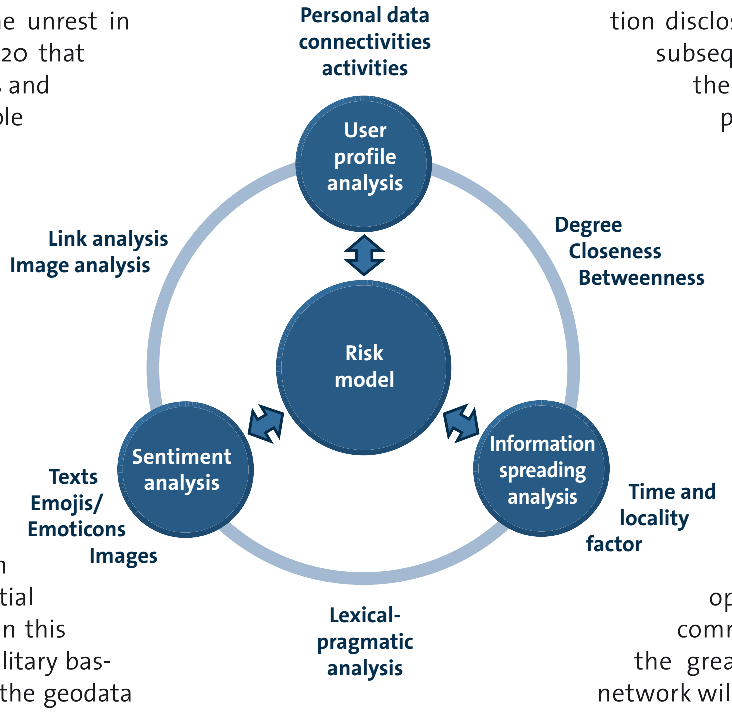
FIG.: ISTOCK / METAMORWORKS; SHUTTERSTOCK / TRUEFFELPIX

Project ADRIAN

Authority-Dependent Risk Identification and Analysis in Online Networks

The aim is to automatically monitor selected (running) apps and analyze their collected data, correlate it with social media profiles, and form clusters of people in order to identify potential targets and assess their risk potential. By correlating this information with additional classified data, it is possible to determine the threat plausibility for the respective (groups of) persons or locations.

It is not only since the unrest in the United States in 2020 that law enforcement officers and other groups of people have faced an increased risk potential on social media platforms. In particular, the linkage of social media accounts and posts (e. g., Twitter or Instagram) with tracking and location data from popular running apps enables the identification of users and their relatives, making them traceable and a potential target for cyberattacks. In this context, the fact that military bases can be located using the geodata collected from running routes is another security-related aspect.



Functional Interaction of the Risk Analysis Methods.

In the first stage of this project, selected running apps will be monitored and the geodata collected will be analyzed. In the second stage, the user profiles from the running apps and social media platforms will be correlated so that a cluster of people can be formed and potential targets can be identified. Since a so-called "digital (running) twin" can be reconstructed in this way as part of the data analysis and knowledge extraction process, extremely sensitive data is generated. If this data can also be correlated with other confidential data (e. g., from security services or military agencies), an assessment of the threat plausibility for corresponding persons (groups) or locations can be made. In order to achieve these goals, the technical implementation of the project must combine, among other things, methods of information retrieval with approaches from forensic linguistics. Furthermore, methods of network analysis and clustering will be used to develop novel evaluation functions for the detection of targets at risk (persons, locations, etc.) on the basis of the information disclosed in Web 2.0. For the subsequent transmission of the insights gained in this process to other services, the use of highly secure quantum encryption is planned as well.

The ADRIAN subproject (Authority-Dependent Risk Identification and Analysis in Online Networks) is funded as part of the MuQuaNet research project, which aims to set up, test and operate a quantum-safe communications network in the greater Munich area. This network will initially be made available to the Universität der Bundeswehr München, but later also to other research institutions, authorities and military agencies.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

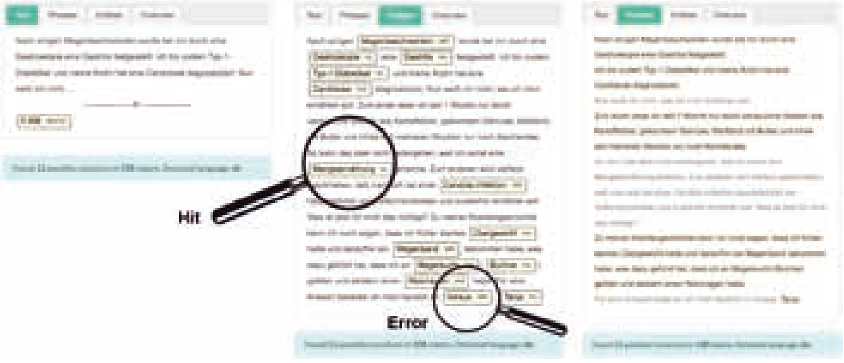
+49 89 6004 7340

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

Project TextBroom

Towards a Multi-Stage Approach to Detect Privacy Breaches in Physician Reviews

The modern web is based on interaction, discussion, and the exchange of information. Over and over, personal information is used against the originators themselves. With TextBroom, a concept has been developed that addresses the detection of information disclosure through a multi-layered processing chain in order to identify critical text sequences and provide an explanation of the possible risks.



TextBroom at Work: Highlighting Private Patient Information in Doctor Reviews.

FIG.: MICHAELA GEIERHOS

Connected World: Open Source Intelligence

The advancing semantic linkage on the Web (the so-called semantic web) also creates a huge, freely accessible source of information for data-driven applications. This may pose a personal risk to individuals. As user-generated data on the web is more and more effectively linked to external resources (so-called knowledge sources) in an automated way, even unintentionally (implicitly) revealed personal information can have harmful consequences for individuals. Although service providers on the web have a duty to ensure the security and privacy of user data, there are still cases where user data is misused and compromised, or publicly available information is used against the original author. Thus, it is also in the interest of users to place only that information in text posts that maintains a certain self-determined degree of anonymity.

Digital Footprint Tempts Data Misuse

Information that has been published bit by bit over a period of years, is no longer manageable for the authors, no longer editable and thus no longer controllable. It has the potential to be used to create a digital representation. A very tangible example here are online forums, where users seek help on health-related topics. In individual posts, the authors are ideally careful not to reveal too much information. However, they forget that the sum of the posts over the entire existence of their user account can be used to create a "digital twin". In the TextBroom project, together with Dr. Frederik Bäumer from the University of Applied Sciences Bielefeld, it could be shown that a revealing information puzzle resulted from many user accounts over several posts and several years.

Privacy at Risk?

How (unwitting) information disclosure manifests itself in linguistic expressions has so far been insufficiently studied. However, this is mandatory in order to identify corresponding privacy-threatening text components and to provide them with an explanation of possible risks. It could be shown that by analyzing the user-generated and domain-specific knowledge resources step-by-step, it is possible to automatically detect isolated privacy-threatening statements. However, this method does not yet meet the challenge in its entirety, since the interaction of individual pieces of information remains unconsidered.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

Prof. Dr. Wolfgang Hommel

Software and Data Security

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 chair of software and data security pursues the goal of developing solutions for real-world-relevant 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. 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, they are integrated as seamlessly as possible into the design, implementation, and operational processes of the intended application areas, also from an organizational perspective. An essential requirement is the concrete implementation with subsequent evaluation, which takes place at a minimum in the laboratory, but if possible also in concrete pilot environments and ideally by individual embedding in scientifically accompanied projects. The role of the human factor in information security, economic and legal constraints is also taken into account.

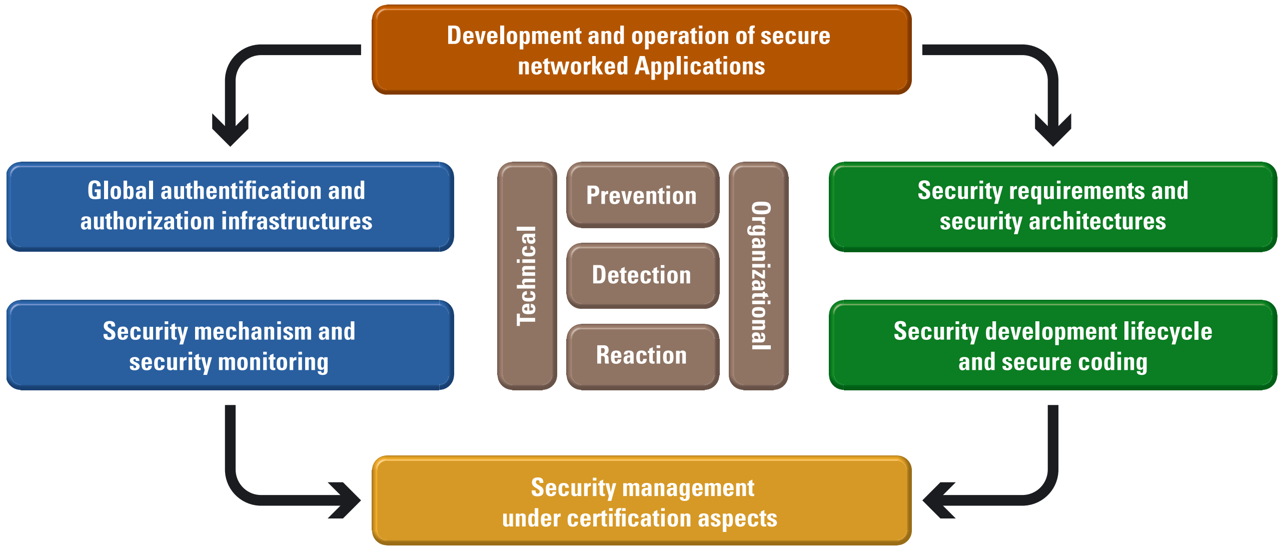
Current research projects and projects work are, for example, being done on the implementation of the self-sovereign identity paradigm for use in global authentication and authorization infrastructures as a data protection-friendly technological advancement of federated identity management that has proved itself in practice. Ongoing work on security monitoring components and policy-driven management platforms for federated software-defined networks is used, for example, in the establishment and expansion of the 5G telecommunications infrastructure and in the dedicated cross-location networking of industrial control systems. In the area of the Internet of Things, the research focus is on the software-side protection of LoRaor 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 2495

www.unibw.de/software-security


Development and operation of secure networked Applications
Global authentification and authorization infrastructures
Security mechanism and security monitoring
Technical
Prevention
Detection
Reaction
Organizational
Security requirements and security architectures
Security development lifecycle and secure coding
Security management under certification aspects

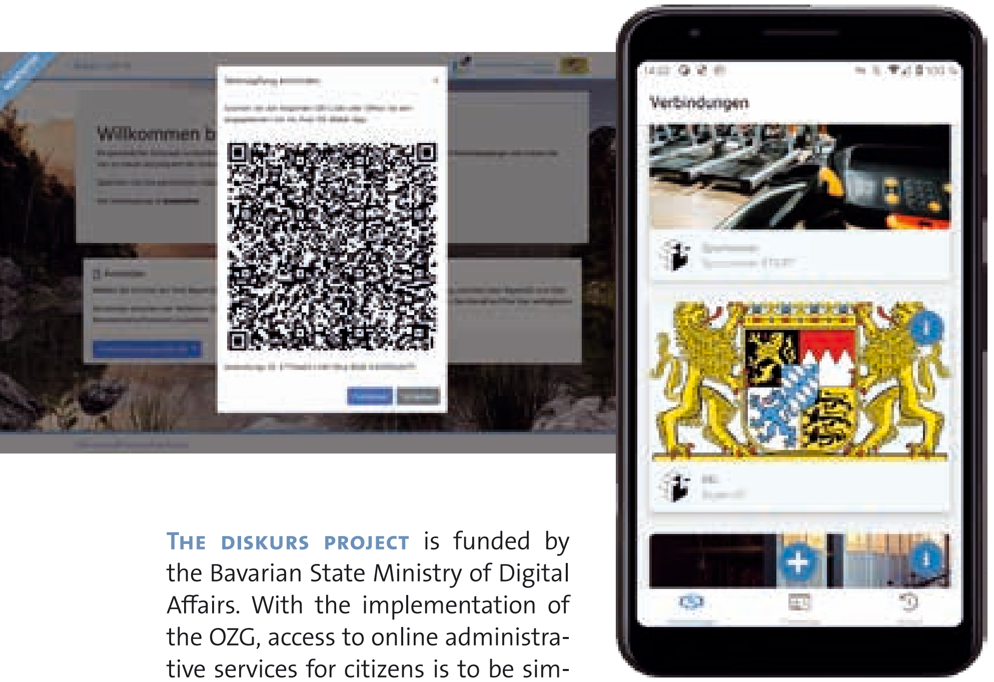
Main Research Topics of the Chair for Software and Data Security.

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

Project DISKURS

Digital Identities for Service Accounts: Implementation Strategies, Guidelines, and Security Aspects

The DISKURS project scientifically accompanies the establishment and operation of the nationwide identity federation FINK and supports it both technically and organizationally. The need for such a federation is a result of the implementation of the Online Access Act (OZG). In addition, future technologies such as Self-sovereign Identity Management (SSI) are also being investigated and demonstrated.



Screenshot of the Prototype for SSI-based Online Administrative Services.

The DISKURS project is funded by the Bavarian State Ministry of Digital Affairs. With the implementation of the OZG, access to online administrative services for citizens is to be simplified. It should be possible to carry out administrative procedures purely online. The necessary infrastructure for secure authentication is created with the FINK federation. This federation is based on the Security Assertion Markup Language (SAML) technology, which has been proven over many years.

Use of Proven Approaches

Due to the relevant experience with this technology in higher education, an important contribution can be made to topics such as the software architecture used, including various data models and profiles, the technical trust levels, and federation-wide IT security.

In addition to the technical aspects, the organizational side of the federation's operation is also considered, thereby optimizing federation-specific processes. This includes, for example, the exchange of metadata between the federation participants, but also the area of IT service management in general.

New Technologies Research

In addition to considering the status quo of the current federal architecture, the project also presents the possibility of including self-sovereign identity management solutions in eGovernment. For this purpose, the potential of SSI technology is shown by means of a demonstrator and the feasibility and advantages of the solution are presented. The focus is not to present a completely new system, but to find commonalities between the SSI approach and the federation. Thus, existing investments can be protected and long-term migration paths can be shown.

Outlook

The relevance of SSI and the associated bring-your-own-identity paradigm is also demonstrated by a large number of similar projects on the topic in Germany, the EU and worldwide. DISKURS can benefit from close networking with the Bavarian federation provider and its leading role in the FINK federation and can focus the investigations on real use cases in eGovernment.

👤 Michael Grabatin
@ michael.grabatin@unibw.de
☎ +49 89 6004 3992

Funded by:
Bavarian State Ministry of Digital Affairs (StMD)

FIG.: MICHAEL GRABATIN; SIEGFRIED BRUNNER

Project Smart Hospitals

Secure Digitization of Bavarian Hospitals

Smart Hospitals is researching how to safeguard Bavarian hospitals in the face of increasing digitalization. Today, practically all activities in hospitals are IT-supported. Hacker attacks, malware, or system failures are therefore a real danger to patients and hospital operations. In coordination with the Bavarian state office for information security, the project is developing solutions for secure digitization.

Digitization in hospitals has many facets: politics, hospital staff, and patients all demand the digital hospital. Hospitals must meet this demand and also survive in a competitive environment. This creates further pressure on hospitals to act. The situation is made more difficult by a shortage of IT personnel, incomplete expertise in IT security in some cases, and impractical and vague guidelines on the subject. Added to this is the growing organizational burden and the diversity of IT systems. With all these challenges, organizational and technical weaknesses creep in. Their exploitation, e. g. by malware, can not only lead to data loss, but can even pose a threat to patient health.

Support by RI CODE

The situation has been analyzed in a structured way by RI CODE, funded by the Bavarian Ministry of Health and Care (StMGP), and improved for the hospitals in Bavaria. To this end, a multi-stage situation analysis was first carried out: almost 40% of the approximately 400 hospitals in Bavaria took part in a survey on the situation of IT security and digitization. In addition, an on-site analysis was carried out at a double-digit number of hospitals, including detailed discussions with IT management, business management, and medical staff, which enabled valuable existing security solutions as well as open gaps to be identified.

SMART HOSPITALS

MAẞNAHMENKATALOG
ZUR VERBESSERUNG DER IT-SICHERHEIT IN
BAYERISCHEN KRANKENHÄUSERN
AUSGABE 2020/2021

Catalog of Measures Cover Page.

A Catalog of Measures for Hospitals

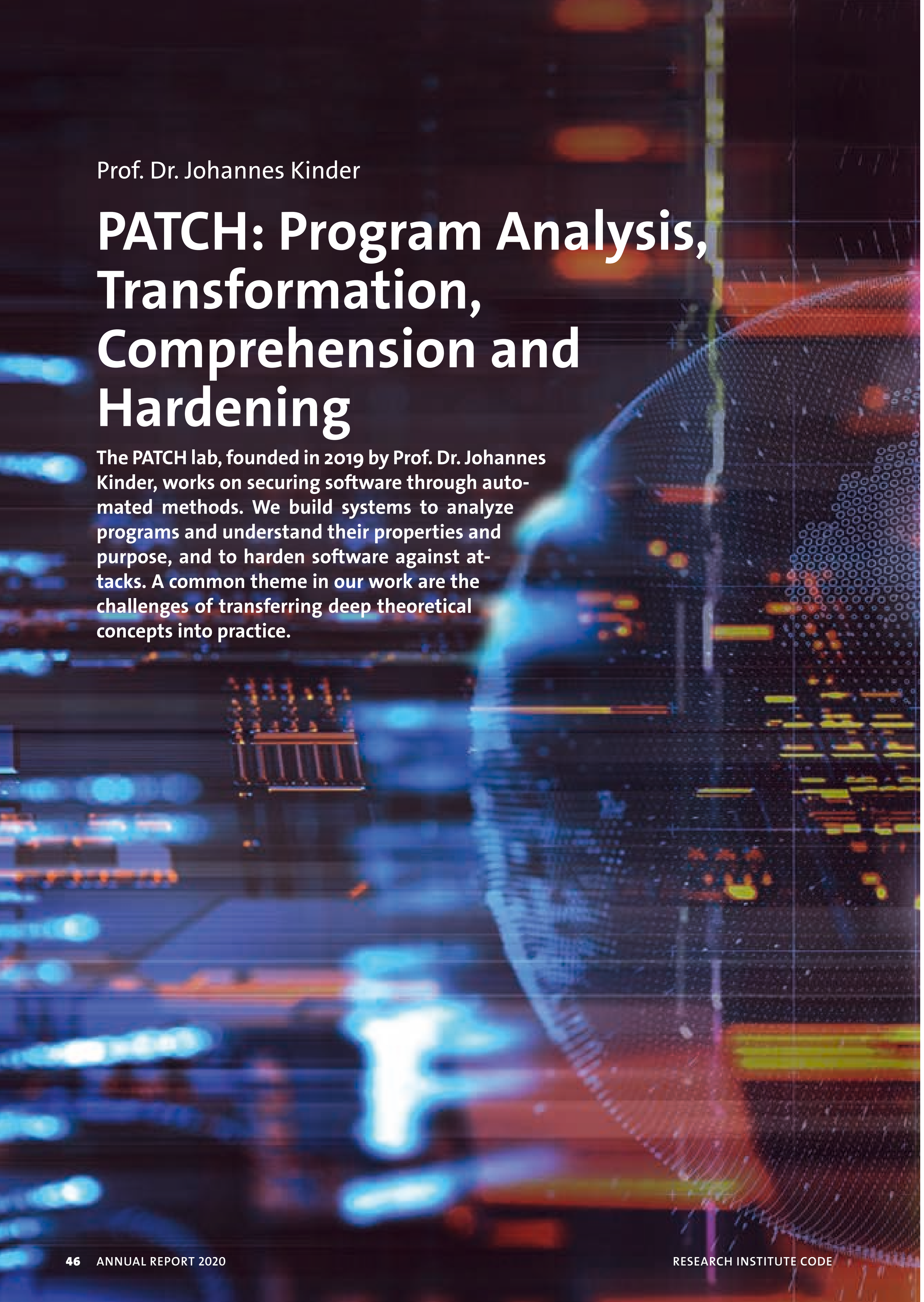
Based on the situation analysis, RI CODE has prepared and published a first edition of a catalog of measures to improve hospital IT security (see figure). 33 measures for the most important topics identified take into account not only the technical perspective, but also important organizational aspects and measures to increase security awareness among hospital staff. The measures were coordinated with the Bavarian State Office for Information Security (LSI) in Nuremberg and its newly developed orientation guide on IT security in hospitals. The catalog of measures is publicly available on the RI CODE website.

Further Improvement

The current catalog of measures is an interim result. It was sent to all Bavarian hospitals and discussed at events with hospital representatives. Their feedback on the catalog of measures is an essential basis for a new, extended, and updated edition in autumn 2021.

👤 Michael Steinke
@ michael.steinke@unibw.de
☎ +49 89 6004 4825
🌐 www.unibw.de/code/smart-hospitals

Funded by:
Bavarian Ministry of Health and Care (StMGP)



Prof. Dr. Johannes Kinder

PATCH: Program Analysis, Transformation, Comprehension and Hardening

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

General Chairs Prof. Kinder and Prof. Cavallaro opening ACM CCS 2019 in London.

THE NAME PATCH defines the core areas of the lab headed by Prof. Dr. Kinder: Program Analysis, Transformation, Comprehension, and Hardening.

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 our research, we tackle the problems arising in practice due to complex runtime environments, such as in JavaScript ecosystems like Node.js or through newly introduced platforms such as WebAssembly.

Program Understanding and Reverse Engineering

To check the suitability and security of software, we develop automated methods to categorize and understand program components. This can allow an organization to discover backdoors or malware in third-party software. To this end, we develop both classic, formal methods-based approaches, as well as models based on statistical and deep learning. The application domains of our research range from desktop programs, services, and device drivers to mobile apps.

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.

International Networking

We put particular emphasis on connecting with the international research community in the field of IT security. Along with a focus on publications with the highest international visibility, we regularly participate in the leading academic conferences. In 2020, this unfortunately mainly implied late-night video streaming for Europeans. Nevertheless, 2019 had ended on a high note with Prof. Dr. Kinder jointly chairing the ACM Conference on Computer and Communications Security (CCS) in London, together with Prof. Dr. Cavallaro of King's College London. Over 1,200 scientists came together at this leading international conference to present and discuss the latest research results.

👤 Prof. Dr. Johannes Kinder

@ johannes.kinder@unibw.de

☎ +49 89 6004 7335

🌐 www.unibw.de/patch

FIG.: iSTOCK / MF3D; MIA ROBERTSON

Efficient Automatic Security Testing for Dynamic Languages

The ExpoSE System Automatically Generates Thousands of Tests for Complex JavaScript Programs

Dynamic programming languages like JavaScript lie at the foundation of the world-wide web, running both in web browsers and on servers. While in JavaScript it is easy to quickly bootstrap new features, websites, and systems, it is also easy to make mistakes. In the EASTEND project (Efficient Automatic Security TEstiNg for Dynamic languages) we devise new methods to automatically find mistakes in JavaScript programs.

EASTEND SOUGHT to prove that an inherently dynamic language is best served by a dynamic approach to verification. We therefore chose to use test generation by dynamic symbolic execution (DSE) to systematically cover paths through programs and check security properties along those paths. While this prevents generating proofs, it ensures that all paths executed are feasible with respect to the execution environment. The two main lines of work were to improve DSE for real-world JavaScript code and to develop a flexible specification methodology for security properties.

JavaScript Symbolic Execution

ExpoSE, the open source DSE engine for JavaScript that we developed as part of the project, is able to automatically generate test cases for most Node.js programs without modifications. The main challenge faced by ExpoSE is that it needs to reason about the effects of the rich JavaScript semantics, including its vast standard library. In particular, most JavaScript programs process strings in some form and often rely on regular expressions, which are often a limiting factor for any kind of automated analysis.

In this project, we devised the first complete strategy to automatically reason about JavaScript regular expressions. We encoded the semantics of regular expression operations using string constraints and classical regular expressions and we devised a refinement scheme to address the problem of matching precedence and greediness: regular expressions will consume as many input characters as possible, from left to right. This constraint has so far been ignored in related work and existing solvers of regular expressions.

Our survey of over 400,000 JavaScript packages from the NPM software repository shows that one fifth make use of complex regular expressions. We implemented our encoding and refinement scheme in ExpoSE and evaluated it on 1,131 Node.js packages, demonstrating that the encoding is effective and can increase line coverage by up to 30%. We used line coverage here as a proxy metric for the effectiveness of the encoding: it demonstrates that more parts of the program can be reached, increasing the analysis surface for detecting bugs and vulnerabilities.

We describe the encoding, refinement, and evaluation in an article published at the 2019 ACM SIGPLAN Conference on Programming Language Design and Implementation (PLDI), one of the two leading international conferences in the field.

JavaScript Security Annotations

Several security-relevant properties, such as data provenance or integrity, cannot be written as assertions in JavaScript itself. We therefore developed an approach to attach additional security annotations to a language. This lightweight metatheory of security annotations allows tests to encode properties not present in the program state. We demonstrated the consistency of our system in a statically typed lambda calculus (published at PEPM 2018) and then followed up with a fully dynamic reference implementation for JavaScript. We specified a partial fragment of the Web-Crypto API in terms of security annotations and demonstrated how to use it to detect security vulnerabilities. This work was published in the 2019 European Symposium on Research in Computer Security (ESORICS), the leading European Conference in its field.

Prof. Dr. Johannes Kinder

johannes.kinder@unibw.de

+49 89 6004 7335

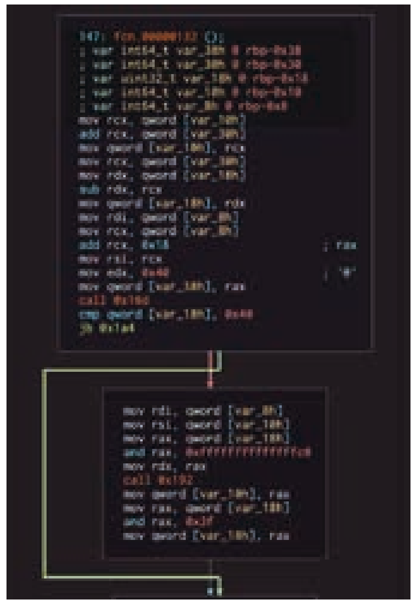
www.unibw.de/patch

Funded by: UK Government & Engineering and Physical Sciences Research Council (EPSRC)

Reverse Engineering Meets Deep Learning

Machine Learning Models Imitate Human Software Developers in Naming Functions in Binary Code

Computer programs are written in source code. For execution, they are compiled into a binary form unreadable to humans. Because the source code is not available in many situations, it is difficult for human reverse engineers to judge the behavior of a binary program. Our machine learning system is trained to label components in binaries with names that are similar to those in the original source code, aiding human analysis.



```
147: fcn.000001f2 ();
; var int64_t var_38h @ rbp-0x38
; var int64_t var_30h @ rbp-0x30
; var uint32_t var_1ch @ rbp-0x1c
; var int64_t var_18h @ rbp-0x18
; var int64_t var_8h @ rbp-0x8
mov rcx, qword [var_30h]
add rcx, qword [var_38h]
mov qword [var_18h], rcx
mov rcx, qword [var_18h]
mov rdx, qword [var_18h]
sub rdx, rcx
mov qword [var_18h], rdx
mov rdi, qword [var_8h]
mov rcx, qword [var_8h]
add rcx, 0x18                          ; rax
mov rsi, rcx
mov edx, 0x40                          ; '@'
mov qword [var_18h], rax
call 0x16d
cmp qword [var_18h], 0x40
jb 0x1a4

    mov rdi, qword [var_8h]
    mov rsi, qword [var_18h]
    mov rax, qword [var_18h]
    and rax, 0xffffffffffffffc0
    mov rdx, rax
    call 0x192
    mov qword [var_18h], rax
    mov rax, qword [var_18h]
    and rax, 0x3f
    mov qword [var_18h], rax
```

Without Debugging Information, Disassemblers Can Assign Only Generic Names.

FIG.: SCREENSHOT SOFTWARE CUTTER/RADORE2 / J. PATRICK-EVANS

FUNCTION NAMES, comments, and other information in source code help engineers to understand and debug the inner workings of a computer program. Such information is usually not included in the binary executables distributed to end users, and even a disassembler cannot reconstruct these annotations. While this is beneficial for protecting intellectual property, it also makes malicious code and vulnerabilities much harder to detect.

Our work aims to gain a fundamental insight into exactly what computer code does and reverse the process of removing human-readable information from executable programs. We use deep learning methods to build a model that "understands" what the different components of binary code do and tag them with human-readable information. Using our technique, we can quickly identify interesting parts of a program and focus further efforts.

The key idea is to learn a numerical representation of machine code that is contained inside each compiled executable. Relying on a large dataset of open-source software that does not have its debugging information removed, we can train a machine learning model to label each functional component.

Labeling Functions in Binaries

It is difficult to predict the labels that humans assign to objects. For example, a picture of an orange may be labeled as a fruit, the color orange, or a food item. All of these labels are correct, but not unique. When labeling computer code, similar pieces of machine code may be labeled very differently.

We start by analyzing compiled programs that have debugging information included in order to determine the name and location of symbols. A symbol is an identifier that describes the location, type, and name of a structure inside an executable file. Our tool then analyzes how this symbol behaves and interacts relative to other symbols. This allows us to build a graph of all the symbols from a program in which connections between symbols represent different relationships based on their interactions.

After extracting a binary's symbols and each symbol's features, we build a numerical vector representation to identify each object. The vector we build expresses arbitrary relationships between symbols that relate to human readable tags we assign to computer code. This representation also allows us to predict the properties of unseen machine code by specifying which human readable tags we wish to include. In particular, these tags can be used to construct human readable function names missing in commercial and malicious software. We describe an initial version of our approach and system in a paper published at the 2020 Annual Computer Security Applications Conference (ACSAC).

Prof. Dr. Johannes Kinder

johannes.kinder@unibw.de

+ 49 89 6004 7335

www.unibw.de/patch

Funded by: Engineering and Physical Sciences Research Council (EPSRC) & Research Institute CODE

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

Project HoBIT

Highly Secure Operating Systems for Embedded IT

The HoBIT project developed methods which allow formal program verification to be applied to operating systems and operating system components in the context of real-world IT security. In particular, the verification of existing and newly developed programs in C is supported, which is still the dominant programming language in operating systems.

Systems and devices with embedded information technology (IT) are only as secure as the operating system used as the basic building block on top of the hardware. The operating system kernel runs in the most permissive hardware mode and if it is compromised it can alter the behavior of every hardware and software component in the system. Programming errors can directly lead to unwanted behavior, or they can be exploited to attack and control the kernel. The best defense against errors is a formal proof that the program code does not contain any errors. However, formal proofs are still only feasible for small programs, much smaller than a real-world operating system kernel.

Microkernels

The answer to this problem are microkernels with a massively reduced functionality which are small enough for formal verification. The most important remaining functionality of the kernel is to strictly separate other software components from each other, the microkernel and the hardware. These other components can then be used to implement the rest of the operating system functionality; together with the microkernel they constitute a full operating system.

The seL4 microkernel has already been successfully formally verified. For operating systems based on seL4 its architecture supports a performance similar to monolithic operating system kernels. The TRENTOS system, developed by Hensoldt Cyber, is an operating system designed in this way. The HoBIT project aimed at methods and tools to provide similar security properties for the whole operating system, as they exist for the seL4 microkernel, through formal verification.

The strict separation of the additional components has the effect that a compromised component cannot affect other components, the microkernel or arbitrary parts of the hardware. However, a compromised component can still be a heavy security risk for a system in a critical environment. A compromised network communication component may still block important communication channels or redirect or copy confidential data to other channels. It is therefore also necessary to apply formal verification to at least some of the operating system components.

Verifying Real-World OS Components

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 HoBIT project we investigated the Cogent language, developed by Data61 (CSIRO, UNSW Sydney), as an interesting candidate. It compiles abstract functional style code to executable code and generates a refinement proof which proves that the resulting code behaves as expected.

In reality, operating system components are most often written in C, which is a low-level language and a nightmare for formal verification. This holds for legacy code, but also for a lot of newly developed code, since the developers are highly specialized and used to programming in C. Therefore, our approach in the HoBIT project was to support formal verification of C code by developing Gencot, a semiautomatic tool for translating C programs into Cogent. It is intended to support C programmers in the task of transferring existing code to Cogent and make it accessible to formal verification. As a proof of concept, it has been successfully applied to TRENTOS components written in C to provide alternative implementations in Cogent. 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

Prof. Dr. Arno Wacker

Privacy and Compliance

Don’t Just Teach Data Privacy and Compliance, Live It!

One of our most important goals is not only to research and teach data privacy and IT Security, but also to bring it into everyday life. In this way complex topics could be communicated in a persuasive and authentic way to the students. Additionally we also want to demonstrate to the public that technologies which support data privacy could be integrated in everyday life, private as well as business.

Teaching

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

Research

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

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

Knowledge Transfer

A special focus of our professorship is to upskill and enlighten interested citizens and to tutor and to inform them on IT security-related questions. This task is achieved with the help of presentations and workshops which for example deal with the topics of penetration testing, secure email in everyday life, and the reconstruction of security breaches. For the last point the professorship offers among others a heartbleed server on which interested people could try, in an isolated environment, to use these exact bugs.

Prof. Dr. Arno Wacker

@ arno.wacker@unibw.de

☎ +49 89 6004 7325

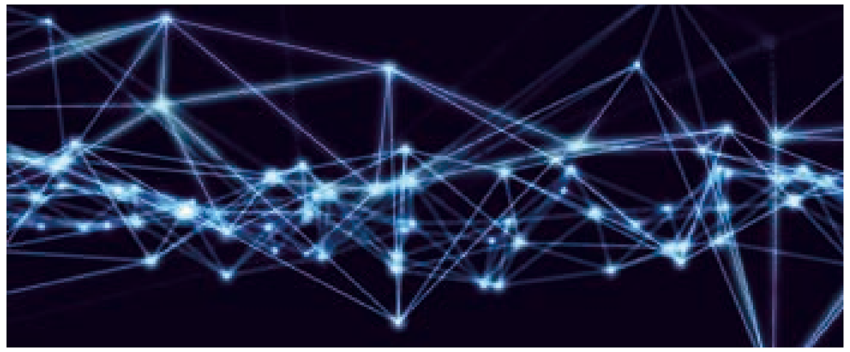
www.unibw.de/datcom

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

FIG.: ISTOCK / MATEJMO; ISTOCK / BAKS

Project Redundant Structures in Fully Distributed Overlay Networks

This research 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 without central node.

The networking infrastructure of many internet services follows a centralized approach. A central node, like a web server, controlled by a company or organization, serves as the system's backbone. It acts as relay in the communication between all other nodes and provides most or all of the system resources. Participating in such a centralized system is fairly easy. All that other nodes, i. e. users, have to do is connect to this central node. As a consequence, the availability of such a system fully depends on the availability of the central node and the availability of that network path.

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 still 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 not only 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 censor 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 top of 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 in 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.

One goal of this research is to harden large, fully distributed systems by analyzing and improving network resilience against targeted attacks and technical failures. The means for this are the creation and exploitation of redundancies in data storage and network connectivity, avoiding single points of failure and control and, thereby, reducing the probability of services being unavailable or censored.

Prof. Dr. Arno Wacker

@ arno.wacker@unibw.de

☎ +49 89 6004 7325

🌐 www.unibw.de/datcom

Project DECRYPT: 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 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 are 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.

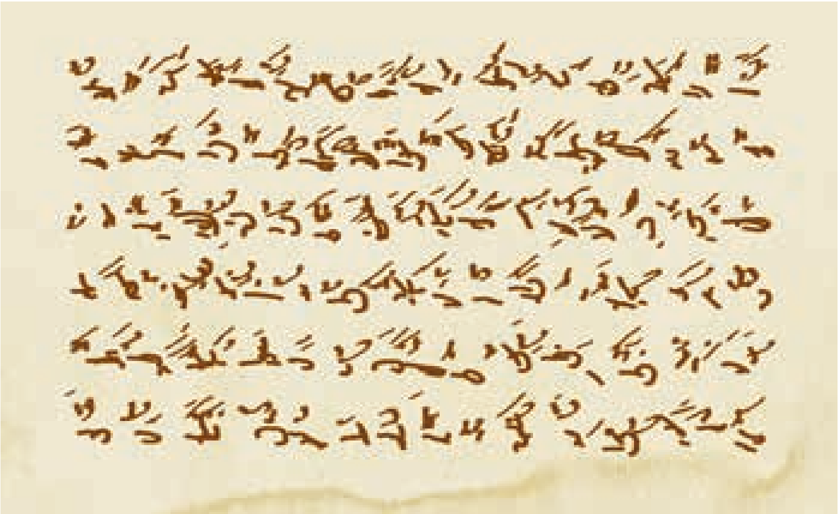


FIG.: ISTOCK / METAMORWORKS; ISTOCK / CARDUUS
Libraries and archives still contain many unsolved mysteries.

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. The user of the database will also be offered the opportunity to upload an encrypted manuscript as a picture and the system will automatically transcribe and decode the text. This is thanks to image processing and decryption algorithms that will be developed during the project and linked to the database. Additionally, we will also provide a large collection of historical texts from different time periods and language models for 15 European languages in a standardized format allowing search and studies of language variation and change over time. 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.

Prof. Dr. Arno Wacker

@ arno.wacker@unibw.de

☎ +49 89 6004 7325

🌐 www.unibw.de/datcom

Funded by:
Swedish Research Council (SRC)

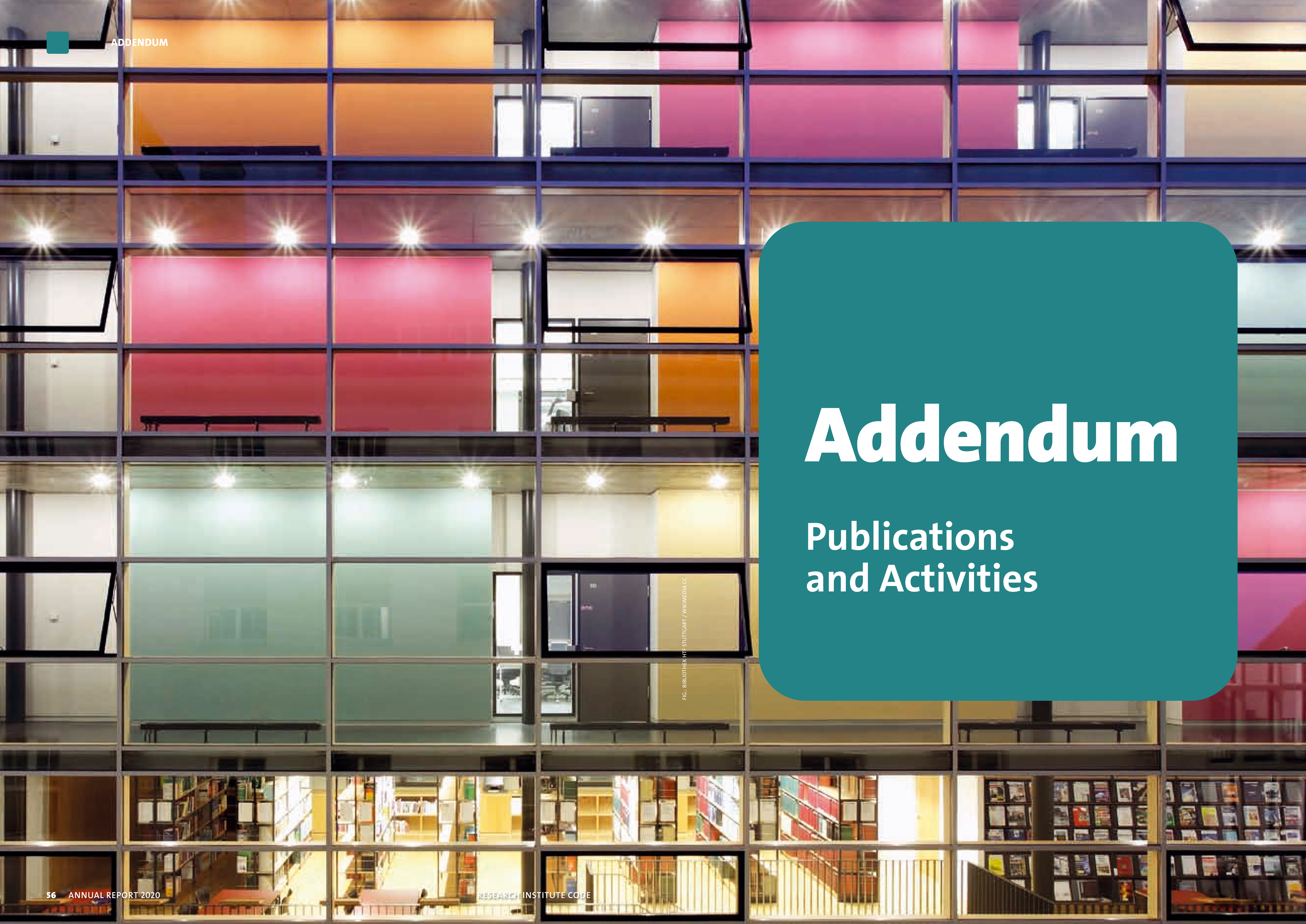


FIG.: BIBLIOTHEK HFT STUTTGART / WIKIMEDIA CC

Addendum

Publications and Activities

Prof. Dr. Florian Alt

Usable Security and Privacy

Publications

Abdrabou, Y., Pfeuffer, K., Khamis, M. & Alt, F.: GazeLockPatterns: Comparing Authentication Using Gaze and Touch for Entering Lock Patterns. Proceedings of the 2020 ACM Symposium on Eye Tracking Research & Applications, ACM, 2020

Abdrabou, Y., Prange, S., Mecke, L., Pfeuffer, K. & Alt, F.: VolumePatterns: Using Hardware Buttons beyond Volume Control on Mobile Devices. Proceedings of the 1st CHI Workshop on Authentication Beyond Desktops and Smartphones, 2020

Braun, M. & Alt, F., Bolock, A. E., Abdelrahman, Y. & Abdennadher, S. (Ed.): Character Computing Identifying Personality Dimensions for DigitalAgents. Character Computing, Springer International Publishing, 2020, 15

Braun, M., Li, J., Weber, F., Pfleging, B., Butz, A. & Alt, F.: What If Your Car Would Care? Exploring Use Cases For Affective Automotive User Interfaces. Proceedings of the 22nd International Conference on Human-Computer Interaction with Mobile Devices and Services, ACM, 2020

Colley, A., Pfleging, B., Alt, F. & Häkkilä, J.: Exploring Public Wearable Display of Wellness Tracker Data. International Journal of Human-Computer Studies, 2020

Englmeier, D., O'Hagan, J., Zhang, M., Alt, F., Butz, A., Höllerer, T. & Williamson, J.: TangibleSphere – Interaction Techniques for Physical and Virtual Spherical Displays. Proceedings of the 11th Nordic Conference on Human-Computer Interaction, ACM, 2020

Fanger, Y., Pfeuffer, K., Helmbrecht, U. & Alt, F.: PIANX – A Platform for Piano Players to Alleviate Music Performance Anxiety Using Mixed Reality. Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia, ACM, 2020

Froehlich, M., Gutjahr, F. & Alt, F.: Don't lose your coin! Investigating security practices of cryptocurrency users. Proceedings of the 2020 ACM Conference on Designing Interactive Systems, ACM, 2020

Gentile, V., Khamis, M., Milazzo, F., Sorce, S., Malizia, A. & Alt, F.: Predicting Mid-Air Gestural Interaction with Public Displays based on Audience Behaviour. International Journal of Human-Computer Studies, 2020

Katsini, C., Abdrabou, Y., Raptidis, G. E., Khamis, M. & Alt, F.: The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, 2020

Khamis, M. & Alt, F., Dingler, T. (Ed.): Augmented Perception and Cognition. Privacy and Security in Augmentation Springer, 2020

Kosch, T., Hassib, M., Reutter, R. & Alt, F.: Emotions on the Go: Assessing Emotional Probes in Real-Time using Facial Expressions. Proceedings of the 2020 International Conference on Advanced Visual Interfaces, Association for Computing Machinery, 2020

Marky, K., Prange, S., Krell, F., Mühlhäuser, M. & Alt, F.: ,You just can't know about everything': Privacy Perceptions of Smart Home Visitors. Proceedings of the 19th International Conference on Mobile and Ubiquitous Multimedia, ACM, 2020

Mäkelä, V., Radiah, R., Alsherif, S., Khamis, M., Xiao, C., Borchert, L., Schmidt, A. & Alt, F.: Virtual Field Studies: Conducting Studies on Public Displays in Virtual Reality. Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, Association for Computing Machinery, 2020

Prange, S. & Alt, F.: I Wish You Were Smart(er): Investigating Users' Desires and Needs Towards Home Appliances. Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, 2020

Prange, S. & Alt, F.: Interact2Authenticate: Towards Usable Authentication in Smart Environments. Proceedings of the 1st CHI Workshop on Authentication Beyond Desktops and Smartphones, 2020

Prange, S., Mecke, L., Nguyen, A., Khamis, M. & Alt, F.: Don't Use Fingerprint, it's Raining! How People Use and Perceive Context-Aware Selection of Mobile Authentication. Proceedings of the 2020 International Conference on Advanced Visual Interfaces, Association for Computing Machinery, 2020

Radiah, R., Maekelae, V., Hassib, M. & Alt, F.: Understanding Emotions in Virtual Reality. Proceedings of the 1st CHI Workshop on Momentary Emotion Elicitation and Capture, 2020

Rittenbruch, M., Schroeter, R., Wirth, F. & Alt, F.: An Exploratory Physical Computing Toolkit for Rapid Exploration and Co-Design of On-Bicycle User Interfaces. Proceedings of the 2020 ACM Conference on Designing Interactive Systems, ACM, 2020

Rivu, S. R. R., Abdrabou, Y., Pfeuffer, K., Esteves, A., Meitner, S. & Alt, F.: StARe: Gaze-Assisted Face-to-Face Communication in Augmented Reality. Proceedings of the 2020 ACM Symposium on Eye Tracking Research & Applications, ACM, 2020

Rivu, R., Abdrabou, Y., Pfeuffer, K., Hassib, M. & Alt, F.: Gaze'N'Touch: Enhancing Text Selection on Mobile Devices Using Gaze. Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, ACM, 2020

Saad, A., Rodriguez, S. D., Heger, R., Alt, F. & Schneegass, S.: Understanding User-Centered Attacks In-The-Wild. Proceedings of the 1st CHI Workshop on Authentication Beyond Desktops and Smartphones, 2020

Research Projects

ubihave

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

Funded by: DFG
Duration: 01/2019 – 07/2021

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 behaviors, different physicalities, and changing sensing and interaction capabilities.

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

PhD Projects

Michael Braun
Affective Automotive User Interfaces

This dissertation explores affective automotive user interfaces and contributes two basic interaction paradigms: firstly, emotion-aware systems react to the current emotional state of the user based on live sensing data, hence allowing quick interventions; and secondly, emotional interaction synthesizes experiences which resonate with the user on an emotional level. The goals of these two approaches are the promotion of safe behavior and an improvement of user experience.

Eva Lösch
Supporting the Exploration of Multi-user Interactive Information Boards in (Semi-) Public Spaces (In German)

This dissertation develops a concept for supporting the exploration of interactive multi-user information displays in (semi-) public spaces. The concept is based on the use of visual stimuli to guide the attention and behavior of users during exploration. In a total of three studies, this concept was evaluated and iteratively improved, providing satisfactory support to users at all stages of exploration.

Teaching

11671 Human-Computer Interaction

11672 Project Human-Computer Interaction

36651 Usable Security

36653 Design of Secure and Usable Systems Lab

3665-V1 Secure Human-Machine Interfaces

Fairs, Conferences, Seminars

Mensch und Computer 2020

August 6–9, 2020, Magdeburg, Germany

The Mensch und Computer conference is the largest European HCI conference, bringing together researchers and practitioners in a 4-day event, including different tracks and workshops.

Workshop on Authentication beyond Desktops and Smartphones (in Conjunction with the ACM Conference on Human Factors in Computing Systems (CHI 2020))

The goal of this workshop is to develop a common understanding of challenges and opportunities smart devices and environments create for secure and usable authentication.

EyeSec: 1st Workshop on Eye-Gaze for Security Applications (in Conjunction with the 12th ACM Symposium on Eye Tracking Research and Applications (ETRA2020))

Eye movements are subtle and thus attractive for security and privacy purposes. The EyeSec workshop allows researchers and practitioners to explore directions for future research in this field.

How to Do HCI research if your Users Are Off-limits?

In this online event we shared experiences on how to move our research forward during times where people around the world are staying home and we cannot interact with them personally. Moderator: Prof. Florian Alt.

How to Make Remote HCI Teaching Useful, Engaging and Exciting? Is your Online Course Really Better than a Book?

In this format we brought together HCI educators and authors with varying backgrounds to discuss what strategies we have to make teaching and learning enjoyable – even if we cannot teach face-to-face. Moderator: Prof. Florian Alt.

Patents, Prizes, Awards

Best of CHI Honorable Mention Award

C. Katsini, Y. Abdrabou, G. Raptidis, M. Khamis, and F. Alt. The Role of Eye Gaze in Security and Privacy Applications: Survey and Future HCI Research Directions. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20), Association for Computing Machinery, New York, NY, USA, 2020. doi:10.1145/3313831.3376840

Additional Functions

Program Committee

- 2020 European Workshop on Usable Security (EuroUSEC 2020) (Member)
- 3rd International Conference on Artificial Intelligence & Virtual Reality (AIVR 2020) (Member)
- ACM Human Factors in Computing Systems (Subcommittee Chair)
- Augmented Humans 2020 (Member)
- GI Sicherheit 2020 (Member)
- Mensch und Computer 2020 (Technical Program Chair)

Cooperations

University of Duisburg-Essen: Behavioral Biometrics

Together with Prof. Dr. Stefan Schneegass, we are investigating in the Scalable Biometrics project how behavioral biometric approaches scale under changes in environment and technology.

Technical University of Darmstadt (Telecooperation Lab): Mental Models in Smart Homes

In a joint research project with Karola Marky M.Sc. and Prof. Dr. Max Mühlhäuser we investigate the mental models of users as well as visitors in smart homes, especially with respect to their understanding of data collection and storage.

University of Glasgow: Use of Eye Tracking for Usable Security

With Dr. Mohamed Khamis, we are working on the development of novel security mechanisms based on eye tracking and investigating how existing systems can be improved in terms of security and usability using gaze information.

Lancaster University: Investigating End-of-Life Scenarios for IoT Devices

Together with Ludwig Trotter M.Sc. and Prof. Nigel Davies, we are investigating user experiences in the context of the Internet of Things (IoT) — in particular cases where users have been permanently or temporarily restricted in their use of or access to IoT devices (for example, through discontinuation of the product/service by the manufacturer).

University of Lisbon: Gaze Behavior in Virtual Reality

Together with Prof. Augusto Esteves (Instituto Superior Técnico), we are exploring the benefits of physiological user interfaces in the context of personal headsets and augmented reality glasses, specifically adaptive user interfaces, personalized information, and new input capabilities.

University of Munich: User Interfaces for Cryptocurrencies

Together with Prof. Dr. Albrecht Schmidt from Media Informatics, we are working on improving the usability of user interfaces for cryptocurrencies. In particular, we develop novel interface concepts and interaction techniques considering different threat models.

Prof. Dr. Harald Baier

Digital Forensics

Teaching

3824	**Digitale Forensik**

Fairs, Conferences, Seminars

- CAST Workshop Forensik/Internetkriminalität, Dec. 10, 2020, cast-forum.de/workshops/infos/292?ts=1623997236497

Cooperations

- National Research Center for Applied Cybersecurity ATHENE
- Darmstadt University of Applied Sciences
- Technical University of Darmstadt
- Friedrich-Alexander University Erlangen-Nürnberg
- Frankfurt University of Applied Sciences
- Vietnamese German University
- Hessen State Office of Criminal Investigations (HLKA)
- Central Office for Information Technology in the Security Sector (ZITiS)

Prof. Dr. Stefan Brunthaler

Secure Software Engineering

Publications

Desharnais, M. & Brunthaler, S. A: Generic Framework for Verified Compilers Using Isabelle/HOL's Locales. In Journées Francophones des Langages Applicatifs (JFLA), Gruissan, France, January 29–February 1, 2020.

Desharnais, M. and Brunthaler, S.: Towards Efficient and Verified Virtual Machines for Dynamic Languages. In CPP'21, co-located with POPL'21. January 2021.

Research Projects

Airborne Cyber Security Enhancement

The Research Institute CODE collaborates with Airbus DS on comprehensive research understanding and addressing cyber-security 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

Teaching

1009	**Seminar Selected Chapters from Programming Languages**
1009	**Seminar Voice-based Security**
3584	**Internship Language-based Security**
3647	**Compiler Construction**
55071	**Language-based Security**

Fairs, Conferences, Seminars

CODE Colloquium Organizer

The CODE Colloquium is a distinguished speaker series where we invite internationally acclaimed speakers to give talks, discuss current and future research goals and talk to grad students.

Additional Functions

- Faculty Council Member
- Vice Dean
- Head of the Examination Board for Cybersecurity Studies

Cooperations

Mathias Payer, EPFL

Stijn Volckaert, KU Leuven

Prof. Dr. Gabi Dreo Rodosek

Communication Systems and Network Security

Publications

Dietz, C., Dreo, G., Sperotto, A. & Pras, A.: Towards Adversarial Resilience in Proactive Detection of Botnet Domain Names by using MTD. NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium, 2020, 1–5

Dreo, G., Eiseler, V., gentschen Felde, N., Gehrke, W., Helmbrecht, U. & Zahn, J., Hommel, W.: Europäische Digitale Souveränität: Weg zum Erfolg? – Ein Bericht zur Jahrestagung CODE 2020. In: Zeitschrift für Außen- und Sicherheitspolitik, Springer, 2020, 13

Hermelink, J., Pöppelmann, T., Stöttinger, M., Wang, Y. & Wan, Y.: Quantum safe authenticated key exchange protocol for automotive application. 18th escar Europe Conference, 2020

Junker, M. & Rodday, N.: Tutorial: Reliable measurements with BGP and RPKI. NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, 2020

Knüpfer, M., Bierwirth, T., Stiemert, L., Schopp, M., Seeber, S., Pöhn, D. & Hillmann, P.: Cyber Taxi: A Taxonomy of Interactive Cyber Training and Education Systems. 2nd Workshop on Model-driven Simulation and Training Environments for Cybersecurity (MSTEC), Springer International Publishing, 2020, 3–21

Mäurer, N., Gräupl, T., Gentsch, C. & Schmitt, C.: Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS. 2020 AIAA/ IEEE 39th Digital Avionics Systems Conference (DASC), 2020, 1–10

Perner, C. & Schmitt, C.: Security Concept for Unoccupied Aerial Systems. 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), 2020, 1–8

Perner, C., Schmitt, C. & Carle, G.: Dynamic Network Reconfiguration in Safety-Critical Aeronautical Systems. 2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC), 2020, 1–8

Poschinger, R., Rodday, N., Labaca-Castro, R. & Dreo, G.: OpenMTD: A Framework for Efficient Network-Level MTD Evaluation. Proceedings of the 7th ACM Workshop on Moving Target Defense, Association for Computing Machinery, 2020, 31–41

Pöhn, D. & Hommel, W.: IMC: A Classification of Identity Management Approaches. European Symposium on Research in Computer Security, Springer, 2020, 3–20

Pöhn, D. & Hommel, W.: An overview of limitations and approaches in identity management. Proceedings of the 15th International Conference on Availability, Reliability and Security, Association for Computing Machinery, 2020, 1–10

Rodday, N., van Baaren, R., Hendriks, L., van Rijswijk-Deij, R., Pras, A. & Dreo, G.: Poster: Evaluating RPKI ROV identification methodologies in automatically generated mininet topologies. Proceedings of the 16th International Conference on emerging Networking Experiments and Technologies, Association for Computing Machinery, 2020, 530–531

Steuber, F., Schoenfeld, M. & Dreo Rodosek, G.: Topic Modeling of Short Texts Using Anchor Words. Proceedings of the 10th International Conference on Web Intelligence, Mining and Semantics (WIMS'20), Association for Computing Machinery, 2020

Streit, K. & Dreo Rodosek, G.: CeTUP: Controller-Equipped Topology Update Process for Tactical Ad-Hoc Networks. Proceedings of the 17th ACM Symposium on Performance Evaluation of Wireless Ad Hoc, Sensor, & Ubiquitous Networks, Association for Computing Machinery, 2020, 57–66

Streit, K., Viehmann, E., Steuber, F. & Dreo Rodosek, G.: Improving Routing with Up-to-date and Full Topology Knowledge in MANETs 2020. Military Communications and Information Systems Conference (MilCIS), 2020, 1–8

Streit, K., Schmitt, C. & Giannelli, C.: SDN-Based Regulated Flow Routing in MANETs. 2020 IEEE International Conference on Smart Computing (SMARTCOMP), 2020, 73–80

Research Projects

BGM Tool

Development of a scientifically usable booking and reporting tool in the context of occupational health management measures in the Federal Ministry of Defence (BMVg).

Funded by: Medical Academy of the Bundeswehr (SanAkBw)
Duration: 04/2018 – 12/2020

BMBF Joint Project BERKoS

Development of a knowledge community platform with the aim of supporting German applicants in obtaining European funding in the field of general security research.

Funded by: Federal Ministry of Education and Research (BMBF), VDI-Technologiezentrum GmbH
Duration: 06/2017 – 02/2021

Cyber Range

Design and effective use of cyber ranges related to cyber technology development, system testing, and training of network administrators, network operators, and IT security personnel.

Funded by: BMVg, BAAINBw
Duration: 2018 – 06/2023

FLIP – Flexible IP Waveform

Creation of a modular waveform with individual, flexibly interchangeable components, with the aim of enabling high-performance secure data transmission adapted to the actual conditions.

Funded by: BMVg, BAAINBw
Duration: 03/2017 – 04/2021

Horizon 2020 Project CONCORDIA

Establishing a cybersecurity competence network with leading capacities in research, technology, industry and public. CONCORDIA provides excellence and leadership in technology, processes and services to create a usercentric, EU-integrated cybersecurity ecosystem for EU digital sovereignty.

Funded by: European Commission (EC)
Duration: 01/2019 – 12/2022

IT Trend Monitoring from a Research Perspective for the BAAINBw

Worldwide monitoring of innovative IT security trends from a research perspective and analysis of their potential for the future, as well as holding an annual Cyber R&T Symposium.

Funded by: BAAINBw
Duration: 02/2018 – 11/2021

Microkernel for IT Security-related Applications

Design and testing of software engineering approaches for the integration of secure and verifiable microkernels in IT security applications and secure IT systems.

Funded by: Airbus Defence and Space
Duration: 09/2019 – 12/2023

Moving Target Defence

The goal is to identify, evaluate, select, and further develop network-based moving target defense technologies, while also establishing a strong academic research community in the field of MTD.

Funded by: BMVg, BAAINBw
Duration: 2018 – 06/2023

Postquantum Cryptography

Analysis and development of cryptographic algorithms in the field of post-quantum cryptography.

Funded by: Infineon Technologies
Duration: 05/2019 – 03/2023

TDL with National Domains

Analysis and evaluation of security issues in the implementation of tactical data links and development of procedures to automate the implementation processes.

Funded by: BAAINBw
Duration: 10/2019 – 11/2022

PhD Projects

Renners, Leonard
Adaptive Prioritization of Network Security Incidents

With the ever rising amount of security and alert information in IT, incident prioritization becomes increasingly important, and is therefore nowadays part of many approaches and tools for network security. A key challenge is, however, a correct prioritization of the events. Currently, the calculation of priorities is rather static, and needs to be defined manually. Incorrect prioritization cannot be reliably or permanently avoided and leads to threatening situations and an increased effort in incident response. Furthermore, the identification of errors in the prioritization rules themselves is another challenge since there is rarely a continuous approach to monitor the prioritization process. In addition, providing corrections as well as defining new, improved rules to address the detected inaccuracies also lacks automated support and again requires manual effort.

To address these problems, this thesis proposes a concept for an adaptive prioritization of network security incidents. Our contributions are novel approaches for the prioritization with a focus on a higher degree of automation. We introduce a customizable incident model and a rule-based approach to specify incident prioritization. Furthermore, a process to gather quantitative feedback from the analyst is proposed in combination with a concept for the assessment of the prioritization rules to monitor quality and to regularly identify deficiencies. These concepts are extended and complemented by machine learning techniques for an increased automation regarding the initial creation of prioritization rules, and more importantly the adaptation of an existing set of rules. Understandability of the prioritization model, its instances and of the automation is hereby viewed as a crucial requirement to establish trust in the system for security experts and allow for a manual interaction within the different tasks if necessary. As a result our approach offers the possibility to realize a continuous improvement of the prioritization which helps to address current challenges in incident prioritization in an effective and efficient way.

Teaching

10102	Network Security
10103	Network Security Lab
10248	IT Security Lab
102412	Computer Networks Lab
11971	Computer Networks
11972	Mobile Communication Systems
11975	Computer Networks Lab 2
38202	Quantum Computer Programming Lab
55131	Secure Mobile Systems
	Cyber Defense Seminar
	IT Security Seminar

Fairs, Conferences, Seminars

Workshop Post Quantum Crypto

On January 28, 2020, a workshop on Post Quantum Computers and Post Quantum Cryptograms was held at the Research Institute CODE in cooperation with companies Infineon and Giesecke + Devrient.

Virtual Hackathon at the IBM Q Hub at UniBwM

From March 30 to April 04, 2020, an online hackathon on quantum computing was organized at the Research Institute CODE in cooperation with colleagues from DLR and LMU.

Virtual Hackathon at the IBM-Q-Hub at UniBwM

From October 10 to 16, 2020, an online hackathon on quantum computing was organized at the Research Institute CODE in cooperation with colleagues from DLR and LMU.

Patents, Prizes, Awards

Awarding research assistants Raphael Labaca Castro and Sinclair Schneider, whose papers "Adversarial Camouflage: Adversarial Machine Learning as Concealment for Military Operations" and "Intelligent News Analysis" were among the top 10 submissions at the CODE 2020 Innovation Day.

Additional Functions

- Executive Director of the Research Institute CODE
- Member of the Digital Council of the Federal Ministry of Defence (BMVg)
- Member of the Advisory Board and Supervisory Board of Giesecke+Devrient GmbH
- Member of the Supervisory Board of Siltronic AG
- Member of the Data Privacy Advisory Board of Deutsche Telekom AG
- Member of the Supervisory Board of BWI GmbH
- Member of the Global Future Council on Cybersecurity of the World Economic Forum
- Member of the National Cybersecurity Council Scientific Working Group
- Member of the Board of Trustees of the Kunsthalle
- Member of the Board of Directors of Sicherheitsnetzwerk München e.V.
- Member of the BaFin IT Expert Panel
- Member of the Advisory Board of Deutschland sicher im Netz (DsiN) e.V.
- Coordinator of the EU project CONCORDIA
- Member of the Münchner Kreis
- Member of the Bavarian Business Advisory Council
- Member of the Münchner Klub
- Reviewer for EU Horizon 2020 projects
- Member of the Munich Security Conference Security Innovation Board

Cooperations

University of Twente (NL)

The scientific cooperation has existed for several years and includes the exchange of scientific personnel, the joint work on research projects, as well as the planning and realization of teaching and training events. There is also a cooperation for the joint implementation of PhD projects (Joint PhD program).

Technical University of Munich

Intensive collaboration with Prof. Dr. Wolfgang Kellerer's Chair is taking place in the areas of Internet of Things (IoT) and 5G. A jointly used research infrastructure is being established here.

Munich Network Management Team (MNM Team)

The Chair is a member of the MNM Team. The Munich Network Management Team (MNM Team) is a research group of scientists at the LMU, the TU München, the LRZ and the Universität der Bundeswehr München (UniBw M). The main research interests of the MNM team are in the area of networked systems management. Recent work focuses on architectures for integrated network and system management as well as implementations of solutions for specific areas of IT management, such as configuration, accounting, and error management.

Central Office for Information Technology in the Security Sector (ZITiS)

Current joint research projects with the Chair are in the areas of IoT/5G, analysis and evaluation of vehicle data and in the area of quantum communication.

Infineon

There is close cooperation and scientific exchange with Infineon in the field of post-quantum cryptography. There are already joint projects being worked on in this field.

Airbus Defence and Space

Joint projects on secure, verifiable microkernels and their use in secure cloud infrastructures are being carried out with Airbus Defence and Space. Furthermore, a joint scientific exchange in the field of European digital sovereignty with a focus on the development of sovereign cloud solutions is envisaged.

CGI

The RI CODE and the CGI cooperate in promoting scientific exchange, joint projects and PhD positions in the field of network security/ IT security. A cooperation agreement has already been signed.

Prof. Dr. Michaela Geierhos

Data Science

Publications

Bäumer, F. S., Kersting, J., Buff, B. & Geierhos, M.: Tag Me If You Can: Insights into the Challenges of Supporting Unrestricted P2P News Tagging. Information and Software Technologies: 26th International Conference, ICIST 2020, Kaunas, Lithuania, October 15–17, 2020, Proceedings, Springer, 2020, 368–382

Buff, B., Kersting, J. & Geierhos, M.: Detection of Privacy Disclosure in the Medical Domain: A Survey. Proceedings of the 9th International Conference on Pattern Recognition Applications and Methods (ICPRAM 2020), SCITEPRESS, 2020, 630–637

Geierhos, M., in: Gronau, N., Becker, J., Kliewer, N., Leimeister, J. M. & Overhage, S. (Ed.): Crawler (fokussiert / nicht fokussiert) Enzyklopädie der Wirtschaftsinformatik Online-Lexikon, GITO-Verlag, 2020

Geierhos, M., in: Gronau, N., Becker, J., Kliewer, N., Leimeister, J. M. & Overhage, S. (Ed.): Webmonitoring. Enzyklopädie der Wirtschaftsinformatik Online-Lexikon, GITO-Verlag, 2020

Geierhos, M., in: Gronau, N., Becker, J., Kliewer, N., Leimeister, J. M. & Overhage, S. (Ed.): Text Mining. Enzyklopädie der Wirtschaftsinformatik Online-Lexikon, GITO-Verlag, 2020

Geierhos, M., in: Gronau, N., Becker, J., Kliewer, N., Leimeister, J. M. & Overhage, S. (Ed.): Sentimentanalyse. Enzyklopädie der Wirtschaftsinformatik Online-Lexikon, GITO-Verlag, 2020

Hadersbeck, M., Ullrich, S., Still, S. & Pichler, A.: Spielräume bei der retroperspektivischen Analyse der Wittgenstein-Edition und die Herausforderungen für das Semantic Clustering. Spielräume: Digital Humanities zwischen Modellierung und Interpretation, 7. Tagung des Verbands Digital Humanities im deutschsprachigen Raum e.V., 2020

Kersting, J. & Geierhos, M.: Neural Learning for Aspect Phrase Extraction and Classification in Sentiment Analysis. Proceedings of the 33rd International Florida Artificial Intelligence Research Symposium (FLAIRS) Conference, AAAI, 2020, 282–285

Kersting, J. & Geierhos, M.: Aspect Phrase Extraction in Sentiment Analysis with Deep Learning. Proceedings of the 12th International Conference on Agents and Artificial Intelligence (ICAART 2020) – Special Session on Natural Language Processing in Artificial Intelligence (NLPinAI 2020), SCITEPRESS, 2020, 391–400

Kersting, J. & Geierhos, M.: What Reviews in Local Online Labour Markets Reveal about the Performance of Multi-Service Providers. Proceedings of the 9th International Conference on Pattern Recognition Applications and Methods, SCITEPRESS, 2020, 263–272

Research Projects

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

This subproject deals with different types of requirement specifications which enable the successful search, composition, and analysis of services. In terms of agile, participative software development, end users will be more involved in the interactive composition of software services to be created on-the-fly. This dialog is to be conducted by a domain-specific chatbot, which will be used on the one hand for targeted inquiries and on the other for resolving ambiguities. For this purpose, the dialog-based requirement compensation and natural language service explanation are the main challenges to be tackled, as deficits in requirements specifications cannot always be compensated automatically and users do not know which requirements resulted in a service.

Funded by: German Research Foundation (DFG)
Duration: 07/2019 – 06/2023

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

The aim of the subproject is to automatically monitor selected apps and analyze the data they collect, correlate it with social media profiles, and form networks/clusters of people in order to identify potential targets of cyberattacks and classify their risk potential on the basis of the given data. If this data is further correlated with other classified data (e.g., from security authorities or military agencies), a threat plausibility for corresponding persons (target groups) or locations can be estimated. Due to the risk involved, the findings generated from this require highly secure encryption when transmitted to other services.

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

Teaching

3851	Information Retrieval
3852	Data Science Applications
3853	Analysis of Unstructured Data

Additional Functions

- Elected member of the German Biography advisory board of the Historical Commission at the Bavarian Academy of Sciences and Humanities
- Member of the Development Council of CLARIAH-DE
- Expert for the European Commission, the Fraunhofer Gesellschaft, the German Academic Exchange Service (DAAD), the Alexander von Humboldt Foundation, and the Federal Ministry of Justice and Consumer Protection

Program Committee

- AAAI 2020 – 34th AAAI Conference on Artificial Intelligence
- EMNLP 2020 – The 2020 Conference on Empirical Methods in Natural Language Processing
- IoTBDS 2020 – 5th International Conference on Internet of Things, Big Data and Security
- SEMANTiCS 2020 – 16th International Conference on Semantic Systems

Peer Review

- Human-centric Computing and Information Sciences
- Journal of Business Research
- Multimedia Tools and Applications

Cooperations

FH Bielefeld, Dr. Frederik S. Bäumer

Automatic identification and highlighting of privacy-threatening text sequences with explanation of the possible risks.

Ludwig-Maximilians-Universität München, Prof. Dr. Hinrich Schütze

Offering a two-week summer school on information retrieval for students of computer science and computational linguistics.

MSH Medical School Hamburg, Prof. Dr. Mathias Kauff

Collaborative research in textual detectability of psychological effects in user-generated content with a focus on patients' opinions

Prof. Dr. Wolfgang Hommel

Software and Data Security

Publications

Fietkau, J. & Stojko, L.: A system design to support outside activities of older adults using smart urban objects. Proc. Europ. Conf. on Computer-Supported Cooperative Work 2020, EUSSET, 2020

Hanauer, T. & Hommel, W.: Enhancing Enterprise IT Security with a Visualization-Based Process Framework. In: Thampi, S., Martinez Perez, G., Ko, R. & Rawat, D. (Eds.), Proceedings of 7th International Symposium on Security in Computing and Communications, Springer Singapore, 2020

Hommel, W. & Steinke, M.: Rückgrat oder Archillesferse? Systematisches Vorgehen bei der Einführung technischer und organisatorischer IT-Sicherheitsmaßnahmen. KU Gesundheitsmanagement, 2020, 07/2020

Hommel, W. & Steinke, M.: Mehr Schutz für Patientendaten – Zur IT-Sicherheit in Krankenhäusern und Arztpraxen. Magazin Gesundheit und Gesellschaft (G+G), 2020, 07/2020

Hommel, W. & Steinke, M.: Prometheus zahlt kein Lösegeld. Management und Krankenhaus, 2020, 12/2020

Knüpfer, M., Bierwirth, T., Stiemert, L., Schopp, M., Seeber, S., Pöhn, D., Hillmann, P., Hatzivasilis, G. & Ioannidis, S. (Eds.): Cyber Taxi: A Taxonomy of Interactive Cyber Training and Education Systems. Model-driven Simulation and Training Environments for Cybersecurity, Springer International Publishing, 2020, 3–21

Pöhn, D. & Hommel, W.: An Overview of Limitations and Approaches in Identity Management. Proceedings of the 15th International Conference on Availability, Reliability and Security, Association for Computing Machinery. 2020.

Pöhn, D. & Hommel, W.: IMC: A Classification of Identity Management Approaches. Proceedings of ESORICS 2020 Workshops – DETIPS 2020: The Interdisciplinary Workshop on Trust, Identity, Privacy and Security in the Digital Economy, Springer International Publishing, 2020

Steinke, M., Brunner, S., Eiseler, V., Hofmann, J., Hofmann, M., Hommel, W., Langer, U. & Riedl, J.: Maßnahmenkatalog zur Verbesserung der IT-Sicherheit in Bayerischen Krankenhäusern, Ausgabe 2020/2021. Universität der Bundeswehr, Forschungsinstitut Cyber Defence (CODE), 2020

Stojko, L.: Intercultural usability of large public displays Adjunct Proceedings of the 2020 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2020 ACM International Symposium on Wearable Computers, ACM, 2020, 218–222

Stojko, L., Fietkau, J. & Koch, M.: Design Guidelines for Micro Information Radiators to increase Seniors' Safety in Urban Space. Proc. Mensch und Computer 2020, 2020

Research Projects

Airborne Cyber Security Enhancement

Research Institute CODE collaborates with Airbus DS on comprehensive research understanding and addressing cyber-security 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 & Space, Manching
Duration: 2020 – 2024

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 will be incorporated into a catalog of measures to further increase the security level, which is currently available in the 2020/21 edition.

Funded by: Bavarian Ministry of Health and Care (StMGP)
Duration: 10/2018 – 09/2021

Digital Identities for Service Accounts: Implementation Strategies, Guidelines and Security Aspects (DISKURS)

The project provides scientific support for the establishment and operation of the national identity federation FINK, which enables the use of online administrative services across the German federal states. In addition, relevant future systems based on self-sovereign identity will be investigated and their possible integration into the existing federation will be demonstrated.

Funded by: Bavarian State Ministry of Digital Affairs (StMD)
Duration: 12/2019 – 03/2021

Teaching

1006	Introduction to Computer Science 1
1007	Introduction to Computer Science 2
3459	Selected Chapters of IT Security
5501	Seminar Information Security in Healthcare
5507	Secure Networked Applications
5508	Security Management

Prof. Dr. Johannes Kinder

Program Analysis, Transformation, Comprehension, and Hardening (PATCH)

Publications

Bouvier, P., Garavel, H. & de León, H. P.: Automatic Decomposition of Petri Nets into Automata Networks – A Synthetic Account. Proc. 41st Int. Conf. Application and Theory of Petri Nets and Concurrency (Petri Nets), Springer, 2020, 12152, 3–23

Lehmann, D., Kinder, J. & Pradel, M.: Everything Old is New Again: Binary Security of WebAssembly. 29th USENIX Security Symposium (USENIX Security), USENIX Association, 2020, 217–234

Patrick-Evans, J., Cavallaro, L. & Kinder, J.: Probabilistic Naming of Functions in Stripped Binaries. Proc. 35th Annu. Computer Security Applications Conference (ACSAC), ACM, 2020, 373–385

Ponce de León, H., Furbach, F., Heljanko, K. & Meyer, R.: Dartagnan: Bounded Model Checking for Weak Memory Models (Competition Contribution). Proc. Tools and Algorithms for the Construction and Analysis of Systems (TACAS), Springer, 2020, 12079, 378–382

Research Projects

Efficient Automatic Security Testing for Dynamic Languages

Dynamic programming languages like JavaScript lie at the foundation of the worldwide web, running both in web browsers and on servers. While in JavaScript it is easy to quickly bootstrap new features, websites, and systems, it is also easy to make mistakes. In the EASTEND project (Efficient Automatic Security TEstiNg for Dynamic languages) we devise new methods to automatically find mistakes in JavaScript programs.

Funded by: UK Government & Engineering and Physical Sciences Research Council (EPSRC)
Duration: 09/2015 – 02/2020

Reverse Engineering meets Deep Learning

Computer programs are written in source code. For execution, they are compiled into a binary form unreadable to humans. Because the source code is not available in many situations, it is difficult for human reverse engineers to judge the behavior of a binary program. Our machine learning system is trained to label components in binaries with names that are similar to those in the original source code, aiding human analysis.

Funded by: Engineering and Physical Sciences Research Council (EPSRC) & Research Institute CODE
Duration: since 10/2016

PhD Projects

Blake Loring
Practical Dynamic Symbolic Execution for JavaScript

In this thesis we develop a practical and scalable approach to dynamic symbolic execution (DSE) of JavaScript programs and prove its effectiveness by implementing ExpoSE, our new DSE engine. ExpoSE uses program instrumentation to implement DSE, enabling analysis of both web applications and Node.js software while also allowing quick support of the latest JavaScript standards. We detail novel encodings of regular expressions, objects, and arrays which allow ExpoSE to analyze programs out of scope of prior work. In particular, we present the first complete encoding of ES6 regular expressions, including symbolic support of capture groups and backreferences. We show the effectiveness of our design through two case studies. In the first study we show that our approach is able to generate a suite of supplementary conformance tests for JavaScript standard library methods that further the official JavaScript testing suite Test262. Test cases are generated through symbolic exploration of polyfill implementations and verified with differential testing. In the second case study we use DSE to automatically deduce what conditions trigger resource loading, enabling our new Oblique speculative loading approach, a proxy which reduces page load times by sending resources before a client requests them.

Claudio Rizzo
Static Flow Analysis for Hybrid and Native Android Applications

In this thesis, we propose new techniques to enable existing analyses to consider the multi-language nature of an Android application. First, we focus on Android Webviews. To this end, we developed BabelView, a tool that uses information flow analysis to assess the security of Webviews. Our idea is that we can make reasoning about JavaScript semantics unnecessary by instrumenting the application with a model of possible attacker behavior — the BabelView. We evaluated our approach on a sample of 25,000 apps from the Google Play Store, finding 10,808 potential vulnerabilities in 4,997 apps, having over 3 billion installations worldwide. We manually validated BabelView on a sample of 50 apps and estimated our fully automated analysis achieves a precision of 81 % at a recall of 89 %.

Second, we focus on enabling analyses for Android native code. We created a new framework, JniFuzzer, which enables fuzzing for Android JNIs. We used JniFuzzer on real-world Android apps, finding potential vulnerabilities that we report as case studies. We then developed TaintSavior, a Proof of Concept (PoC) tool which uses a black-box approach to generate summaries for JNIs.

We implemented TaintSavior as a JniFuzzer plug-in, and we present a preliminary evaluation showing that our approach is viable and practical.

Teaching

38191	Reverse Engineering
38192	Reverse Engineering Lab
55011	Software Hardening Seminar
55011	Seminar Machine Learning in Reverse Engineering & Malware Detection
55101	Dynamic Program Analysis
55102	Static Program Analysis
55103	Fuzzing Lab

Fairs, Conferences, Seminars

General Chair

- 26th ACM Conference on Computer and Communications Security (CCS), November 11-15, 2019, in London, UK

Additional Functions

- Advisory Board Member, Centre for Doctoral Training in Cyber Security for the Everyday, Royal Holloway, University of London
- PhD reviever for Ivan Radiček, Faculty of Computer Science, TU Wien
- Expert Code Review at WTD-81, Greding

Cooperations

- Universität Stuttgart, Prof. Dr. Michael Pradel and Daniel Lehmann. Studying the security and attack surface of Web Assembly binaries compared to JavaScript and native x86/x64 code.
- King's College London, Prof. Lorenzo Cavallaro. Building machine learning classifiers to predict function names in binaries.

Prof. Dr. Gunnar Teege

Formal Methods for Securing Things (FOMSET)

Research Projects

Highly Secure Operating Systems for Embedded IT (HoBIT)

Basic principles for the development of highly reliable and highly secure operating systems are investigated and basic technologies are prototyped. Basic investigations are carried out on an exemplary target system on the basis of the existing seL4 microkernel. For a later implementation, suitable tools and post-verification possibilities will also be investigated.

Funded by: Bavarian Ministry of Economic Affairs, Regional Development and Energy
Duration: 01/2018 – 09/2020

Extension of the Basics for Formal Verification of Software and its Application (SW_GruVe)

For the approval of IT systems, the tools with which the systems are created are also evaluated with increasing approval requirements. In this project, corresponding quality requirements are evaluated, tools for formal verification are further developed and particularly safety-critical operating system components are formally verified as examples.

Funded by: Bavarian Ministry of Economic Affairs, Regional Development and Energy
Duration: 10/2020 – 09/2022

Microkernel for IT Security Relevant Applications

Secure startup process architectures are investigated for the application of microkernels in static and cloud-based high-security applications. Available solution approaches are analyzed and evaluated and prototypically implemented in the context of a static gateway and a cloud system.

Funded by Airbus CyberSecurity GmbH
Duration: 12/2020 – 12/2023

Teaching

5505	Operating System Security

Cooperations

- CSIRO Dat61, Canberra, Australia
- Hensoldt Cyber GmbH, Taufkirchen
- Technical University of Munich

Prof. Dr. Arno Wacker

Privacy and Compliance

Publications

Megyesi, B., Esslinger, B., Fornés, A., Kopal, N., Láng, B., Lasry, G., Leeuw, K. d., Pettersson, E., Wacker, A. & Waldispühl, M.: Decryption of historical manuscripts: the DECRYPT project. Cryptologia, Taylor & Francis, 2020, 1-15

Research Projects

Redundant Structures in Fully Distributed Overlay Networks

This research topic 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.

DECRYPT: 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. This will result in faster progress in decoding and contextualizing historical encrypted manuscripts, hitherto buried in archives and libraries.

Funded by: Swedish Research Council (SRC)
Duration: 01/2019 – 12/2024

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

Internationality

The RI CODE maintains a large network worldwide. In 2020, the employees came from 14 countries. There were 79 cooperation partners in 28 countries.

FIG.: ISTOCK / BLUE PLANET STUDIO

Employees

Nationality
Argentina
Austria
Bangladesh
Benin
Brazil
Bulgaria
Canada
Croatia
Egypt
Finland
Germany
Great Britain
Republic of Korea
Spain

International Cooperation Partners

Country	Partner
Australia	CSIRO Data 61
	Queensland University of Technology
	University of Melbourne
	University of New South Wales
Austria	SBA Research
	Software Competence Center Hagenberg
Belgium	EIT Digital
	KU Leuven
Canada	University of Waterloo
China	Xidian University
Cyprus	Cyprus University of Technology
Czech Republic	Flowmon Networks
	Masaryk University
Egypt	German University Cairo
Finland	Aalto University
	University of Lapland
	University of Oulu
France	Centre de Recherche de l'École de l'Air (CREA)
	CyberDetect
	INRIA / Université de Lorraine
	INRIA / Université de Toulouse
	Institut Politechnique de Paris
	Université Catholique de l'Ouest (UCO)
Great Britain	Heriot Watt University
	Imperial College London
	King's College London
	Lancaster University
	Royal Holloway, University of London
	University of Glasgow
Greece	ATHENA Research
	Center Human Opsis
	Foundation for Research and Technology Hellas
	National Cyber Security Authority of the Ministry of Digital Governance
	University of Patras
Hungary	Eötvös Loránd University
Ireland	Cork Institute of Technology
Israel	Ben-Gurion University of the Negev
Italy	Centro Ricerche Fiat
	Telecom Italia
	University of Insubria
	University of Milan
	Università degli Studi di Palermo
Luxembourg	University of Luxembourg
Netherlands	Arthur's Legal B.V.
	SIDN
	SURFnet
Netherlands	TU Eindhoven
	University of Twente
	VU Amsterdam
Norway	Norwegian University of Science and Technology
	Oslo Metropolitan University
	Telenor Group
	University of Oslo
Portugal	Efacec Electric Mobility
	Universidade de Lisboa
Republic of Korea	Korea Institute of Science and Technology Information (KISTI)
Romania	Babeș-Bolyai University
	Bitdefender
Sweden	ERICSSON
	RISE – Research Institutes of Sweden
	University of Gothenburg, Department of Languages & Literatures
	Uppsala University, Department of Linguistics and Philology
Switzerland	École Polytechnique Fédérale de Lausanne
	RUAG
	University of Zurich
Slovenia	Jožef Stefan Institute
	University of Maribor
Spain	Atos Spain S.A.
	CaixaBank
	Telefonica I+D
	Universitat Autònoma de Barcelona, Computer Vision Center
	Universidad de Cadiz
	Universidad Carlos III de Madrid
USA	Auburn University, College of Engineering
	George-Marshall-Center
	Michigan Tech
	University of California Irvine
	University of California Santa Barbara
Vietnam	Vietnamese-German University

How to Find Us

Research Institute Cyber Defence (CODE)
Universität der Bundeswehr München
Carl-Wery-Straße 22
81739 Munich
Germany

@ code@unibw.de
☎ +49 89 6004 7302 or 7303
🌐 www.unibw.de/code

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

Location Map

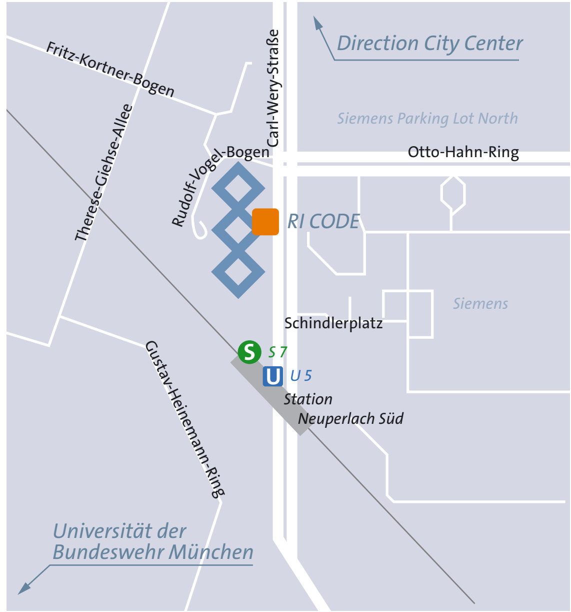


ABB.: TAUSENDBLAUWERK.DE

Imprint

Publisher

Research Institute CODE
Universität der Bundeswehr München
Carl-Wery-Str. 22
81739 Munich
Germany

Management of RI CODE

Prof. Dr. Gabi Dreo Rodosek,
Executive Director

Prof. Klaus Buchenrieder, PhD,
Technical Director (until 02/2020)

Prof. Dr. Udo Helmbrecht,
Technical Director (03/2020–01/2021)

Prof. Dr. Wolfgang Hommel,
Technical Director (since 02/2021)

Dipl.-Inf. Volker Eiseler,
Managing and Academic Director

Professors at RI CODE

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

Prof. Dr. Harald Baier,
Professor for Digital Forensics (since 09/2020)

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

Prof. Klaus Buchenrieder, PhD,
Professor für Eingebettete Systeme/
Rechner in Technischen Systemen

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

Prof. Dr. Michaela Geierhos,
Professor for Data Science (since 04/2020)

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

Prof. Dr. Gunnar Teege,
Professor for Distributed Systems

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

Members of the Advisory Board (in 2020)

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

Prof. Dr. Uwe Borghoff

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Wolfgang Hommel

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

Editing and Coordination

Prof. Dr. Michaela Geierhos,
Professor for Data Science

Lisa Scherbaum M.A.,
Public Relations Officer

Art direction

Tausendblauwerk Design Agency
Michael Berwanger
www.tausendblauwerk.de

Benjamin Bellgrau M.Sc.,
Research Associate, Chair for Data Science
(Preliminary Layout)

Proofreading

Lektorat Unker
www.unker.com

Printed by

Holzer Druck und Medien
www.druckerei-holzer.de

Regulations

Editorial Deadline: May 2021

ISBN: 978-3-943207-57-6 | ISSN: 2748-9485

Also published as an electronic publication
(ISBN: 978-3-943207-58-3 | ISSN: 2748-9507)
as well as in German language
(ISBN: 978-3-943207-55-2 | ISSN: 2748-8780).

der Bundeswehr
Universität München

RI
CODE

Research Institute
Cyber Defence
Universität der Bundeswehr München