der Bundeswehr
Universität München

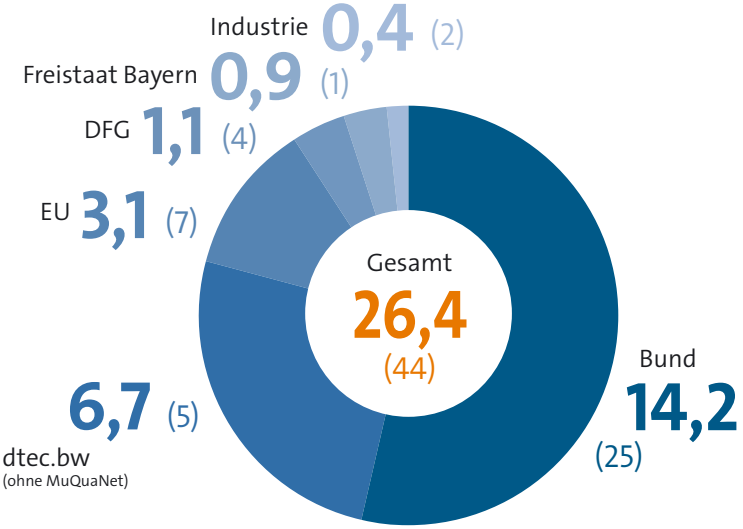
CODE
JAHRESBERICHT
2024

Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Projektförderung

2024 wurden insgesamt 44 drittmittelfinanzierte Projekte am FI CODE bearbeitet oder eingeworben. dtec.bw-Projekte erhalten Mittel aus dem Etat des Geschäftsbereichs BMVg.

Drittmittel*



* Angaben in Millionen Euro, Anzahl der Projekte in Klammern.

dtec.bw-Projekt**

MuQuaNet – Das Quanten-Internet im Großraum München

MuQuaNet
The Munich Quantum Network

Beteiligte Professuren

Prof. Dr. Wolfgang Hommel
Hon.-Prof. Dr. Udo Helmbrecht
Prof. Dr. Michaela Geierhos
Prof. Dr. Arno Wacker

** Unter Beteiligung des FI CODE mit Projektstart im Jahr 2020, nicht in der Drittmittel-Übersicht (links) enthalten.

Internationalität

Das FI CODE unterhält ein internationales Netzwerk.

Mitarbeitende***

Die Mitarbeitenden des FI CODE stammten im Jahr 2024 aus 17 Ländern.

Kooperationspartner***

Im Jahr 2024 arbeitete das FI CODE mit 76 Partnern in 26 Ländern zusammen.

Legende

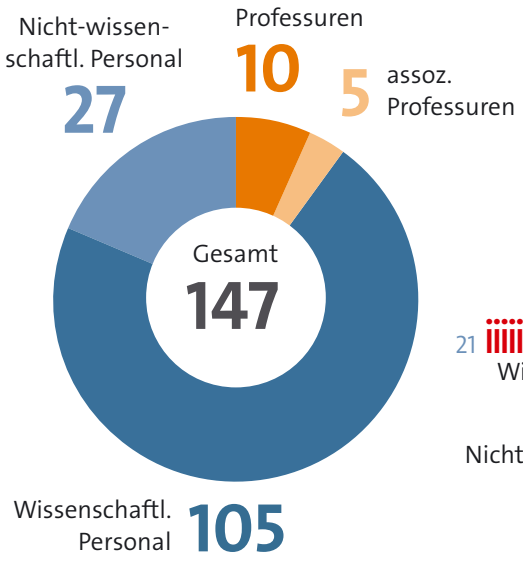
- Standort FI CODE
- 1 — Anzahl von CODE-Mitarbeitenden aus den Herkunftsländern
- 1 — Anzahl internationaler Kooperationspartner im betreffenden Land
- Länder mit Kooperationspartnern und Mitarbeitenden

*** Weitere Informationen zu Kontakten und Kooperationspartnern finden Sie ab S. 88.

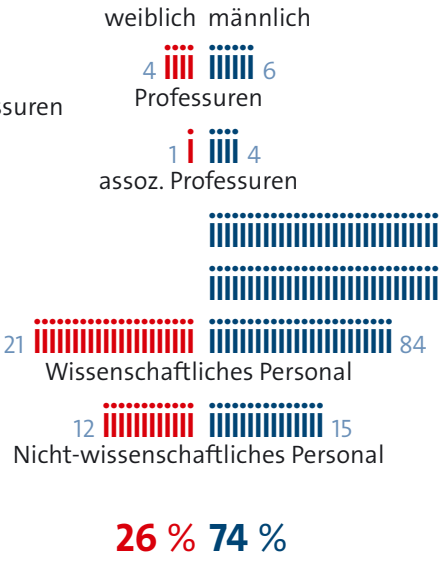
Personalstruktur

Das FI CODE hatte 2024 insgesamt 147 Mitarbeitende. Der Frauenanteil betrug 26 %.

Mitarbeitende



Geschlechteranteil



26 % **74 %**

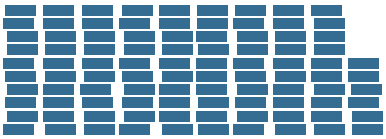
Forschungsarbeit

Übersicht der Promotionen und Publikationen am FI CODE 2024

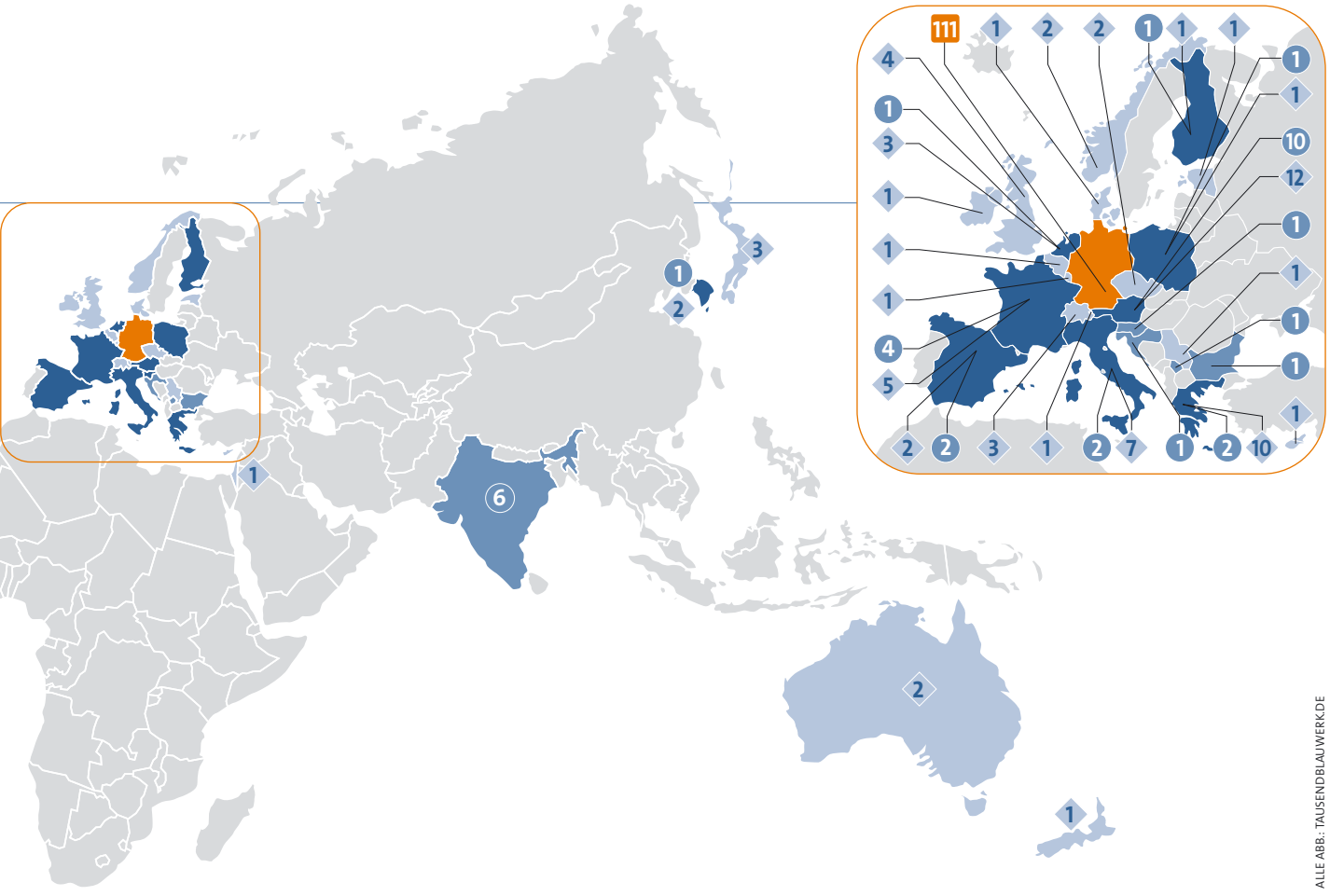
Promotionen

3

Publikationen



96



ALLE ABB.: TAUSENDBLAUWERK.DE

der Bundeswehr
Universität München

CODE
JAHRESBERICHT
2024

FI CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

Vorwort der Präsidentin

Angesichts einer zunehmend vernetzten Welt, die von geopolitischen Spannungen und der rasanten Entwicklung von Künstlicher Intelligenz geprägt ist, ist Cybersicherheit eine der größten Herausforderungen unserer Zeit. Cyberangriffe auf kritische Infrastrukturen, Unternehmen und Privatpersonen haben zugenommen und erfordern präventive Maßnahmen und innovative Lösungen. In unsicheren Zeiten wie diesen ist es unerlässlich, die Forschung im Bereich Cybersicherheit voranzutreiben und neue Technologien zu entwickeln. Mit seiner interdisziplinären Grundlagenforschung sowie anwendungsnahen Forschung in den Bereichen Cyber Defence, Smart Data und Quantum Technology leistet CODE einen unmittelbaren Beitrag für Gesellschaft und Bundeswehr und ist damit ein wesentlicher Baustein unseres Profils „Sicherheit und Nachhaltigkeit in Technik und Gesellschaft".

Das CODE forscht bereits über ein Jahrzehnt erfolgreich auf nationaler und internationaler Ebene. In 2024 wurden mit verschiedenen Partnern wieder zahlreiche Projekte durchgeführt und weiterentwickelt. Theorie und Praxis wurden verzahnt, um Forschungsergebnisse in konkrete Anwendungen umzusetzen.

Bereits seit dem Jahr 2015 arbeitet CODE mit dem Bayerischen Landeskriminalamt (BLKA) zusammen und führt u. a. Cyber Range Trainings für das Personal des BLKA sowie des Bayerischen Landesamtes für Sicherheit in der Informationstechnik durch. Um die langjährige und erfolgreiche Zusammenarbeit mit dem BLKA auszubauen, wurde Ende September 2024 eine Kooperationsvereinbarung unterzeichnet. Durch die enge Abstimmung zwischen dem BLKA und der UniBw M sollen Anforderungen und Forschungsbedarfe für die zivile Sicherheit konkretisiert und Anwendungen für zivile Sicherheit in Projektvorhaben auf nationaler und internationaler Ebene erarbeitet werden.

Ein großer Erfolg für die UniBw M bestand 2024 darin, dass wir mit unserem Palladion Defence Accelerator als einziger deutscher Accelerator für das NATO DIANA Programm ausgewählt wurden. An diesem Programm, das für Startups Zugang zu erstklassigen Forschungs- und Testeinrichtungen bietet, nimmt CODE bereits als Testcenter teil und fügt sich hervorragend in das Innovationsökosystem der UniBw M ein. Das Testcenter wird gemeinsam mit IBM Deutschland sowie Instituten der Fraunhofer-Gesellschaft organisiert und setzt seinen Schwerpunkt auf Innovationen im Bereich der Quantentechnologien.

CODE trägt dazu bei, Deutschland und die Welt sicherer zu machen, indem es innovative Lösungen für die Herausforderungen von morgen entwickelt und unsere digitale Resilienz stärkt. Ich gratuliere dem gesamten Institut zu einem abermals erfolgreichen Jahr! Freuen Sie sich auf interessante Einblicke in die Welt der Cybersicherheit!

Mit den besten Grüßen

Prof. Dr. mont. Dr.-Ing. habil. Eva-Maria Kern, MBA
Präsidentin Universität der Bundeswehr München

Wolfgang Hommel, Marcus Knüpfer, Michaela Geierhos

Liebe Leserinnen und Leser,

das Forschungsinstitut CODE verbindet an der Universität der Bundeswehr München sowohl Grundlagen- als auch anwendungsorientierte Forschung mit universitärer Lehre für die zukünftigen Fachkräfte sowie den Führungsnachwuchs der Bundeswehr und ausgewählter Bundesbehörden. Technisch spannende und gleichermaßen gesellschaftlich wie militärisch relevante Innovationen und Weiterentwicklungen in unseren Themenbereichen Cyber Defence, Machine Learning und Quantentechnologien motivieren ein tiefgehendes Technologieverständnis und lebenslanges Lernen auf der Arbeits-, aber auch der Führungs- und Entscheidungsebene, das sich auch in unseren Weiterbildungsangeboten widerspiegelt.

Im Jahr 2024 durften wir uns zum einen über die Reakkreditierung unseres Masterstudiengangs Cyber-Sicherheit samt lobender Worte über dessen Inhalte durch die externen Gutachter freuen, zum anderen zeigt die nochmals intensivierte Nutzung unserer Cyber Range beispielsweise im Rahmen der zweiwöchigen CYBER PHOENIX unsere Rolle als Praxispartner bei Training und Weiterqualifizierung.

Wie über die letzten Jahre etabliert rückt der vorliegende Jahresbericht unsere Forschungsgruppen und deren Projekte in die Mitte. Er gibt Ihnen damit einen Ein- und Überblick über den öffentlichen Teil unserer Handlungsfelder und zeigt Ihnen Ansprechpartner und deren Expertise auf, die wir auch weiterhin in enger Kooperation mit Ihnen ausbauen und zur Anwendung bringen wollen.

Unser Bericht fasst aber auch weitere charakteristische Highlights des Jahrs 2024 zusammen: So hat in diesem Jahr als kleines Jubiläum das 10. CODE Capture-The-Flag-Event unter dem Motto „Predator – Threat Hunting“ stattgefunden, für das sich die besten 20 Teams für ein Wochenende auf dem Campus versammelten. Im Rahmen der ersten Jahrestagung von dtec.bw hatten wir die Möglichkeit, ausgewählte Projekte und deren Zwischenergebnisse anschaulich zu präsentieren.

Auch im Rahmen größerer von CODE ausgerichteter Veranstaltungen wie der Tagung des BMBF-Schirmprojekts Quantenkommunikation (SQuaD) und dem Board Meeting und Networking Day des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) konnten wir zur Weiterentwicklung auf fachlicher und politischer Ebene beitragen.

Wir wünschen Ihnen eine anregende Lektüre und freuen uns auf die weitere Zusammenarbeit und gemeinsame Aktivitäten!

Prof. Dr. Wolfgang Hommel

Prof. Dr. Michaela Geierhos

Marcus Knüpfer
Leitung des Forschungsinstituts CODE

ABB.: UNIBW M; A. WAGENER FOTOGRAFIE

Inhalt

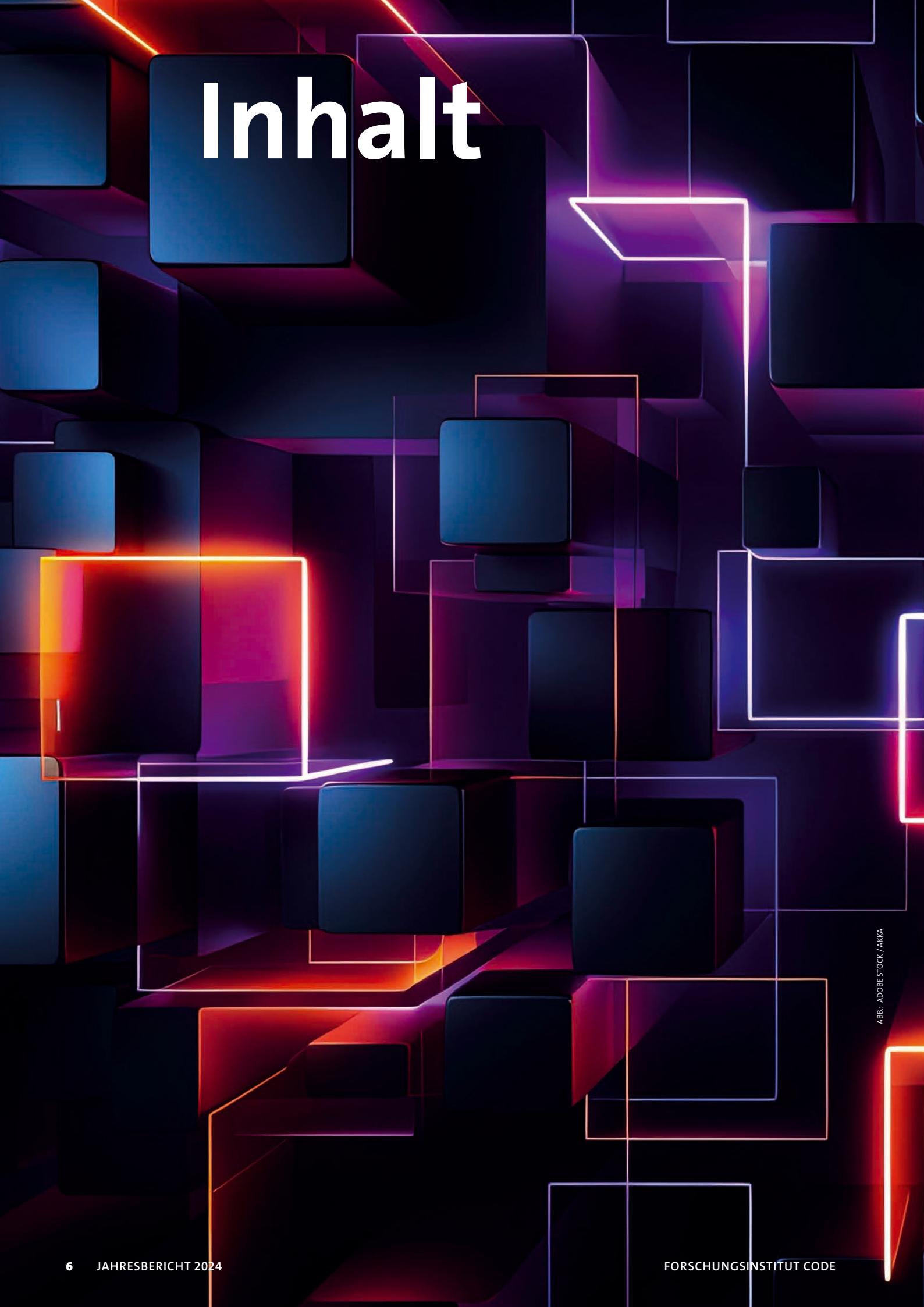


ABB.: ADOBE STOCK / AKKA

Highlights
Aus dem Institut

Forschung
Porträts und Projekte

Weitere Forschungsgruppen und Projekte

Kooperationen
Deutschland und die Welt

Nachwuchsförderung
Chancen und Angebote

Addendum
Publikationen und Aktivitäten

Organisation

Rubriken

UNSER LEITBILD

ABB.: ADOBE STOCK / STNAZKUL

Das Forschungsinstitut CODE ist eine zentrale wissenschaftliche Einrichtung der Universität der Bundeswehr München. Wir setzen unsere Expertise zum Mehrwert der Gesellschaft und der Bundeswehr ein und tragen durch Innovationen im Bereich Cyber/IT dazu bei, Deutschland ein Stück sicherer zu machen.

Drei Säulen stehen dabei im Fokus unseres Handelns:

- **Forschung und Technologie-Entwicklung**
- **Wissenstransfer sowie Beratung von Entscheidungsträgern**
- **Aus- und Weiterbildung**

Wir betreiben sowohl Grundlagen- als auch anwendungsnahe Forschung und Technologie-Entwicklung in den Themenfeldern Cyber Defence, Smart Data und Quantum Technology. Unsere Arbeit fokussiert sich dabei auf den konkreten und perspektivischen Nutzen für die Gesellschaft und die Bundeswehr. Durch unsere engen Verbindungen mit der Teilstreitkraft CIR (Cyber- und Informationsraum) der Bundeswehr sind wir in einer einzigartigen Position, durch Forschung in einer sicheren Umgebung Lösungen für die aktuellen und zukünftigen Herausforderungen in der Domäne CIR zu erarbeiten.

Unser Ziel ist es, technische Innovationen und Konzepte zum Schutz von Daten, Software und Systemen ganzheitlich und interdisziplinär zu erforschen. Wir legen besonderen Wert darauf, anwendungsnahe Technologien zu entwickeln und die gesellschaftliche Akzeptanz für sichere Technologien zu fördern. Dafür arbeiten wir eng mit der Bundeswehr, Behörden, Forschungseinrichtungen und der Wirtschaft zusammen, damit unsere Partner neue Forschungserkenntnisse und Technologien wertschöpfend in die Praxis transferieren können.

Wir sind offen für den wissenschaftlichen Diskurs und verfolgen langfristige Kooperationen. Mit den breit gefächerten Kompetenzen unserer Professuren und Forschungsgruppen stehen wir Entscheidungsträgern aus Bundeswehr und Politik beratend zur Seite und fördern den Wissenstransfer. Unser wissenschaftlicher Beirat unterstützt das FI CODE mit seiner fachlichen Expertise aktiv bei der strategischen Weiterentwicklung.

Für die Aus- und Weiterbildung bieten wir optimale Rahmenbedingungen. Unsere IT-Infrastruktur erlaubt Forschung und Ausbildung auf höchstem Niveau. Wir bereiten in der Lehre Studierende an der Universität der Bundeswehr München auf die Herausforderungen ihres Berufslebens vor und bilden Angehörige der Bundeswehr und Cyber-Reserve in unserer modernen Cyber Range praktisch weiter. Der direkte Zugang zu Quantencomputern ermöglicht uns bereits heute, innovative Lösungen für die Herausforderungen von morgen zu finden.

Wir stehen zu unserer Verantwortung und Vorbildfunktion, gemeinsam mit unseren Partnern und vor allem der Bundeswehr für den Schutz der freiheitlichen demokratischen Gesellschaft einzutreten. Wir arbeiten täglich daran, einen wesentlichen Beitrag zum Schutz vor den Gefahren im Cyber- und Informationsraum zu leisten und sind bereit, uns daran messen zu lassen. ■

ABB.: ADOBE STOCK / PINKEYES

Highlights

Aus dem Institut

Mit weit über 500 Teilnehmenden verzeichnete die CODE-Jahrestagung 2024 einen neuen Besucherrekord. Auf der begleitenden Fachausstellung präsentierten sich ausgewählte Unternehmen dem Fachpublikum.

CODE-Jahrestagung 2024

Bedrohungen und Chancen durch KI

„Gemeinsam mit KI gegen neue Cyber-Bedrohungen“ war das Leitthema der CODE-Jahrestagung 2024. Vertreterinnen und Vertreter aus Forschung, Industrie und Bundeswehr nahmen an dem zweitägigen Event am 10. und 11. Juli auf dem Campus der Universität der Bundeswehr München (UniBw M) teil. Mit weit über 500 Teilnehmenden war es die bisher größte Jahrestagung für CODE. Zu den zahlreichen hochrangigen Gästen zählten u. a. der Bundestagsabgeordnete Dr. Reinhard Brandl, Bayerns Digitalminister Dr. Fabian Mehring und Generalleutnant Michael Vetter.

DAS TAGUNGSPROGRAMM wurde mit den Grußworten von Prof. Dr. Uwe M. Borghoff, Vizepräsident der UniBw M, und Prof. Dr. Michaela Geierhos, Technische Direktorin des Forschungsinstituts Cyber Defence und Smart Data (CODE) eröffnet. Im Anschluss folgte die Keynote von Brigadegeneral Michael Volkmer. Der Kommandeur des Zentrums für Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw) berichtete u. a. über die aktuellen Bestrebungen des ZDigBw zur Bereitstellung einer Basisinfrastruktur für die Digitalisierung der Streitkräfte bis 2029. Das Thema „IT-Sicherheit und Künstliche Intelligenz" beleuchtete Prof. Dr. Norbert Pohlmann, Professor für Informationssicherheit sowie Geschäftsführer des Instituts für Internet-Sicherheit (if(is)) an der Westfälischen Hochschule Gelsenkirchen.

Nach den Eröffnungsvorträgen und einer Pause wurde das Nachmittagsprogramm mit drei Beiträgen zum Thema Künstliche Intelligenz fortgesetzt. Prof. Dr. Christian Hummert, Forschungsdirektor und Geschäftsführer der Cyberagentur, stellte in seinem Vortrag „Sicherheit für KI" u. a. die KI-Perspektiven und Förderaktivitäten der Cyberagentur vor. Der „Einfluss von KI auf die Cyberbedrohungslandschaft" war Thema des Beitrags von Dr. Christoph Martin vom Bundesamt für Sicherheit in der Informationstechnik (BSI). Er warnte insbesondere vor dem zunehmenden Reifegrad von Social Engineering Angriffen in Text, Ton, Bild und Video. Auch Malware werde inzwischen mit Hilfe von KI so weit optimiert, dass sie nicht mehr erkannt werden könne. Andrea Martin von der IBM Deutschland GmbH stellte die Frage „Künstliche Intelligenz und Cyberspace – Wer profitiert mehr: Verteidiger oder Angreifer?".

Fachausstellung und Workshops

Begleitet wurde Jahrestagung von einer zweitägigen Fachausstellung. An beiden Tagen konnten sich ausgewählte IT-Unternehmen präsentieren und über die neuesten Entwicklungen im Cyberbereich informieren. Während der Programmpausen gab es zudem in der Coffee Corner für die Gäste die Möglichkeit, Vorträge zu aktuellen Themen der Cybersicherheit zu hören.

Der weitere Nachmittag stand ganz im Zeichen der Workshops. Von Quantentechnologien bis KI – in insgesamt fünf parallel stattfindenden Workshop erwartete die Teilnehmenden ein breites Themenspektrum.

Zum Abschluss des ersten Veranstaltungstages beleuchtete Susanne Dehmel, Mitglied der Geschäftsleitung des Digitalverbands BITKOM e.V., in ihrem Vortrag das Thema Cybersicherheit aus Sicht der Wirtschaft. Ihr Plädoyer für eine stärkere Vernetzung der Akteure in diesem Bereich stieß beim Publikum auf große Zu-

Zu den hochkarätigen Rednern auf der CODE-Jahrestagung zählten auch der Bundestagsabgeordnete Dr. Reinhard Brandl (r.) sowie Bayerns Digitalminister Dr. Fabian Mehring (2.v.r.). Begrüßt wurden sie vom Leitenden Direktor Prof. Dr. Wolfgang Hommel und der Technischen Direktorin Prof. Dr. Michaela Geierhos.

BEIDE ABB.: FI CODE / ANGELIKA WAGENER FOTOGRAFIE

stimmung. Dem konnte dann auch unmittelbar beim Get-together nachgekommen werden, mit dem die Veranstalter den ersten Tag ausklingen ließen.

Politische Keynotes und Innovationstagung

Den zweiten Tag auf der CODE-Jahrestagung eröffnete der Leitende Direktor Prof. Dr. Wolfgang Hommel. Er begrüßte insbesondere die hochrangigen Gäste aus Politik und Bundeswehr und gab einen Überblick über die aktuellen Entwicklungen am FI CODE. Ihm folgte Generalleutnant Michael Vetter. Der Abteilungsleiter CIT und CIO im Bundesministerium der Verteidigung (BMVg) sprach in seiner Keynote über Software-Defined Defense als neues Paradigma für die Fähigkeitsentwicklung der Streitkräfte“. Der Bundestagsabgeordnete Dr. Reinhard Brandl stellte in seinem Vortrag ein Zehn-Punkte-Programm vor, mit dem die Zeitenwende auch in der Cyberabwehr umgesetzt werden kann. Im Anschluss sprach der bayerische Staatsminister für Digitales, Dr. Fabian Mehring, vor den Tagungsteilnehmenden zum Thema Cybersicherheit und den Herausforderungen in diesem Bereich. Man dürfe nicht die Fehler der Vergangenheit wiederholen und sich im Zuge der Digitalisierung in neue Abhängigkeiten begeben und damit erpressbar machen, mahnte er. Dazu sei es besonders wichtig, die Hoheit über die eigenen Daten zu schützen, aber auch das Thema Cybersicherheit stärker in den Alltag der Menschen zu integrieren.

An die politischen Keynotes des Vormittags schloss sich die Innovationstagung Cyber/IT an. Mit diesem Ideenwettbewerb möchte die Bundeswehr neue Wege bei der Identifizierung von IT-Innovationen für eine mögliche Verwendung im Geschäftsbereich des BMVg einschlagen. Insgesamt gingen in diesem Jahr über 30 Bewerbungen ein, aus denen eine Fachjury im Vorfeld die acht besten Konzepte auswählte und zur Tagung einlud. In jeweils siebenminütigen Kurzvorträgen präsentierten die acht Finalisten ihre Ideen dem Fachpublikum. Diese reichten von hochsicheren Routing-Architekturen in Quantum-Key-Distribution-Netzwerken, über neuartige Sensormodule für die teilautonome Gefechtsfeldaufklärung bis hin zu transportablen Quantencomputern. Dabei hatten auch die Gäste beim anschließenden Meet-the-Speakers die Möglichkeit, mit den Vortragenden in Kontakt zu treten. Den Sieg holte sich am Ende Simon Klink von der SE3 Labs GmbH. Seine Idee einer Echtzeit 3D-Aufklärung mittels autonomer Drohnen (UAVs) mit KI-Cockpit konnte die Fachjury überzeugen

Gruppenbild mit Teilnehmern der Innovationstagung (v. l. n. r.): (obere Reihe): Andreas Walbrodt (Enclaive GmbH), Prof. Dr. Wolfgang Hommel (Leitender Direktor des FI CODE), Brigadegeneral Armin Fleischmann (Unterabteilungsleiter CIT I im BMVg), Dr. Wolfgang Meißner (ARQUE Systems GmbH), Simon Klenk (SE3 Labs GmbH), João Schneider (Universität Gießen) (untere Reihe): Dr.-Ing. Emmanuel Stapf (SANCTUARY Systems GmbH), Peter Horoschenkoff (Rohde & Schwarz Cybersecurity / TU München), Hussein Hasso (Fraunhofer FKIE), Dr.-Ing. Felix Heilemann (Sagio GmbH).

BEIDE ABB.: FI CODE / ANGELIKA WAGENER FOTOGRAFIE

Paneldiskussion (v. l. n. r.): Felix Broßmann (Moderator des Panels, SKAD AG), Miriam Schnürer (Mitglied des Vorstands, Bundesverband für den Schutz Kritischer Infrastrukturen e. V.), Dr. Pascal van Overloop (Industry Advisor Defense & Intelligence, Microsoft Deutschland GmbH), Victoria Toriser (Cybergrundlagen und Innovation, Österreichisches Bundesheer), Cora Lisa Perner (R&T Cybersecurity, Airbus Defence and Space), Dr. Kai Martius (Mitglied des Vorstands / Chief Technology Officer, secunet Security Networks AG).

und ihm ein Preisgeld in Höhe von 15.000 € sichern. Die Plätze 2 und 3 gingen an João Schneider, Universität Gießen („Das VERITAS-System Hornisse: Lückenlose Lagebilderstellung dank KI gestützter Sensordatenauswertung“) und Dr. Markus Adrian Peter Beckers, ARQUE Systems GmbH („Neuartige Chiparchitektur für einen kurzfristig verfügbaren transportablen Quantencomputer zum Einsatz direkt in Konfliktfällen für diverse Anwendungen“). Auch die restlichen Finalisten wurden mit einer Prämie von 1.000 € ausgezeichnet.

Science Track und Paneldiskussion

Das Nachmittagsprogramm startete nach einer Pause mit dem Science Track. Zwei Wissenschaftlerinnen und ein Wissenschaftler gaben dem Auditorium Einblicke in ihre aktuelle Forschung. PD Dr. Sabine Wölk vom Deutschen zentrum für Luft- und Raumfahrt (DLR) sprach über Risiko und Potential von Quantencomputing. Prof. Dr. Daniel Slamanig und Prof. Dr. Marta Gomez-Barrero, beide seit Ende 2023 am FI CODE, stellten ihre Forschung zu Kryptografie und KI bzw. Biometrische Erkennung vor.

Der Nachmittag wurde fortgesetzt mit den Vorträgen „Technologische Bedrohungen aus der Luft Drohnen, Schwärme und Smart Dust als Risiken für kritische Infrastrukturen“ von Miriam Schnürer, Bundesverband für den Schutz Kritischer Infrastrukturen (BSKI), und „Cyber & KI im Russlandkrieg“ von Volker Kozok, Netzwerk für Cyber Intelligence.

In der abschließenden Paneldiskussion zum Thema „Innovation im Korsett – KI-Sicherheit in Deutschland“ sprachen Expertinnen und Experten aus Militär und Industrie. Mit dabei waren Dr. Kai Martius (Mitglied des Vorstands / Chief Technology Officer, secunet Security Networks AG), Miriam Schnürer (Mitglied des Vorstands, Bundesverband für den Schutz Kritischer Infrastrukturen e. V.), Cora Lisa Perner (R&T Cybersecurity, Airbus Defence and Space), Victoria Toriser (Cybergrundlagen und Innovation, Österreichisches Bundesheer) und Dr. Pascal van Overloop (Industry Advisor Defense & Intelligence bei der Microsoft Deutschland GmbH). Moderiert wurde die Diskussion von Felix Broßmann (SKAD AG). Mit dem Schlusswort des CODEs Leitendem Direktor Prof. Dr. Wolfgang Hommel endete das Vortragsprogramm der CODE-Jahrestagung 2024. Mit 540 Teilnehmenden war es die bisher größte Jahrestagung für CODE. Er dankte allen Beteiligten und Unterstützern für Ihren großartigen Einsatz und lud bei der Gelegenheit gleich zur nächsten Tagung am 8. und 9. Juli 2025 ein. ■

Mehr Informationen zur CODE-Jahrestagung

www.unibw.de/code/events/jahrestagungen

www.youtube.com/c/FzcodeDeubw

code@unibw.de

Bericht zur dtec.bw-Jahrestagung 2024

Zukunftstechnologien zum Anfassen

Bei der ersten Jahrestagung des Zentrums für Digitalisierungs- und Technologieforschung der Bundeswehr am 17. und 18. September 2024 präsentierte CODE zwei zukunftsweisende Forschungsprojekte dem Fachpublikum.

ÜBER 600 GÄSTE aus Bundeswehr, Forschung, Industrie und Start-Ups zog es Mitte September 2024 auf den Campus der Universität der Bundeswehr München (UniBw M). Unter dem Motto „Forschung mit Mehrwert für alle Dimensionen“ hatte das Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr (dtec.bw) nach Neubiberg eingeladen, um die vielfältigen Forschungsprojekte für das Fachpublikum erlebbar zu machen. In einem abwechslungsreichen Programm präsentierten sich an zwei Tagen zahlreiche Projekte aus den Dimensionen Luft, Land, See, Mensch, Weltraum und Cyber, die an den Bundeswehr-Universitäten in Hamburg und München bearbeitet werden. Auch das Forschungsinstitut CODE war mit zwei seiner insgesamt sechs dtec.bw-geförderten Projekten vertreten.

Quantensichere Kommunikation in der Anwendung

Die Tagung begann mit der feierlichen Eröffnung durch die Präsidentin der UniBw M, Prof. Dr. Eva-Maria Kern und Grußworten hochrangiger Vertreter aus dem Bun-

Mit einem Showcase zeigte das MuQuaNet-Team eindrucksvoll eines von vielen möglichen Anwendungsszenarien für eine quantensicher verschlüsselte Datenübertragung.

desministerium der Verteidigung. Als ausgewähltes Projekt aus der Forschungsdimension Cyber stellte Prof. Dr. Wolfgang Hommel den zahlreichen Gästen im Audimax das Forschungsprojekt Munich Quantum Network (MuQuaNet) vor. Ziel des Projektes ist es, mit der UniBw M als Kernpunkt ein quantensicheres Kommunikationsnetz für Forschung und Evaluierung zu entwickeln, aufzubauen, zu betreiben und weiteren Forschungseinrichtungen sowie Behörden und militärischen Dienststellen zur Verfügung zu stellen. Aufgebaut aus unterschiedlichen Komponenten, soll es die nahtlose Integration in die bereits bestehende Netzkommunikation vorbereiten, die vielfältigen Einsatzmöglichkeiten demonstrieren und als Blaupause für den Aufbau maßgeschneiderter, hochsicherer Kommunikationsnetze dienen. Über großes Interesse konnten sich später die Mitarbeiterinnen und Mitarbeiter am MuQuaNet-Stand im Foyer freuen, wo sie spannende Einblicke in ihre For-

Technische Komponenten für die quantensichere Verschlüsselung.

schungsarbeit gaben und anhand einer quantensicher verschlüsselte Virtaul-Reality-Fernwartungsumgebung einen eindrucksvollen Anwendungsfall für die Technologie zeigten.

Krisenkommunikation: Auch im Notfall informiert bleiben

Am zweiten Tag der dtec.bw-Jahrestagung hatten die Besucherinnen und Besucher gelegenheit, sich auf verschiedenen Schwerpunkttouren über den Uni-Campus zu bewegen und dabei die vielfältigen dtec.bw-geförderten Projekte aus nächster Nähe zu erleben. Neben MuQuaNet präsentierte sich auch das Projekt Resilient Operation of LoRa Networks (ROLORAN). An ihrem Stand präsentierten sie unter anderem eine Infrastruktur für die Blackout-Krisenkommunikation, wie sie beispielsweise nach schweren Naturkatastrophen gewährleistet werden muss. Die LoRa-Funktechnologie, die dabei zum

Das ROLORAN-Projektteam um Prof. Hommel (r.) präsentierte ein selbstentwickeltes System für die Blackout-Krisenkommunikation.

Einsatz kommt, ist nicht nur besonders energie- und kosteneffizient, sondern zeichnet sich zudem durch hohe Reichweiten aus. Bereits im Jahr 2025 soll ein entsprechendes System in der Gemeinde Neuhaus (Kärnten, Österreich) aufgebaut und evaluiert werden.

Die dtec.bw-Jahrestagung 2024 zeigte deutlich, wie viele Ergebnisse in der ersten Förderphase (bis Ende 2024) bereits erreicht werden konnten und wie eng die Universitäten der Bundeswehr dabei sowohl untereinander als auch mit externen Partnern zusammenarbeiten, um Forschungsergebnisse in praxisrelevante Anwendungen zu übertragen. Die nächste Jahrestagung wird im September 2025 in Hamburg stattfinden. ■

dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

Mehr Informationen

www.dtecbw.de

go.unibw.de/roloran

go.unibw.de/muquanet

ALLE ABB.: FI CODE / B. BELLGRAU

LSI-Präsident Bernd Geisler (r.) besuchte die Trainingsteilnehmenden am FI CODE.

BLKA und LSI trainieren am FI CODE

Gemeinsam im Einsatz

Mitarbeiterinnen und Mitarbeiter vom Bayerischen Landeskriminalamt (BLKA) und dem bayerischen Landesamt für Sicherheit in der Informationstechnik (LSI) trainierten im März in der Cyber Range des FI CODE für den Ernstfall. LSI-Präsident Bernd Geisler und Vizepräsident Dr. Thomas Kaiser sowie Vertreter des BLKA besuchten die zwölf Teilnehmenden vor Ort und nutzten die Gelegenheit für Gespräche mit CODE-Direktor Prof. Dr. Wolfgang Hommel.

Ein Schlüsselaspekt des Trainings war die enge Zusammenarbeit innerhalb des gemischten Teams.

IN DER CYBER RANGE des FI CODE trainierten am 21. und 22. März Mitarbeitende von BLKA und LSI gemeinsam die Bekämpfung von Cyberangriffen. Die zwölf aktiven Teilnehmenden wurden in einem realitätsnahen Szenario herausgefordert. Ziel war es, die Reaktion auf einen komplexen Cyberangriff auf ein Krankenhaus zu üben.

Realitätsnahe Herausforderung: Ein Advanced Persistent Threat (APT)

Im Szenario „InTime“ sahen sich die Teilnehmenden mit einer bedrohlichen Situation konfrontiert: Das IT-System eines Krankenhauses war durch Ransomware verschlüsselt worden. Dies hatte katastrophale Aus-

wirkungen auf den Betrieb und die Patientensicherheit. Jedoch blieb es nicht bei einem einfachen einstufigen Angriff. Der Angriff stellte einen sogenannten Advanced Persistent Threat (APT) dar, bei dem der Angreifer sich nicht nur Zugang zum Netzwerk verschafft, sondern dort auch weiterhin unauffällig agiert, indem er sich tarnt und weitere Systeme übernimmt. Auch Evasion-Techniken zur Umgehung von Sicherheitssoftware wurden von Angreifer eingesetzt.

Besonders herausfordernd war dabei die Tatsache, dass den Teilnehmenden keinerlei Zusatzinformationen, wie beispielsweise Netzpläne, zur Verfügung gestellt wurden. Alle relevanten Informationen mussten selbst beschafft werden, sei es durch Befragung der Lagedarsteller oder durch andere investigative Methoden. Dies spiegelt die Realität wider, in der Forensiker und IT-Experten oft mit unvollständigen Informationen arbeiten müssen.

Um den Angriff so authentisch wie möglich zu gestalten, wurden reale Vulnerabilitäten ausgenutzt. Drei Schwachstellen aus dem Jahr 2021 wurden von den Trainingsleitern miteinander verknüpft, um den fiktiven Angreifern den Zugriff auf das System zu ermöglichen. Diese Art der Herangehensweise bot den Teilnehmenden die Gelegenheit, auch ihre Fähigkeiten hinsichtlich Identifizierung und Behebung von Sicherheitslücken zu schärfen.

Praxisnahe Übung und intensive Herausforderung: Reaktion auf den Angriff und forensische Analyse

Das Training begann mit einfachen Übungen, bei denen sich die Teilnehmenden mit dem verwendeten System und den Tools vertraut machen konnten. Das eigentliche Szenario, das den APT-Angriff simulierte, startete dann am Mittag des ersten Trainingstages und lief bis zum Ende des zweiten Tages. Während dieses Zeitraums mussten die Ermittelnden nicht nur den Angriff selbst bewältigen, sondern auch forensische Analysen durchführen und die Abläufe im Krankenhausnetzwerk verstehen.

Die enge Zusammenarbeit innerhalb des gemischten Teams war dabei ein Schlüsselaspekt des Trainings. Durch den Austausch von Know-how und Ressourcen konnten die Teilnehmenden wertvolle Einblicke gewinnen und ihre Fähigkeiten im Umgang mit Cyberangriffen weiterentwickeln. Solche Übungen sind entscheidend, um die Sicherheit der digitalen Infrastruktur auch in Zukunft zu gewährleisten und die Reaktionsfähigkeit der Behörden in Krisensituationen weiter zu stärken.

In einer parallel zur Übung stattfindenden Gesprächsrunde zwischen hochrangigen Vertreterinnen und Vertretern von LSI, BLKA und FI CODE sprach man am Donnerstagnachmittag über den weiteren Bedarf an Cyber-Range-basierten Trainings sowie über zukünftige Möglichkeiten zur engeren Zusammenarbeit der drei Institutionen ■

Sprachen über den weiteren Bedarf an Cyber-Range-basierten Trainings und die Möglichkeiten zur engeren Zusammenarbeit (v. l. n. r.): Dr. Thomas Kaiser (Vizepräsident LSI), Prof. Dr. Wolfgang Hommel (Leitender Direktor FI CODE), Bernd Geisler (Präsident LSI), KD Dieter Hausberger (Dezernatsleiter Cybercrime, BLKA), LtdKD Simone Lang (Abteilungsleiterin Zentrale kriminalpolizeiliche Dienste, BLKA).

ALLE ABB.: FI CODE / B. BELLGRAU

Die Quantenchips von IBM bilden das Herzstück der Vision eines quantenzentrierten Supercomputers.

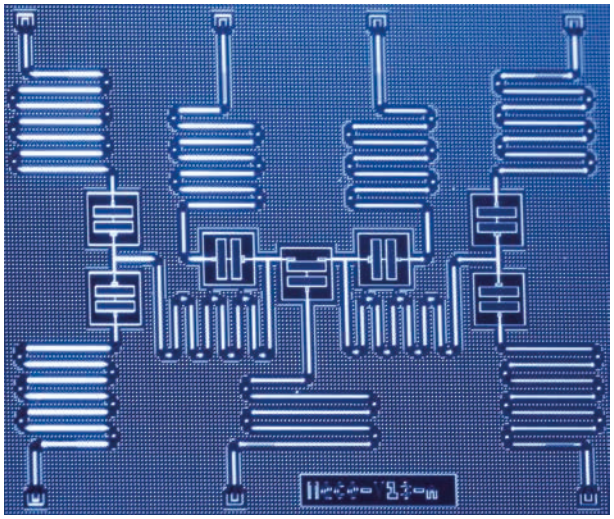
Entscheidungsfindung unter Unsicherheit und Optimierung

Grundlagenforschung als Wegbereiter für praxisnahe Anwendungen

Quantentechnologien verändern die Bereiche Computing, Sensing und Kommunikation durch drei Schlüsselkomponenten: Quantencomputer, die einige komplexe Berechnungen mit bisher unerreichter Geschwindigkeit durchführen; Quantensensoren, die physikalische Phänomene mit extremer Genauigkeit erfassen; und Quantennetzwerke, die Quantensysteme über große Entfernungen sicher miteinander verbinden. Zusammen bilden diese Elemente die Grundlage für innovative (Quanten-) Informationsverarbeitung.

DIE Quanteninformationswissenschaft baut auf der Grundlagenforschung auf, um praktische Anwendungen zu entdecken und relevante Anwendungsfälle zu identifizieren. Indem sie die Kernprinzipien der Quantenmechanik anwenden, können Forschende im Bereich Computing, Sensing und Kommunikation Innovationen vorantreiben. Dieses tiefe Verständnis der wissenschaftlichen Grundlagen erleichtert die Übertragung theoretischer Quantenkonzepte in reale Anwendungen und Simulationen auf Testbeds wie dem IBM Quantum Chip.

Das Quantencomputing bietet ein erhebliches Potenzial, um Vorteile im Computing zu erzielen. Eine wesentliche Voraussetzung für die Effizienz eines Quantenalgorithmus ist die gezielte Nutzung bestimmter Quanteneigenschaften wie Überlagerung, Interferenz, Verschränkung und Unbestimmtheit. Klassische Algorithmen wurden sowohl theoretisch als auch empirisch entwickelt, wobei empirische Methoden manchmal später zu theoretischen Erkenntnissen führten. Im Gegensatz dazu war die Entwicklung von Quantenalgorithmen aufgrund der begrenzten Verfügbarkeit von Hardware in erster Linie theoretisch, aber dies änderte sich mit dem Aufkommen z. B. von Gatter-basierten Quantencomputern mit Dutzenden von Qubits, die komplexe Schaltkreise ausführen können, die bereits an die Grenzen der Simulationsfähigkeiten klassischer Computer stoßen.



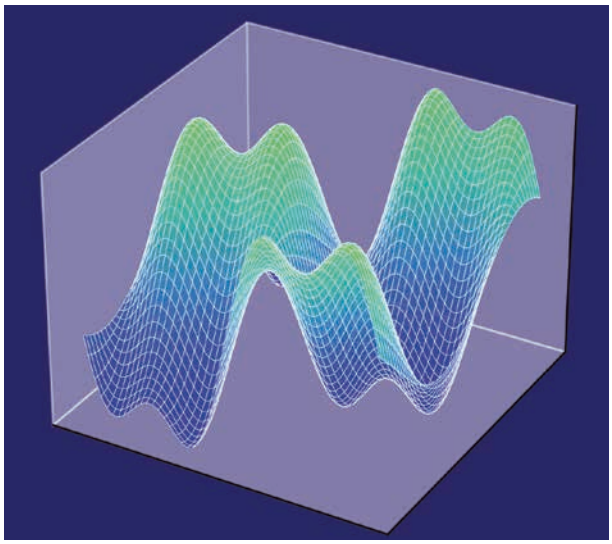
Quantencomputer als Testumgebung für die Quanteninformationsverarbeitung.

Netzwerk mit Markov-Prozessen.

Am FI CODE wird Quantencomputing unter anderem eingesetzt, um komplexe Entscheidungsprobleme unter Unsicherheit zu lösen, welche oft die Fähigkeiten klassischer Computer übersteigen. Verwendet werden Paradigmen des Quantencomputings, um das Management komplexer stochastischer Modelle zu verbessern. Ein Schwerpunkt liegt insbesondere auf mehrdimensionalen Markov-Prozessen, die bei der Entscheidungsfindung unter Unsicherheit von maßgeblicher Bedeutung sind. Quantencomputing nutzt die Quantenmechanik, um Informationen effizienter zu verarbeiten als klassische Systeme und bietet innovative Lösungen für diese Herausforderungen.

Ein weiterer Forschungsfokus am FI CODE liegt auf den Quantenwalk-Algorithmen. Sie stellen ein quantenmechanisches Gegenstück zu klassischen Zufallspfaden dar und sind von zentraler Bedeutung für die Entwicklung von Quantenalgorithmen. Sie bieten einen Rahmen, der die Quantenmechanik nutzt, um komplexe Netzwerke

ABB.: IBM; IBM RESEARCH / SCIENCE PHOTO LIBRARY; CHATGPT



Exemplarische Visualisierung einer Optimierung.

und Wahrscheinlichkeitsverteilungen zu erforschen. Bei der Entscheidungsfindung unter Unsicherheit können Quantenwalks einen erheblichen Rechenvorteil bieten.

Quantenwalks steigern erheblich die Effizienz von Suchalgorithmen auf spezifischen Graphen und Datenstrukturen, beschleunigen die Identifikation von kritischen Faktoren innerhalb komplexer Datensätze und verbessern strategische Entscheidungsprozesse.

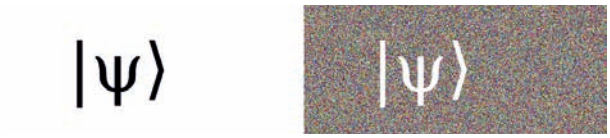
Quantenwalks und Quantenoptimierung sind wichtige Techniken im Quantencomputing, um komplexe Rechenherausforderungen zu bewältigen. Quantenwalks zeichnen sich dadurch aus, dass sie schnell durch umfangreiche Lösungsräume navigieren, um optimale oder nahezu optimale Lösungen in Szenarien mit mehreren komplexen und unsicheren Variablen zu finden. Diese Techniken werden eingesetzt, um bestimmte Optimierungsprobleme in verschiedenen Bereichen wie Logistik, maschinellem Lernen und Ingenieurwesen effizienter zu lösen als mit klassischem Computing.

Darüber hinaus sind Quantenwalks entscheidend für die **Simulation verteilter Quanteninformationen in Netzwerken**, die für eine sichere Quantenkommunikation unerlässlich sind. Dies umfasst die detaillierte Modellierung von Quantenzuständen, Netzwerkkomponenten und Interaktionen, unterstützt durch robuste Quantensoftware-Tools. Mit dem Fortschritt der Quantencomputertechnologie wird die Fähigkeit, Quantennetzwerke genau zu simulieren und zu optimieren, immer entscheidender für die Entwicklung praktischer Quantenkommunikationssysteme und -protokolle.

Quantenalgorithmen für Markov-Prozesse nutzen die Prinzipien der Quantenmechanik, um Systeme mit markovscher Dynamik effizient zu analysieren und zu simulieren, und bieten potenzielle Rechenvorteile gegenüber klassischen Ansätzen. Diese Algorithmen sind ideal für Szenarien, in denen die Dynamik Markov-Prozessen folgt. Quantenwalks, eine Schlüsseltechnik in diesem Bereich, ermöglichen die Simulation von Quantensystementwicklungen, die markovschen Regeln folgen, und wenden Quantendynamiksimulationen effektiv auf solche Systeme an. Quantenwalks haben das Potenzial, Entscheidungsprozesse unter Unsicherheit zu verbessern, indem sie eine grundlegend neue Art und Weise der Berechnung, Erforschung und Vorhersage komplexer Systeme bieten.

Da das **inhärente Rauschen in Quantensystemen** die Rechengenauigkeit erheblich beeinträchtigen kann, ist die Fehlerreduktion von essentieller Bedeutung. Zwei wichtige Techniken in diesem Bereich sind die probabilistische Fehlerkompensation und die „Zero Noise Extrapolation". Diese Strategien tragen dazu bei, die Zuverlässigkeit von Quantenberechnungen zu verbessern, ohne auf eine vollständige Quantenfehlerkorrektur zurückgreifen zu müssen, welche erhebliche Ressourcen erfordert.

Probabilistic Error Cancellation: Dieser Ansatz beinhaltet eine ausgeklügelte Methode, bei der Fehler in Quantenoperationen modelliert und dann durch Anwendung einer quasi-wahrscheinlichkeitsbasierten Darstellung des inversen Rauschprozesses kompensiert werden. Diese Methode hängt stark von einem genauen Rauschmodell ab und beinhaltet die Anpassung der Ergebnisse auf Grundlage der Wahrscheinlichkeiten verschiedener Fehlerprozesse.



Visualisierung von Rauschen.

Zero Noise Extrapolation: Diese Technik verfolgt einen eher empirischen Ansatz, bei dem der Rauschpegel, der das System beeinflusst, manipuliert wird. Durch Ausführung derselben Quantenschaltkreise bei verschiedenen kontrollierten Rauschpegeln und Extrapolation der Ergebnisse wird abgeschätzt, wie die Ergebnisse in einer idealen rauschfreien Umgebung aussehen würden. Diese Technik erfordert kein so detailliertes Wissen über das Rauschmodell, hängt aber entscheidend von der Fähigkeit ab, das Rauschen genau zu skalieren, und von der Angemessenheit des verwendeten Extrapolationsmodells.

Auf dem Gebiet der **Quantenfehlerkorrektur** wurden bereits bedeutende Fortschritte erzielt. Die derzeitigen Techniken sind Zwischenlösungen, die genauere Berechnungen auf Noisy Intermediate-Scale Quantum (NISQ)-Geräten ermöglichen. Mit der Weiterentwicklung der

Quantentechnologie werden wahrscheinlich ausgefeiltere und ressourceneffizientere Fehlerkorrekturmethoden entwickelt werden. Diese Fortschritte könnten potenziell längere, komplexere und genauere Quantenberechnungen ermöglichen. Darüber hinaus könnte die Integration von Techniken zur Fehlerminimierung mit fortgeschrittenen Protokollen zur Quantenfehlerkorrektur den Weg für die nächste Generation von Quantencomputern ebnen. Diese Integration könnte praktisches Quantencomputing in einem Maßstab und mit einer Genauigkeit ermöglichen, die mit heutigen Technologien nicht erreichbar sind. Fortschritte in diesem Bereich werden nicht nur von theoretischen Fortschritten abhängen, sondern auch von Verbesserungen in der Quantenhardware, wie z. B. einer besseren Kohärenz von Qubits, verbesserten Quantengattern und einer effektiveren Rauschcharakterisierung und -kontrolle. Diese Entwicklungen werden dazu beitragen, das langfristige Ziel eines vollständig fehlerkorrigierten Quantencomputers zu erreichen und neue Möglichkeiten in verschiedenen Bereichen wie Kryptographie, Materialwissenschaften und Simulation komplexer Systeme eröffnen.

Am FI CODE werden **Lehrmaterialien** entwickelt, die die Studierenden in die praktischen und theoretischen Aspekte des Quantencomputings einführen. Die Erkundung dieser Ansätze umfasst sowohl theoretische Studien als auch praktische prototypische Implementierungen. Dieser zweigleisige Ansatz hilft den Studierenden, komplexe Konzepte zu verstehen und sie in realen Szenarien anzuwenden. Darüber hinaus wird das Lehrmaterial durch Experimente mit Quantencomputern und der Semantik von Quantenschaltkreisen angereichert, die durch computergestützte symbolische Berechnungen unter Verwendung von Werkzeugen wie Computeralgebrasystemen und theoretischen Modellen wie dem ZX-Kalkül unterstützt werden. Dieser umfassende Ausbildungsrahmen fördert ein tieferes Verständnis und erleichtert automatisiertes Denken in der Quantenprogrammierung, wodurch die Studierenden auf weiterführende Studien und Forschung im Bereich des Quantencomputings vorbereitet werden.

Da sich die Quantentechnologien durch Verbesserungen bei der Quantenhardware in Verbindung mit ausgefeilteren Algorithmen rasch weiterentwickeln, eröffnen sich neue Anwendungsmöglichkeiten, z. B. bei der Entscheidungsfindung unter Unsicherheit und bei der Optimierung. Darüber hinaus wird die interdisziplinäre Zusammenarbeit zwischen Quantenphysikern, Datenwissenschaftlern und Informatikern entscheidend sein, um Quantenlösungen für spezifische Entscheidungsprobleme maßzuschneidern und so den Quantenvorteil zu maximieren. Obwohl sich das Quantencomputing noch in den Kinderschuhen steckt, verspricht es, die Art und Weise, wie komplexe Entscheidungen unter Unsicherheit getroffen werden, zu verändern. ■

ABB.: CHATGPT (2)

IBM Innovationszentrum

DAS FI CODE an der Universität der Bundeswehr München hat als IBM Innovationszentrum seit 2018 Zugang zur IBM Quantencomputing-Infrastruktur. Die derzeitige Verfügbarkeit von Quantencomputern mit geringem Rauschen (bis zu 156 Qubits) ermöglicht es Wissenschaftlern Quantenalgorithmen, Heuristiken, Fehlerkorrektur und Fehlerminderungsschemata zu testen, sowie Experimente durchzuführen, um die Quanteninformationsverarbeitung zu erforschen sowie Quantennetzwerke und Quantensensoren zu simulieren. Die Forschung am FI CODE konzentriert sich auf die Entwicklung von Algorithmen und Anwendungen in den Bereichen Quantenoptimierung, Quantenmaschinenlernen, Quantensimulation sowie Quantenfehlerkorrektur. Weiterhin werden Quantenwalk-Algorithmen entwickelt und auf IBM Quantencomputern implementiert, wobei Techniken zur Schaltkreisoptimierung und Fehlerreduktion zum Einsatz kommen. Die Quantencomputer werden mit dem Softwareentwicklungs-Kit „Qiskit“ auf Schaltkreis- und Algorithmen-Ebene programmiert, und entsprechende Experimente werden durchgeführt. Parallel dazu wird das Lehrprogramm für die Studierenden weiter ausgebaut und Vorlesungen, Laborpraktika und Workshops zur Quanteninformationsverarbeitung angeboten.

Neueste Veröffentlichungen des Quantum Innovationszentrums

YIN, R., WANG, Q., TORNOW, S., BARKAI, E.: Restart uncertainty relation for monitored quantum dynamics. PNAS 122 (1), e2402912121, (2025).

DEVRA, A., VAN DAMME, L., ENDE, F. V., MALVETTI, E., GLASER, S. J.: Theory and Experimental Demonstration of Wigner Tomography of Unknown Unitary Quantum Gates. arXiv preprint arXiv:2411.05404, (2024).

ABBAS, A., AMBAINIS, A., AUGUSTINO, B., BÄRTSCHI, A., BUHRMAN, H., COFFRIN, C. et al.: Challenges and opportunities in quantum optimization, Nature Reviews Physics, 1–18 (2024).

WANG, Q., REN, S., YIN, R., ZIEGLER, K., BARKAI, E., TORNOW, S. : First Hitting Times on a Quantum Computer: Tracking vs. Local Monitoring, Topological Effects, and Dark States Entropy 26 (10), 869 (2024).

TORNOW, S., ZIEGLER, K.: Measurement-induced quantum walks on an IBM quantum computer. Physical Review Research 5 (3), 033089, (2024).

OECD GFTech focus group on quantum technologies: A quantum technologies policy primer OECD DIGITAL ECONOMY PAPERS January 2025 No. 371

Quantenkommunikations-Workshop SQuaD an der UniBw M

Mit dem SQuaD-Workshop fand vom 16. bis 18. April 2024 erstmals eine der wichtigsten Tagungen im Bereich der Quantenkommunikation auf dem Uni-Campus in Neubiberg statt. Führende Wissenschaftlerinnen und Wissenschaftler, Forschende und Fachleute aus der Industrie kamen zusammen, um die neuesten Fortschritte und Forschungsergebnisse im Bereich der Quantenkommunikation zu diskutieren.

QUANTENKOMMUNIKATION ist eine Schlüsseltechnologie für die Sicherheit digitaler Infrastrukturen in unserer Gesellschaft. Die Tagung im Rahmen der Projekte „SQuaD“ (Schirmprojekt Quantenkommunikation Deutschland) und „MuQuaNet“ (Munich Quantum Network), brachte erstmals Förderprojekte des Bundesministeriums für Bildung und Forschung (BMBF) sowie des Bundesministeriums der Verteidigung (BMVg) mit ihren Expertinnen und Experten und Netzwerken zusammen. Die Präsidentin der Universität der Bundeswehr München (UniBw M), Prof. Dr. Eva-Maria Kern, betonte in ihrer Eröffnungsrede die hohe Relevanz von Vernetzung und Kooperation im Kontext aktueller Herausforderungen und dass das FI CODE maßgeblich zum Aufbau eines Ökosystems rund um das Thema Quantenkommunikation beigetragen habe. Prof. Wolfgang Hommel, Leitender Direktor des FI CODE, unterstrich zudem die hohe gesamtgesellschaftliche Bedeutung von sicherer Quantenkommunikation.

In seiner Rede hob Prof. Dr. Wolfgang Hommel die Bedeutung von quantensicherer Kommunikation für die Gesamtgesellschaft hervor.

ABB.: UNIBW M / SIEBOLD

Quantenkommunikation ist Schlüsseltechnologie

Im Verlauf der beiden Veranstaltungstage wurde ein breites Themenspektrum abgedeckt, welches tiefe Einblicke in den aktuellen Stand und die künftigen Möglichkeiten der Quantenkommunikation bot. Die Teilnehmenden hatten Gelegenheit, sich über die neuesten Forschungsergebnisse in Projekten wie SQuaD, MuQuaNet, 6G-QuaS und DE-QOR zu informieren. Diese Projekte setzen auch international Maßstäbe in der Entwicklung von Netzwerken und Technologien der Quantenkommunikation. Ein weiteres zentrales Thema waren die Marktentwicklungen im Bereich Quantenschlüsselaustausch (QKD), einer theoretisch abhörsicheren Methode für die Übertragung von Verschlüsselungsschlüsseln, basierend auf den Prinzipien der Quantenmechanik. Die Dringlichkeit der Entwicklung und Implementierung von QKD-Systemen wurde vor dem Hintergrund zunehmender Bedrohungen durch fortgeschrittene und leistungsstarke Rechentechnologien wie Quantencomputer, die herkömmliche Verschlüsselungsmethoden potenziell brechen können, und einer erhöhten Bedrohungslage auf dem europäischen Kontinent unterstrichen.

Die Bedeutung der Quantenkommunikation als Schlüsseltechnologie für die Sicherheit zukünftiger Kommunikationsnetze wurde durch die Veranstaltung eindrucksvoll unterstrichen. Die Projekte SQuaD und MuQuaNet zeigten das starke Engagement und die hohen Investitionen in Forschung und Entwicklung auf nationaler und internationaler Ebene. Beide Projekte bündeln die Expertise und das Know-how aus Wissenschaft und Industrie, um gemeinsam an der Entwicklung einer sicheren Kommunikationsinfrastruktur der Zukunft zu arbeiten. Durch diese Pionierarbeit werden bereits heute die technologischen Grundlagen für zukünftige Quantenkommunikationsnetze gelegt und der intensive Austausch zwischen Forschungseinrichtungen und Industrie vorangetrieben, um innovative Lösungen für die Herausforderungen der Datensicherheit im Zeitalter der Quanteninformatik zu finden. ■

Beim NCC-Netzwerktreffen im Oktober kamen auf dem Uni-Campus in Neubiberg Vertreterinnen und Vertreter aus den 27 EU-Mitgliedsstaaten sowie Norwegen und Island zusammen.

ABB.: FI CODE / B. BELLGRAU

EU-Cybersicherheit: Netzwerktreffen in Neubiberg

Als Teil des deutschen Nationalen Koordinierungszentrums für Cybersicherheit (NKCS/ NCC-DE) richtete das Forschungsinstitut CODE (FI CODE) vom 9. bis 11. Oktober 2024 auf dem Campus der Universität der Bundeswehr München das Netzwerktreffen der Nationalen Koordinierungsstellen für Cybersicherheit (NCCs) sowie die 10. Sitzung des Verwaltungsrats des Europäischen Kompetenzzentrums für Cybersicherheit (ECCC) aus. Organisiert wurde die Veranstaltung in Kooperation mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der Kopfstelle des NKCS.

Insgesamt kamen an den drei Tagen rund 120 Teilnehmende aus den 27 EU-Mitgliedsstaaten, Norwegen und Island auf dem Campus der Universität der Bundeswehr München zusammen. Eröffnet wurde der erste Tag von Laurie Tanker, der Vorsitzenden des NCC-Netzwerks. Anschließend begrüßten der Geschäftsführer des ECCC Luca Tagliaretti und Prof. Dr. Wolfgang Hommel, Leitender Direktor des FI CODE, die Teilnehmenden. In seiner Begrüßung hob Prof. Hommel insbesondere die Konsortialstruktur des NKCS hervor und unterstrich die Rolle, die das FI CODE in diesem Kontext erfüllt. FI CODE schaffe mit seiner Forschung nicht nur einen Mehrwert für die Bundeswehr, sondern auch für die europäische Gesellschaft insgesamt.

Auf dem weiteren Programm des NCC-Netzwerktags standen nicht nur Präsentationen der Europäischen Kommission, des ECCC und der Agentur der Europäischen Union für Cybersicherheit (ENISA), sondern auch zahlreiche Gruppensitzungen, bei denen sich die NCC-Vertreterinnen und -Vertreter vernetzen und dabei u. a. auch ihre Erfahrungen im Zusammenhang mit der Umsetzung des Digital Europe Programme (DEP) auf nationaler Ebene austauschen konnten.

Am Ende des Tages wurde Laurie Tanker vom NCC Estland von den Vertreterinnen und Vertreter der Nationalen Koordinierungszentren in ihrem Amt als Vorsitzende des NCC-Netzwerks bestätigt. Ebenfalls gewählt wurden zwei neue stellvertretende Netzwerk-Vorsitzende aus Luxemburg und Island.

In den folgenden zwei Tagen fand am 10. und 11. Oktober dann die Sitzung des ECCC-Verwaltungsrats statt, bei der die Vertreterinnen und Vertreter der EU-Mitgliedstaaten, Norwegens und Islands zusammenkamen, um über die weitere Ausrichtung des Digital Europe Programme (DEP) für den Zeitraum 2025 bis 2027 zu beraten und zu entscheiden. Im Zuge dessen wurden sechs Arbeitsgruppen eingerichtet, welche die weitere Entwicklung des DEP auch zukünftig diskutieren und unterstützen sollen. ■

Ausführliche Informationen über die Aktivitäten des deutschen NCC finden Sie unter:

https://nkcs.bund.de/

Der Vorsitzende der GOR, Prof. Dr. Alexander Martin (l.), verleiht die Ehrenmitgliedschaft der GOR an Prof. Dr. Stefan Pickl (r.).

Auszeichnung für Prof. Dr. Stefan Pickl

Bei der Jahrestagung der deutschen Gesellschaft für Operations Research (GOR) in München wurde Prof. Dr. Stefan Pickl die Ehrenmitgliedschaft verliehen. Die GOR würdigt damit sein herausragendes Engagement im Beirat sowie als Herausgeber der Vereinszeitschrift OR News.

DIE JAHRESTAGUNG der deutschen Gesellschaft für Operations Research (GOR) fand 2024 als gemeinsame Tagung mit der Österreichischen Gesellschaft für Operations Research (ÖGOR) und der Swiss Operations Research Society (SVOR/ASRO) unter dem Motto „Data, Learning, and Optimization“ vom 3. bis 6. September an der Technischen Universität München statt.

Anerkennung für außergewöhnliches Engagement

Ein besonderer Höhepunkt war die feierliche Auszeichnung von Prof. Dr. Stefan Pickl. Im Rahmen der Opening Ceremony und im Beisein der rund 700 Teilnehmerinnen und Teilnehmern der OR 2024 wurde ihm vom Vorsitzenden der GOR, Prof. Dr. Alexander Martin, die Ehrenmitgliedschaft verliehen. Die GOR würdigte damit seine herausragende und langjährige Mitarbeit als Vorsitzender des wissenschaftlichen Beirates sowie als engagierter Herausgeber der Vereinszeitschrift „OR News“. Diese Verleihung ist Ausdruck höchster Anerkennung und wird nur an Persönlichkeiten mit außergewöhnlichen Verdiensten vergeben – Prof. Pickl ist das 20. und bisher jüngste Ehrenmitglied der GOR.

Aufnahme in die Akademie der Technikwissenschaften

Erst Ende 2023 war Prof. Pickl in die Akademie der Technikwissenschaften (acatech) gewählt worden. Mit der acatech-Mitgliedschaft wird Prof. Pickl in einen Kreis herausragender Persönlichkeiten aufgenommen, die durch ihre wissenschaftliche Exzellenz und gesellschaftliche Wirkung zur Gestaltung technischer Innovationen in Deutschland beitragen. Seine besondere Expertise bringt Prof. Pickl insbesondere im Themenfeld „Sicherheit“ ein, wo er sich für einen interdisziplinären Dialog zwischen Wissenschaft, Technik und Gesellschaft engagiert. ■

Prof. Dr. Stefan Pickl (l.) bei der Verleihung der Ernennungsurkunde in Berlin durch den Präsidenten von acatech, Prof. Dr. Jan Wörner.

ABB.: UNIBW M / S. PICKL; TU MÜNCHEN

Erste Internationale NATO Summerschool: Decision Making for the Future

Offiziere treffen Entscheidungen – oft unter extremem Druck. Im digitalen Zeitalter haben sich die Grundlagen dafür wesentlich verändert: Die verfügbare Informationsmenge wächst stetig, ebenso wie die Methoden ihrer Analyse – etwa durch Künstliche Intelligenz. Vor diesem Hintergrund lud die Universität der Bundeswehr München gemeinsam mit der NATO Science and Technology Organization (STO) zur ersten NATO-Summerschool ein, die in Kooperation mit dem Forschungsinstitut CODE ausgerichtet wurde.

Generalmajor a. D. Reinhard Wolski (l.) sprach zur Rolle von KI in militärischen Entscheidungen.

ABB.: UNIBW M / S. PICKL

UNTER DEM MOTTO „Decision Making for the Future" kamen rund 40 Teilnehmerinnen und Teilnehmer aus mehr als acht Nationen zusammen. Den Auftakt bildete ein gemeinsames Barbecue am Campus, bei dem Vizepräsident Prof. Dr. Uwe Borghoff und CODE-Direktorin Prof. Dr. Michaela Geierhos begrüßten. Wissenschaftlicher Leiter der NATO Summerschool war Prof. Dr. Stefan Pickl, der zusammen mit dem militärischen Co-Chair Oberst Matthias Kinkel vom Planungsamt der Bundeswehr die Konferenz entwickelte und organisierte.

Führung in Zeiten von KI und geopolitischer Unsicherheit

In seiner Eröffnungsrede betonte Generalmajor Wolfgang Gäbelein, Amtschef des Planungsamts der Bundeswehr, die Bedeutung technologischer und wissenschaftlicher Überlegenheit der NATO angesichts aktueller geopolitischer Herausforderungen. Trotz aller Fortschritte in der KI müsse der Mensch immer in der Verantwortung bleiben. Er verwies zudem auf das 200. Jahr des preußischen Kriegsspiels – ein Bezug, der die historische Dimension von Entscheidungsfindung unterstreicht.

Jackie Eaton vom NATO Joint Analysis and Lessons Learned Centre (JALLC) eröffnete mit einer Plenarrede und ging auf die Bedeutung von Operational Analysis innerhalb der NATO ein. Prof. Dr. Daniel Nussbaum von der Naval Postgraduate School stellte die von ihm gegründete Task Force „Energie" vor, der auch Prof. Pickl angehört. Weitere Beiträge kamen u. a. von Dr. Zenon Matthews vom Schweizer Armeestab zu datenbasierter Verteidigungsanalyse sowie Generalmajor a.D. Reinhard Wolski zur Rolle von KI in militärischen Entscheidungen.

Vom Planspiel zur Praxis: Entscheidungsprozesse erlernbar gemacht

Ein Wargaming des Planungsamts der Bundeswehr verdeutlichte praktische Entscheidungsprozesse, begleitet von Vorträgen zur Entwicklung und Bedeutung dieser Methode. Leadership, Ethik und Zukunftstechnologien wie Biometrie wurden ebenfalls thematisiert.

Die Summerschool wurde eingerahmt vom 50. Todestag des Operations-Research-Pioniers Patrick Blackett und dem 80. Jahrestag des Stauffenberg-Attentats. In der Abschlusspräsentation erinnerte Prof. Pickl an Blacketts Maxime: „Seien Sie stets offen für neue Ansätze und stellen Sie sich dem interdisziplinären Diskurs."

2025 wird die Summerschool in Ankara fortgesetzt, zu der sich im Vorfeld bereits mehr 60 Teilnehmende angekündigt haben. ■

ABB.: ADOBE STOCK / ITCHAZNONG

Forschung

Porträts und Projekte

Die Forschung am FI CODE

Am Forschungsinstitut CODE werden derzeit 44 drittmittelfinanzierte Projekte in verschiedenen Forschungsgruppen durchgeführt. Eine Auswahl finden Sie auf den folgenden Seiten. Übergreifend forscht CODE in drei Geschäftsbereichen: Cyber Defence, Smart Data und Quantum Technology.

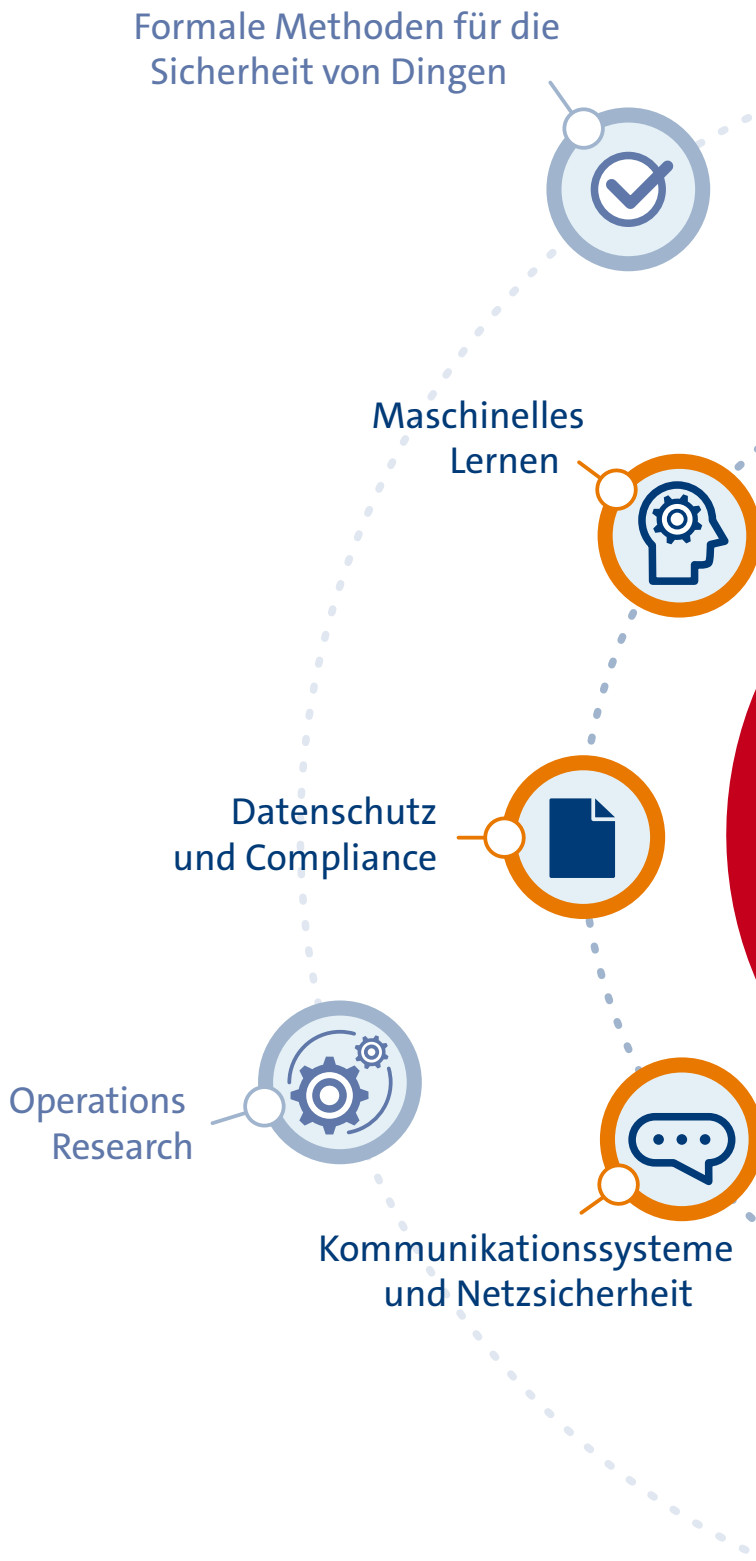
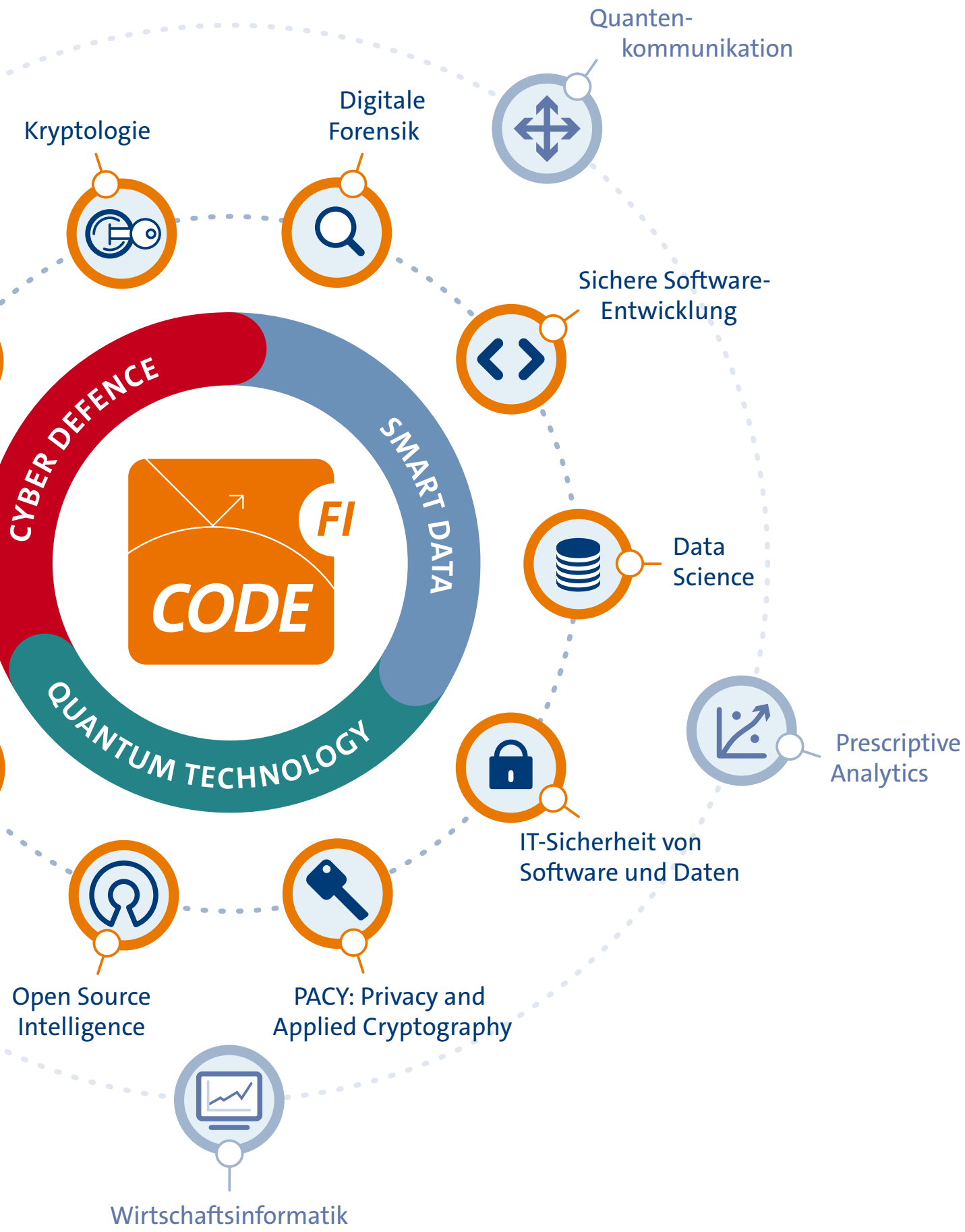


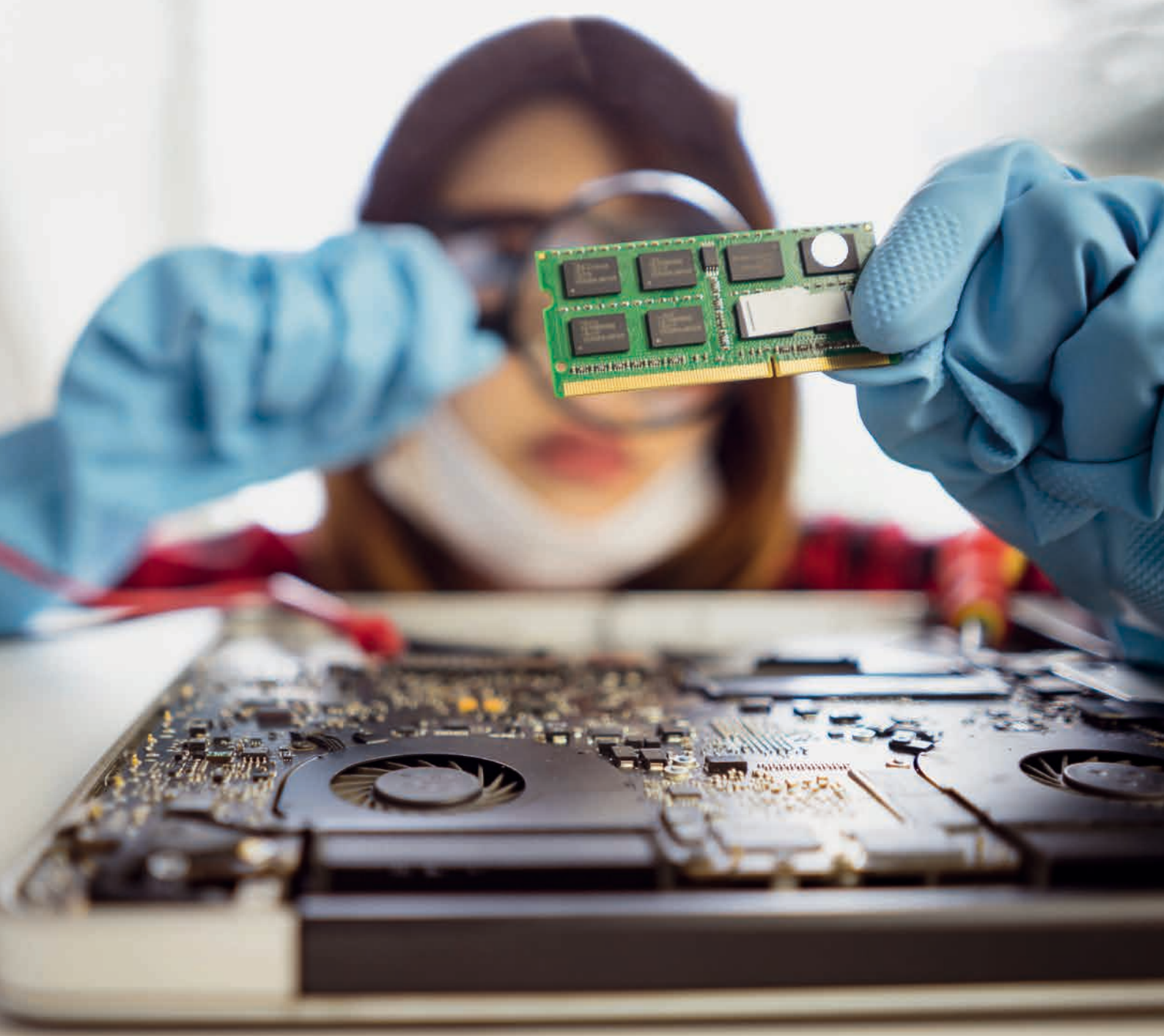
ABB.: TAUSENDBLAUWERK.DE


Quanten-
kommunikation
Digitale
Forensik
Kryptologie
Sichere Software-
Entwicklung
CYBER DEFENCE
SMART DATA
QUANTUM TECHNOLOGY
FI
CODE
Data
Science
Prescriptive
Analytics
IT-Sicherheit von
Software und Daten
Open Source
Intelligence
PACY: Privacy and
Applied Cryptography
Wirtschaftsinformatik

Prof. Dr. Harald Baier

Digitale Forensik

Durch die zunehmende Digitalisierung und das damit verbundene Wachsen von Cyberkriminalität steigen der Bedarf und die Anforderungen an die IT-forensische Aufarbeitung von Schadensfällen. Im Fokus der Professur für Digitale Forensik stehen der Umgang mit großen Datenmengen in IT-forensischen Untersuchungen, die Erzeugung synthetischer Datensätze für die Bewertung IT-forensischer Tools, Anti-Forensik sowie Hauptspeicherforensik.



DIE DIGITALE FORENSIK kommt als digitales Pendant zu den klassischen forensischen Disziplinen immer dann ins Spiel, wenn eine Antwort auf eine Zweifelsfrage im Zusammenhang mit einem IT-System gesucht wird. Ein Beispiel dafür wäre, dass eine ferngesteuerte Drohne zum Transport von Drogen eingesetzt wird, beim Transport aber auf das Grundstück eines Unbeteiligten abstürzt. Die zu Hilfe gerufene Polizei übernimmt die Drohne und soll die Zweifelsfragen klären, wer die Drohne gesteuert hat und welche Routen sie geflogen ist. Dazu sichern die unterstützenden IT-Forensiker die Datenträger der Drohne, analysieren diese und versuchen, Antworten auf die Zweifelsfragen zu geben.

Zugriff gesucht

Eine IT-forensische Untersuchung ist mit zahlreichen Herausforderungen verbunden, mit denen sich die Professur für Digitale Forensik beschäftigt. Eine erste wichtige Herausforderung ist die Frage, wie Daten – insbesondere von innovativen IT-Geräten wie Drohnen oder Autos – gesichert und analysiert werden können. Hintergrund ist, dass diese Geräte oft nur unbekannte Schnittstellen zum Zugriff bieten und die Datenspeicherung im Hinblick auf Partitionierung, Dateisystem und Dateiformat herstellerabhängig ist.

Trainingsdaten gesucht

Eine zweite wichtige Herausforderung ist die Korrektheit von IT-forensischen Tools, was bedeutet, dass diese so arbeiten sollen wie spezifiziert. Dazu werden standardisierte Testdatensätze benötigt. Für diese sind die zu entdeckenden digitalen Spuren a priori bekannt und werden gegen die entdeckten Spuren vom jeweiligen Tool abgeglichen. Solche Datensätze stehen aber der Community nur unzureichend zur Verfügung.

Streue Sand ins Getriebe

Eine dritte bedeutende Aufgabe ist der Umgang mit Anti-Forensik, also allen Maßnahmen seitens des Angreifers, seine Spuren zu verschleiern oder zu vernichten. Anti-Forensik wird seit jeher von Kriminellen angewendet – beispielsweise trägt ein Einbrecher Handschuhe, um keine verräterischen Fingerabdrücke zu hinterlassen. In der digitalen Forensik ist es wichtig, anti-forensische Methoden seitens der Angreifer zu verstehen und zu entdecken.

Prof. Dr. Harald Baier

harald.baier@unibw.de

+49 89 6004 7345

www.unibw.de/digfor

Eine Herausforderung der IT-Forensik besteht darin, Daten zu sichern und zu analysieren.

ABB.: ADOBE STOCK / NOPPONPAT; ADOBESTOCK / MICROGEN

Untersuchung von Selbstbaudrohnen

IT-forensische Datenanalyse: selbstgebaute Drohnen im Fokus der Strafverfolgung

Der dynamisch wachsende Markt für unbemannte Flugsysteme bietet neben kommerziellen Drohnen auch eine Vielzahl an Bausätzen, mit denen sich sogenannte Selbstbaudrohnen herstellen lassen. Drohnen werden zunehmend auch für kriminelle Aktivitäten eingesetzt, um beispielsweise Drogenschmuggel oder Diebstahldelikte vorzubereiten und durchzuführen. Selbstgebaute Drohnen können dabei an spezielle Bedürfnisse angepasst werden.

DROHNEN LASSEN SICH in verschiedene Kategorien einteilen. Die Merkmale dazu sind beispielsweise Größe, Gewicht, Spannweite, Einsatzzweck oder auch regionale Gesetzgebungen.

Strafverfolgung

Bei Ermittlungen im Zusammenhang mit der IT-forensischen Sicherung und Untersuchung digitaler Beweismittel nimmt die Anzahl an Drohnen stetig zu. Bisher werden noch überwiegend kommerzielle Drohnen sichergestellt, die in der Regel mit gebräuchlicher, kommerzieller Software zur Sicherung und Untersuchung bearbeitet werden.

Selbstbaudrohnen

Hersteller von IT-forensischer Software beachten allerdings nicht den Bereich der Selbstbaudrohnen. Bei den auch als DIY-Drohnen (Do-It-Yourself-Drohnen) bekannten Flugsystemen handelt es sich um Bausätze oder Einzelteile, die sich individuell zusammensetzen lassen. Diese Drohnen können im Funktionsumfang und Leistung stark angepasst sein oder bei Verlust niedrigere Kosten verursachen. Mit selbstgebauten Drohnen können beispielsweise die Umgehung von Flugverbotszonen oder das Ausspähen von Liegenschaften ermöglicht werden. Diese Möglichkeiten zur Anpassung führen dazu, dass die kommerziellen Softwarepakete bei der Sicherung und Untersuchung von Selbstbaudrohnen oft nicht verwendbar sind, weil sie keine Möglichkeit der Datensicherung oder -analyse der neuen Schnittstellen und Datenformate anbieten.

Selbstgebaute Drohne der Forschungsgruppe Digitale Forensik, die im Projekt FOCUS zusammen mit weiteren Referenzgeräten zur Datengenerierung dient.

Digitale Forensik

Zur Aufklärung von Straftaten können die auf den sichergestellten Drohnen generierten Daten behilflich sein. Während der Benutzung einer Drohne können Daten wie beispielsweise Flughöhe, Geschwindigkeit, Start- und Rückkehrorte, festgelegte Flugrouten oder auch aufgenommenes Bild- und Videomaterial gesichert werden. Mit Methoden der Digitalen Forensik können die Datenspeicher von Drohnen aufgespürt und ausgelesen werden. Die Strafverfolgungsbehörden können so wichtige Ermittlungshinweise erhalten.

Projekt FOCUS

Die Forensische Untersuchung von Selbstbaudrohnen (FOCUS) adressiert die Erforschung zweier Szenarien im Zusammenhang mit Selbstbaudrohnen:

1. Auffinden im Zusammenhang mit kriminellen Aktivitäten und
2. Verlust während des Einsatzes durch Sicherheitsbehörden.

Der Forschungsschwerpunkt bildet die Extraktion und Analyse gespeicherter Daten. Szenario 1 zielt auf die Sicherung von Beweismitteln ab. Szenario 2 versucht den unbefugten Zugriff auf die Daten der Drohne zu verhindern.

Ziel des Projekts ist es, Empfehlungen für den Einsatz von selbstgebauten Drohnen und Werkzeugketten für forensische Untersuchungen zu entwickeln, die zur Strafverfolgung genutzt werden können.

HptFw d. R. Mario Winkler, M.Sc.
mario.winkler@unibw.de
+49 89 6004 7346
www.unibw.de/digfor

Gefördert durch: BMBF

ABB.: FI CODE / MARIO WINKLER

Besitz oder nicht Besitz …

… das ist hier die Frage: Illegale WhatsApp Sticker auf Android und deren strafrechtliche Verfolgung.

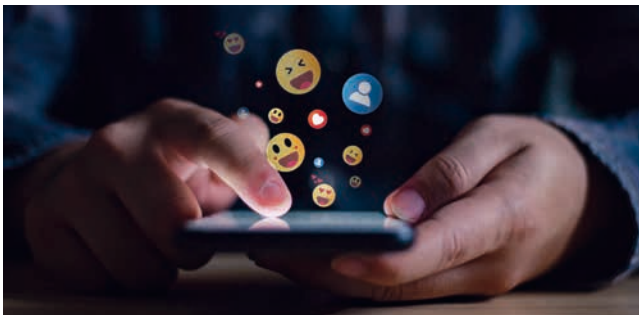
WhatsApp-Sticker sind eine beliebte Mischung aus Emojis und Bildern oder Videos, die von den Nutzern selbst erstellt werden können. Sie unterliegen daher keiner Kontrolle und verbreiten sich automatisch von Nutzer zu Nutzer. Dadurch können sie „viral gehen", nicht nur lustige, sondern auch illegale Sticker. Dies bringt Nutzer und Strafverfolgungsbehörden zunehmend in Bedrängnis.

Sticker von lustig bis illegal

2018 führte Meta Sticker in WhatsApp ein. Seitdem wird die Erstellung und Nutzung immer weiter vereinfacht. Aktuell führt WhatsApp eine Funktion ein, die es wirklich jedem Nutzer ermöglicht, aus einem beliebigen Bild einen eigenen Sticker zu erstellen. Für die Nutzer scheint dies eine gute Nachricht zu sein, denn schließlich werden Sticker meist für legitime Zwecke geteilt. Allerdings tauchen in Chats immer wieder Sticker mit illegalen Inhalten wie Kinderpornografie oder Nazi-Propaganda auf. Solche Sticker beschäftigen daher immer wieder die Strafverfolgungsbehörden und Gerichte. Zum einen gibt es Fälle, in denen Nutzer in ganz normalen Gruppenchats unwissentlich kinderpornografisches Material erhalten haben. Andererseits gibt es auch Fälle, in denen Nutzer willentlich und wissentlich mit solchem Material interagiert haben.

Strafbarer Besitz?

In diesen Fällen geht es juristisch meist um die Frage, ob ein Nutzer im Besitz eines solchen illegalen Stickers war oder nicht. Interessanterweise ist das Konzept des Besitzes zwar leicht auf die digitale Welt übertragbar, aber schwer zu entscheiden. In den meisten Rechtssystemen bedeutet Besitz, dass eine Person die tatsächliche Herrschaft über einen



Die Verfolgung von strafbaren WhatsApp Stickern gestaltet sich schwierig.

Gegenstand, in diesem Fall einen Sticker, hat was einen Besitzwillen einschließt. Dies bedeutet aber, dass technische Unkenntnis zur Entkräftung des Besitzvorwurfs herangezogen werden kann. Es ist offensichtlich nicht im Sinne des Gesetzgebers, dass vorsätzliche Interaktionen z. B. mit kinderpornographischem Material für (vermeintlich) technisch unbedarfte Beschuldigte straffrei bleiben.

Ergebnisse ermöglichen rechtssichere Strafverfolgung

Um Strafverfolgungsbehörden und digitalen Forensikern wertvolle Erkenntnisse zu liefern, hat die Professur für Digitale Forensik eine umfassende digital-forensische Analyse des gesamten Lebenszyklus von Stickern durchgeführt. Die Ergebnisse zeigen unter anderem deutlich, dass das bloße Auffinden eines Stickers auf einem Android-Gerät nicht ausreicht, um auf dessen Besitz zu schließen, da ein Sticker auch ohne Wissen oder Wollen des Nutzers auf dessen Gerät gespeichert werden kann. Um den Besitz oder die Verbreitung von Stickern rechtssicher nachweisen zu können, liefert das Forschungsprojekt auch eine detaillierte Beschreibung von Artefakten und deren Interpretation für die Strafverfolgung,

Es ist zu hoffen, dass dieses Forschungsprojekt einen Beitrag zu den laufenden Bemühungen leistet, die Verbreitung illegaler Inhalte über Messaging-Anwendungen zu bekämpfen, ohne dabei die unschuldigen Nutzer aus den Augen zu verlieren.

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

ABB.: ISTOCK / CHOOCHART CHOOCHAIKUPT

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

Die Forschungsgruppe von Stefan Brunthaler beschäftigt sich primär mit sogenannter sprachbasierter Sicherheit, also der Absicherung von Software durch sprachbasierte Transformationen. Dadurch können auch große Softwaresysteme, wie z. B. Web Browser, vollständig automatisch, transparent und effizient geschützt werden.

DAS Munich Computer Systems Research Laboratory (µCSRL) konnte im vergangenen Jahr seinem Clausewitz'schen Leitspruch „Sprachbasierte Sicherheit ist die Fortsetzung des Übersetzerbaus mit anderen Mitteln" folgen und weiter ausbauen.

Im Jahr 2024 konnten wir den eingeschlagenen Wachstumskurs beibehalten: Zwei Masterstudenten – Matheo Vergnolle und Alina Weber-Hohengrund – der TU München forschten an zwei verschiedenen Projekten und haben ihre jeweiligen Masterarbeiten erfolgreich abgeschlossen. Matheo kam als Student der Ecole Polytechnique über die TU München zu µCSRL und forschte im Rahmen des Dependable Production Systems Projekt an einer Generalisierung der bestehenden Code-basierten Bit Flip Technik zu Daten-basierten Bit Flips. Alina untersuchte neue Diversifikationstechniken um leichtgewichtige, abgeschottete Komponenten unter Verwendung des Oracle Lab's Graal Systems automatisch in bestehende node.js Programme einzuziehen. Neben diesen beiden Masterstudenten konnten wir auch einen neuen Doktoranden zu µCSRL holen: Tim Matussek von der Heinrich-Heine-Universität Düsseldorf ist seit 1. September letzten Jahres wissenschaftlicher Mitarbeiter.

Unserem Plan folgend, konnten wir 2024 mehrere wissenschaftliche Arbeiten in hochkompetitiven und renommierten Konferenzen publizieren. Insgesamt konnten wir zwei Arbeiten bei der 38. European Conference on Object Oriented Programming (ECOOP), eine Arbeit bei der 21. Konferenz zur Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), und eine weitere beim 3. Fuzzing Workshop präsentieren. Neben diesen Konferenzbesuchen waren wir vollzählig beim Workshop der GI Fachgruppe Programmiersprachen und Rechenkonzepte in Bad Honnef. Prof. Brunthaler war zusätzlich beim Workshop der IFIP-Arbeitsgruppe 2.4, Software Implementation Technology, in Lugano und dem DWT SWG Workshop zum Thema „Software Defined Defense" in Bonn.

Aus Forschungsperspektive war 2024 ein sehr produktives Jahr. Einerseits konnten wir als erste Forschungsgruppe neue Optimierungstechniken für den Python Interpreter und dessen C Erweiterungen erforschen und vorstellen (siehe unsere ECOOP'24 Arbeit zu Cross-Module Quickening, in welcher bis zu dreifache Geschwindigkeitssteigerungen beschreiben werden), als auch enorme Forschungsfortschritte im Bereich des Fuzzing erzielen. Dieser Fortschritt zeichnet sich durch die Fertigstellung eines Datacenter-weiten Fuzzing-Systems aus, welches unter anderem auch eine bahnbrechende Anwendung der kombinatorischen Optimierung zur signifikanten Verbesserung der Datacenter-Effizienz beinhaltet. Wir planen die Resultate dieser Forschung 2025 zu veröffentlichen. Im Bereich der Lehre haben wir gemeinsam die Skripten unserer Bachelorvorlesung „Maschinennahe Programmierung" und Mastervorlesung „Compilerbau" auf Jupyter Books umgestellt, welche unter anderem interaktive Inhalte erlauben.

Prof. Dr. Brunthaler war 2024 im Programmkomitee der ACM SIGPLAN International Conference on Object-Oriented Programming Systems, Languages, and Applications (OOPSLA'24 in Pasadena, CA, USA), der IEEE SecDef Konferenz und diente weiterhin als Vorsitzender des „Software Security" Bereichs des *Journal on Systems Research* (*JSys*). Die µCSRL Forschungsgruppe wurde 2024 sowohl vom Bundesministerium der Verteidigung als auch von der Österreichischen Forschungsföderungsgesellschaft (FFG) finanziert.

Prof. Dr. Stefan Brunthaler

brunthaler@unibw.de

+49 89 6004 7330.

https://unibw.de/ucsrl

ABB.: ISTOCK / DE M10

Cross-Module Quickening – C-Erweiterungen und deren Optimierung

Richtungsweisende Modulgrenzen-übergreifende Optimierung von am Beispiel von Python und NumPy

Python verbessert die Produktivität des Programmierers auf Kosten der Ausführungsgeschwindigkeit. Ein enormes Angebot von Bibliotheken erlaubt es Programmierern schnell Anwendungen zu erstellen. In gewissen Situationen ist die mangelnde Geschwindigkeit von Python Programmen inakzeptabel. Für diese Fälle bietet Python sog. C-Erweiterungen an, die Programmierern erlauben, erkannte Flaschenhälse durch C Code zu optimieren.

EIN BEISPIEL FÜR C-Erweiterungen ist NumPy. Python bietet von Haus aus keinen Datentyp für mehrdimensionale, im Speicher zusammenhängende Arrays. Stattdessen sind Pythons Arrays aufgeteilt: Jede Dimension befindet sich in separaten Speicherbereichen. Diese Aufteilung verhindert die Nutzung effizienter SIMD-Befehle, welche für effiziente numerische Berechnungen essenziell sind. NumPy erweitert Python um einen Datentyp, der zusammenhängende Speicherbelegung anbietet und effiziente SIMD-Befehle erlaubt.

Die Leistungsvorteile von C-Erweiterungen wie NumPy sind auf ihre spezifischen Aufgaben, z. B. numerische Berechnungen, begrenzt. Um weitere Optimierungen zu erreichen, gibt es Tools wie Numba und NumPyPy. Numba kompiliert Python-Code zu Maschinencode schränkt dessen dynamisches Verhalten jedoch stark ein. NumPyPy schreibt NumPys C-Code in Python um, damit der PyPy-JIT-Compiler diesen optimieren kann. Beide Ansätze haben Nachteile: Numba muss bei jeder neuen Python-Version aktualisiert werden, während NumPyPy sich ständig an Änderungen in NumPy anpassen muss.

Im September 2024 stellten die µCSRL-Mitglieder Felix Berlakovich und Stefan Brunthaler Cross-Module Quickening (CMQ) vor. CMQ basiert auf Brunthalers Vorarbeiten, die seit Python 3.9 verwendet werden. Diese Resultate beruhen auf der Feststellung das Interpreter JIT-Compiler imitieren können, indem langsame Anweisungen stetig durch schnellere ersetzt werden. Bisher war es jedoch nicht möglich, Modulgrenzen-übergreifend zu optimieren, da Module nach der Kompilierung Blackboxes darstellen. CMQ öffnet diese Blackboxes durch eine sog. Optimierungsschnittstelle. Diese ermöglicht es Erweiterungen, interne Daten offenzulegen. Der CMQ-Interpreter passt sich dynamisch an, um diese Daten zu nutzen und löst damit ein langstehendes Problem der Modulgrenzen-übergreifenden Optimierung.

Der Forschungsprototyp wurde am Beispiel von CPython und NumPy verwirklicht. Nach mehrmonatiger Implementierung konnte die Evaluierung des Prototyps in den NPBench-Benchmarks signifikante Optimierungspotenziale erzielen. CMQ erreichte in einigen Fällen bis zu 3-fache Geschwindigkeitssteigerungen. In Fällen, in denen numerische Berechnungen jedoch die gesamte CPU-Zeit beanspruchen, stellt der Interpreter keinen Flaschenhals dar.

Zusammenfassend stellt CMQ einen maßgebenden Fortschritt dar, um die Optimierungslücke zwischen Python und seinen C-Erweiterungen zu schließen. Die Modulgrenzen-übergreifende Optimierung ermöglicht eine flexible und effiziente Alternative zu bestehenden Ansätzen und macht Python schneller und leistungsfähiger für numerische und wissenschaftliche Berechnungen – essenziell für viele KI-Anwendungen.

Felix Berlakovich
felix.berlakovich@unibw.de
+49 89 6004 7332
www.unibw.de/ucsrl

LOOL: Low-Overhead Optimization-Log-Guided Compiler Fuzzing

Verbesserung der Compiler Fuzzing Effizienz durch Verwendung von Optimierungslogs

Low-Overhead Optimization-Log-Guided Compiler Fuzzing stellt einen neuen Ansatz zur Effizienzsteigerung beim Testen von Compilern vor. Anstelle der traditionellen Code-Coverage-Analyse nutzt LOOL Optimierungslogs – detaillierte Aufzeichnungen von Code-Transformationen – als leichtgewichtige Alternative. Implementiert im GraalVM-Fuzzing-Framework setzt LOOL genetische Algorithmen ein, um ungetestete Compiler-Pfade gezielt zu analysieren und Bugs effizienter zu finden.

COMPILER SIND essenzielle Werkzeuge, die von Entwicklern geschriebenen Code in maschinenlesbare Anweisungen übersetzen. Fehler in Compilern können jedoch zu falschem Verhalten, Abstürzen oder Sicherheitslücken führen, die schwer zu entdecken sind. Um solche Bugs zu identifizieren, greifen Entwickler oft auf Fuzzing zurück, ein Verfahren, das große Mengen Testcode generiert und ausführt, um den Compiler zu analysieren.

Traditionelle Compiler-Fuzzing-Tools verwenden Code-Coverage als Feedback-Steuerungskanal. Code Coverage misst, wie viel der internen Logik eines Compilers durch Testfälle erreicht wird. Diese Methode ist zwar effektiv, hat jedoch Nachteile: Sie ist ressourcenintensiv und verfehlt oft weniger getestete oder komplexere Compiler-Bereiche.

2024 schlugen Felix Berlakovich sowie Wissenschaftler von Oracle Labs Österreich und der Universität Linz eine Alternative vor: Low-Overhead Optimization-Log-Guided Compiler Fuzzing (LOOL). LOOL nutzt Optimierungslogs, die moderne Compiler während des Kompiliervorgangs erzeugen. Diese Logs dokumentieren Analysen und Transformationen wie das Entfernen von Redundanzen oder Performance-Verbesserungen. LOOL verwendet diese Logs als kostengünstige und detaillierte Feedback-Quelle, um den Fokus einer Fuzzingkampagne auf weniger erforschte Compiler-Bereiche zu lenken. Dadurch werden gleichzeitig Effizienz und Bug-Erkennung verbessert.

Zur Bewertung von LOOL wurde ein Prototyp im GraalVM Framework realisiert. Mit Hilfe genetischer Algorithmen konnte Fuzzing gezielt Eingaben generieren, die ungetestete Pfade im Compiler aufdeckten. Besonders wertvoll war diese Methode bei der Analyse komplexer Optimierungen, die mit traditionellen Verfahren schwer zu testen sind. Die Prototypentwicklung dauerte mehrere Monate, da die Integration in GraalVM herausfordernd war. Dennoch zeigte die Evaluierung mit realen Benchmarks signifikante Verbesserungen. LOOL entdeckte teils neue Fehler, die traditionelle Methoden übersehen hatten, und bot durch den geringen Overhead der Optimierungslogs eine effiziente, tiefere Analyse der Compiler-Logik.

Zusammenfassend ist LOOL ein vielversprechender Fortschritt im Compiler-Fuzzing. Es ergänzt traditionelle Tools durch die Nutzung bestehender Compiler-Informationen und erweitert die Möglichkeiten zur Bug-Erkennung. LOOL legt den Grundstein für weitere Innovationen im Testen und Debuggen moderner Compiler, insbesondere von Just-in-Time-Compilern.

Felix Berlakovich

felix.berlakovich@unibw.de

+49 89 6004 7332

www.unibw.de/ucsrl

Prof. Dr. Michaela Geierhos

Data Science

Das interdisziplinäre Team der Professur für Data Science vereint Kompetenzen aus den Bereichen Informatik und Computerlinguistik, um aktuelle und zukunftsorientierte Forschungsfragen in den Bereichen Semantische Informationsverarbeitung und Knowledge & Data Engineering zu bearbeiten.

Angewandte Forschung

Data Science ist eine interdisziplinäre, angewandte Wissenschaft. Ihr Ziel ist es, aus Daten Wissen zu generieren, um beispielsweise Entscheidungsprozesse zu unterstützen. Dabei kommen Methoden und Erkenntnisse aus Bereichen wie Statistik, Informatik und Computerlinguistik zum Einsatz.

Die Professur für Data Science erforscht Methoden zur Informationsgewinnung aus Daten und entwickelt datengetriebene Problemlösungen durch Verarbeitung, Aufbereitung, Analyse und Inferenz großer Datenmengen (Big Data). Dazu zählt insbesondere die Entwicklung von Algorithmen zur (semantischen) Textanalyse, die ihre praktische Anwendung im Social Media Mining findet, das wiederum zur Gefährdungserkennung von Schutzobjekten oder zur Identifikation von Desinformationskampagnen eingesetzt werden kann. Die Art der Daten ist dabei sehr vielfältig: Neben Texten werden auch Audiosignale und Bilder verarbeitet.

Praxisorientierte Lehre

Allen Data Science-Veranstaltungen liegt ein Lehrkonzept zugrunde, das Theorie und Praxis verbindet. Die Studierenden profitieren dabei von Anfang an von der Möglichkeit, das in den Vorlesungen erworbene theoretische Wissen in abwechslungsreichen Übungen und vielfältigen praxisnahen Projekten direkt anzuwenden. Damit leistet die Professur für Data Science einen Beitrag zur exzellenten akademischen Ausbildung der Studierenden an der Universität der Bundeswehr München.

Data Science Use Cases: Praxisorientierte Forschung

Das Data Science-Team unterhält zahlreiche Kooperationen mit Partnern aus Militär, Wirtschaft und dem öffentlichen Sektor, um auch in der Forschung Theorie und Praxis miteinander zu verknüpfen. Die Anwendungsgebiete reichen derzeit von der Erkennung von Desinformationskampagnen über die Identifikation von sogenannten Deepfakes bis hin zum Einsatz von vertrauenswürdiger KI in polizeilichen Anwendungen. Ein Forschungsziel beschäftigt sich mit der permanenten Gefahr von Cyberangriffen. Informationsreiche Cyber-Threat-Intelligence-Berichte bieten tiefgehende Einblicke in die Taktiken, Techniken und Verfahren von Angreifern sowie in die neuesten Bedrohungen und Schwachstellen. Das Ziel ist die Extraktion von strukturiertem Wissen aus diesen Berichten, welches in einen Graphen überführt wird, der wiederum eine zeitliche Analyse sowie die Vorhersage von Zusammenhängen aufgrund bestehenden Wissens im Bereich der Cybersicherheit ermöglicht.

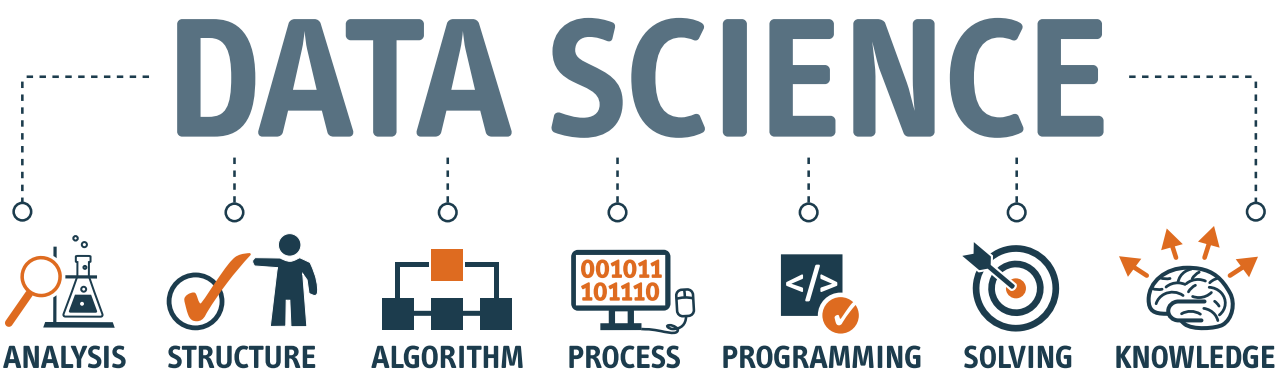
Ein anderes Forschungsziel verfolgt die Entwicklung eines Frühwarnsystems für die Gefährdung von Schutzobjekten durch die Analyse von Aktivitätsdaten in Lauf-Apps sowie nutzergenerierten Daten in anderen sozialen Netzwerken. Nutzer haben oftmals Accounts auf mehreren sozialen Netzwerken, auf denen sie unterschiedliche, persönliche Informationen preisgeben. Durch Zusammenführen aller verfügbaren Informationen können Nutzer eindeutig identifiziert werden, was die Gefahr des Identitätsdiebstahl oder des Social Engineerings erhöht. Eine besondere Gefahr entsteht, wenn Nutzer ihre Geo-Daten aus Lauf-Apps öffentlich teilen. Mit diesen Daten können physische Bewegungsprofile erstellt werden und z. B. militärische Standorte lokalisiert werden. Durch Abgleich solcher Daten mit weiteren vertraulichen Daten (z. B. von militärischen Dienststellen), kann eine Abschätzung der Gefährdungsplausibilität für Personen ermittelt werden.

Prof. Dr. Michaela Geierhos

michaela.geierhos@unibw.de

+49 89 6004 7340

www.unibw.de/datascience



Aufgabenspektrum der Professur für Data Science.

ABB.: ADOBE STOCK / AI FARM; SHUTTERSTOCK / TRUEFFELPIX

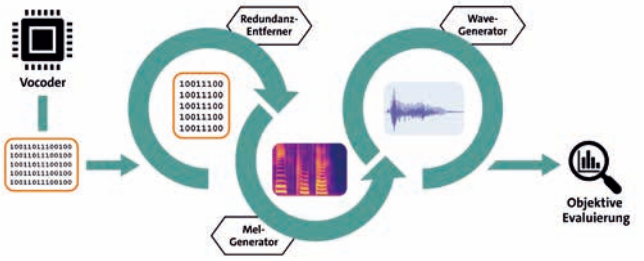
Projekt KI-basierter Audiodecoder

Neuronale Netzwerke zur Sprachsignaldekodierung

Bei der Übertragung von Audiodaten kommen meist proprietäre Vocoder zum Einsatz. Diese bestehen aus zwei Gegenstücken: einem Encoder, welcher die Audiodaten vor der Übertragung beim Sender in einen Bitstrom wandelt und einem Decoder, der den Bitstrom beim Empfänger wieder in ein Audiosignal zurückinterpretiert. Dieses Projekt beschäftigt sich mit der Frage, ob neuronale Netzwerke in der Lage sind, den Decoder zu ersetzen.

Architektur des KI-basierten Decoders

Aufgabe des KI-basierten Decoders ist die Decodierung eines encodierten Bitstroms und die Rekonstruktion der Sprachinformation. Die Rekonstruktion der Bitströme wird durch drei aufeinanderfolgende neuronale Netzwerke realisiert. Im ersten Schritt wird ein Netzwerk zur Entfernung von Redundanz eingesetzt. Das darauffolgende Netzwerk, der Mel-Generator, dient der Umwandlung von redundanzfreien Bitströmen in Mel-Spektrogramme. Abschließend generiert das Wave-Generator-Netzwerk abspielbare Audiodateien im wave-Format. Um die Qualität der generierten Audiodateien automatisiert evaluieren zu können, kommen zwei Methodiken zum Einsatz.



Überblick über die Architektur der drei aufeinanderfolgenden neuronalen Netzwerke zur Erzeugung eines KI-basierten Decoders.

Redundanz-Entferner

Unter Redundanz versteht man Informationen, die zusätzlich zu den eigentlichen Daten übertragen werden. Mittels dieser Informationen können etwaige während der Datenübertragung auftretende Fehler vom Empfänger korrigiert werden. Die nachfolgenden Netzwerke arbeiten auf Basis von redundanzfreien Bitströmen, weshalb dieses Netz Anwendung findet.

Mel-Generator

Mit Hilfe des Mel-Generators werden aus den redundanzfreien Bitströmen sogenannte Mel-Spektrogramme erzeugt, die Audioinformationen in einer diskreten Form darstellen. Die Spektrogramme orientieren sich an der Mel-Skala, welche das menschliche Geräuschempfinden nachahmt. Um die Bandbreite gering zu halten, verwenden die betrachteten Vocoder lediglich eine geringe Abtastrate. Diese kann durch den Mel-Generator so erhöht werden, dass CD-Qualität erreicht wird.

Wave-Generator

Das Generieren von abspielbaren wave-Dateien aus Mel-Spektrogrammen ist ein oftmaliger Bestandteil von Text-to-Speech Systemen, weshalb in diesem Forschungsbereich bereits vielversprechende Frameworks (z. B. MelGAN oder HifiGAN) existieren und hier zum Einsatz kommen.

Evaluierung

Zur objektiven Evaluierung der resultierenden Audiodateien und somit der Sprachrekonstruktion werden zwei Verfahren verwendet:

1. **Basierend auf Transkription:** Ein neuronales Netzwerk transkribiert die Audiodaten und das Transkriptionsergebnis wird anschließend mit dem originalen Transkript des Audiodatensatzes verglichen.

2. **Basierend auf Audiobewertungsalgorithmen:** Zur Bewertung von Kommunikationskanälen existieren Algorithmen, die zwei Audiosignale miteinander vergleichen. Das Vergleichsergebnis ist meist ein Wert zwischen 1 („unverständlich“) und 5 („keine Qualitätseinbußen“) auf der Mean-Opinion-Skala.

Hendrik Bothe, M.Sc.
hendrik.bothe@unibw.de
+49 89 6004 7343
https://go.unibw.de/vocoder

ABB.: FI CODE / H. BOTHE

Projekt KiTIE

Identifikation und Evaluation von Kooperationspartnern anhand von Patentinformationen

Der Technologietransfer, insbesondere bei Großforschungseinrichtungen, wird durch die komplexe und zeitaufwendige Suche nach passenden Kooperationspartnern erschwert. Angesichts zunehmend vernetzter Innovationsprozesse wird im Projekt KiTIE eine intelligente Plattform entwickelt, die durch die Analyse von Patent-, Publikations- und Unternehmensdaten potenzielle Partner für Forschungseinrichtungen systematisch identifiziert.

Wie funktioniert das intelligente Partner-Matching?

Die Plattform verarbeitet Daten wie u. a. Patente, wissenschaftliche Publikationen, Forschungsprojekte, Webseitentexte und Unternehmensinformationen potenzieller Partner mittels semantischer Analyse und KI-Methoden. Der Matching-Prozess beginnt mit der Eingabe einer Technologiebeschreibung und umfasst folgende Schritte:

1. **Patentklassen-Zuordnung:** Klassifikation von Technologiebeschreibungen in Patentklassen durch Kombination von semantischer Suche und Large Language Models (LLM).

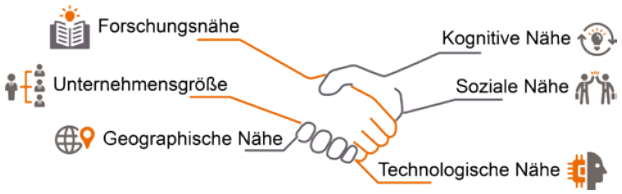
2. **Unternehmensprofiling:** Analyse und Klassifikation von Unternehmensdaten zur Erstellung technologischer Unternehmensprofile auf Basis von Patentklassen.

3. **Matching-Analyse:** Vergleich von Technologiebeschreibung und Unternehmensprofil hinsichtlich technologischer Nähe und technologischer Komplementarität.

Warum ist intelligentes Partner-Matching relevant?

Die traditionelle Partnersuche im Technologietransfer basiert oft auf persönlichen Netzwerken und erreicht damit ihre Grenzen bei zunehmend komplexen technologischen Fragestellungen. Eine datengestützte Bewertung potenzieller Partner auf Basis verschiedener Datenquellen und Indikatoren wird zum Schlüsselfaktor für Technologietransfer. Im Projekt KiTIE analysiert ein mehrdimensionales Bewertungssystem die Eignung potenzieller Partner anhand definierter Nähe-Indikatoren:

- **Forschungsnähe:** Übereinstimmung wissenschaftlicher Schwerpunkte
- **Technologische Nähe:** Kompatibilität der Patentportfolios
- **Kognitive Nähe:** Ähnlichkeit in Innovationsprozessen
- **Soziale Nähe:** Bestehende Kooperationsbeziehungen
- **Strukturelle Nähe:** Geografische und organisatorische Kompatibilität



Die KiTIE-Plattform berücksichtigt verschiedene Indikatoren zwischen Organisationen, um optimale Kooperationspartner zu ermitteln.

Entwicklung der interaktiven KiTIE-Plattform

Die Plattform ermöglicht Forschenden auf Basis ihrer Projektbeschreibung passende Kooperationspartner zu identifizieren. Für die Suchergebnisse wird ein Matching-Score berechnet, der die Eignung der Kandidaten quantifiziert. Die interaktive Benutzeroberfläche bietet flexible Filteroptionen an und stellt die Matching-Ergebnisse auf transparente Weise dar. Die aufbereiteten Unternehmensprofile mit relevanten Kennzahlen und Informationen ermöglichen eine fundierte Entscheidungsfindung. Die Analyseergebnisse lassen sich in interaktiven Netzwerkvisualisierungen erkunden und ermöglichen detaillierte Partnervergleiche. Ein Prototyp durchläuft derzeit einen systematischen Entwicklungs- und Evaluierungsprozess. Daher ist die Gestaltung nutzerorientiert mit Integration von Pilot-Anwendungsfeedback und die Plattform-Funktionalitäten werden iterativ implementiert. Zudem findet eine kontinuierliche Anpassung an reale Nutzungsszenarien statt.

Benjamin Vehmeyer, M.Sc.
benjamin.vehmeyer@unibw.de
+49 89 6004 7341
https://go.unibw.de/kitie

Gefördert durch:
Bundesministerium für Bildung und Forschung

ABB.: FI CODE / B. VEHYMEYER

Prof. Dr. Marta Gomez-Barrero

BioML: Biometrics and Machine Learning Lab

Das BioML Lab unter der Leitung von Prof. Dr. Marta Gomez-Barrero erforscht Methoden zur Entwicklung zuverlässiger, sicherer, fairer und datenschutzfreundlicher biometrischer Erkennungssysteme. Der Schwerpunkt der Gruppe liegt auf hochinnovativer und angewandter interdisziplinärer IT-Sicherheitsforschung, basierend auf Architekturen des Machine/Deep Learnings sowie auf kryptografischen Methoden.

BioML: Biometrics and Machine Learning Lab

Das BioML Lab wurde im Oktober 2023 eingerichtet und ist Teil des Forschungsinstituts CODE und der Fakultät für Informatik. Unter der Leitung von Prof. Dr. Marta Gomez-Barrero erforscht BioML Methoden zur Entwicklung zuverlässiger, sicherer, fairer und datenschutzfreundlicher biometrischer Erkennungssysteme. Zu diesem Zweck sind Kenntnisse in Algorithmen des Machine/Deep Learnings und der Kryptographie erforderlich.

BioML co-organisiert und nimmt an internationalen akademischen Konferenzen wie IEEE Int. Joint Conference on Biometrics (IJCB) und IEEE Int. BIOSIG Conference teil und leistet einen Beitrag sowohl zur European Association for Biometrics (EAB) als auch zur internationalen Normung in ISO/IEC JTC1 SC37.

Forschungsschwerpunkte am BioML Lab

Unter biometrischer Erkennung versteht man die automatische Erkennung von Personen auf der Grundlage ihres Verhaltens und ihrer biologischen Charakteristika. Beispiele für Charakteristika, mit denen die Gruppe arbeitet, sind Gesicht, Iris, Fingerabdruck, Fingervenen oder handschriftliche Unterschriften sowie Kombinationen dieser Merkmale in multibiometrischen Systemen. Neben dem Versuch, die Erkennungsgenauigkeit und die Recheneffizienz der Systeme zu erhöhen, konzentrieren wir uns auf andere wichtige Aspekte dieses Forschungsgebiets. Die Wahrung der Privatsphäre der Subjekte steht im Mittelpunkt unserer Forschung, wofür wir biometrische Vorlagenschutzsysteme in Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO) und den einschlägigen ISO-Normen nach dem Prinzip Privacy-by-Design entwickeln. Darüber hinaus ist die Erkennung verschiedener Formen von Angriffen auf biometrische Systeme (z. B. Präsentationsangriffe oder Morphing-Angriffe) der Schlüssel zur Erhöhung der Sicherheit und Zuverlässigkeit der Systeme. Nicht zuletzt zielt das Team auf die Erklärbarkeit und Transparenz der Algorithmen ab, um die Akzeptanz und den Einsatz der biometrischen Erkennung zu fördern.

Aktivitäten

2024 war ein lebhaftes und ereignisreiches Jahr im BioML-Labor. Drei Forscher traten der Gruppe bei: Erik Trolliet, Osman Demir, und Camilo Linares. Sie begannen mit der Erforschung verschiedener Themen: biometrische Template-Schutzsysteme auf der Grundlage von Deep Hashes für Iris- und Fingerabdruckproben; Methoden zur Erkennung von Präsentationsangriffen auf Iris- und Gesichtsbilder; die Vorteile großer Sprachmodelle für die biometrische Erkennung; und die Verwendung synthetischer Daten zur Verbesserung biometrischer Systeme.

Auf internationaler Ebene haben wir unsere Zusammenarbeit durch verschiedene Aktivitäten verstärkt. Gemeinsam mit Vedrana Krivokuca und Sébastien Marcel von Idiap (Schweiz) und Arun Ross von der Michigan State University (USA) geben wir das in Kürze erscheinende Springer „Handbook on Biometric Template Protection“ heraus. Marta Gomez-Barrero leitet auch den Review der ISO/IEC-Norm 30136 über „Performance testing of biometric template protection schemes“, die auf der letzten Sitzung des ISO SC 37 in Wellington das Stadium der CD erreicht hat. Über die European Association for Biometrics (EAB) haben wir den Martigny Biometrics Workshop gemeinsam mit dem US Center for Identification Technology Research (CITeR) und dem Idiap Research Institute organisiert. Außerdem haben wir erneut die Darmstädter Biometrie-Woche zusammen mit dem Fraunhofer IGD organisiert. Wir haben auch neue Initiativen gestartet, wie z. B. den EAB Council of Wisdom, bei dem Experten Fragen der Öffentlichkeit zu verschiedenen Themen im Zusammenhang mit biometrischer Erkennung beantworten.

Prof. Dr. Marta Gomez-Barrero
+49 89 6004 7425
marta.gomez-barrero@unibw.de
www.unibw.de/bioml

ABB.: ADOBE STOCK / DILOK; FI CODE / MARTA GOMEZ-BARRERO

Synthetic Data and Biometrics

Advantages and Challenges of Using Synthetic Data in Biometric Recognition Systems

Synthetische Gesichtsbilder können für die Erstellung von Deepfakes verwendet werden, höchstwahrscheinlich in böser Absicht, aber sie können auch guten Zwecken dienen. Wenn wir zum Beispiel in der Lage wären, Bilder von unterrepräsentierten Minderheiten in unseren Trainingsdaten zu erzeugen, könnten wir die Bias gegenüber diesen Gruppen bekämpfen. Trotz der zahlreichen Ansätze zur Erzeugung synthetischer Bilder ist ihr Nutzen für die biometrische Erkennung noch nicht klar.

Synthetische Daten für die Biometrie

Es gibt eine Reihe von Gründen für die Verwendung synthetischer Daten in biometrischen Erkennungssystemen. Zunächst einmal ist es nicht immer möglich, die großen Datensätze zu sammeln, die für das geeignete Training von Deep-Learning-Algorithmen erforderlich sind. Durch die Verwendung synthetischer Daten können wir also die Größe unserer Datensätze erhöhen. Außerdem können wir uns auf unterrepräsentierte Gruppen konzentrieren (z. B. ältere Menschen bei der Datenerfassung an einer Universität oder ethnische Gruppen, die in einem bestimmten Gebiet weniger präsent sind), so dass das biometrische System lernt, sie richtig zu erkennen. Aus einem anderen Blickwinkel betrachtet könnte die Verwendung synthetischer Daten anstelle echter Daten die Risiken für den Schutz der Privatsphäre verringern, die sich aus einer Datenverletzung ergeben.

Biometrische Qualität und Diversität

Trotz der großen Zahl von Veröffentlichungen über die Erzeugung synthetischer Gesichtsbilder gibt es immer noch einige Probleme bei deren Verwendung für biometrische Zwecke. In erster Linie weisen diese synthetischen Bilder, auch wenn sie visuell realistisch sind, nicht immer eine hohe biometrische Qualität auf. Dies bezieht sich nicht nur auf die Schärfe des Bildes, sondern auch auf andere Eigenschaften, die zu einer schlechten Erkennungsleistung führen können: ein extremer Gesichtsausdruck oder eine schlechte Ausleuchtung. Ebenso leiden viele Modelle unter einer geringen Vielfalt: nur eine Handvoll Identitäten kann synthetisiert werden. Für large-scale biometrische Anwendungen benötigen wir jedoch eine entsprechend große Anzahl von Identitäten, um die Variabilität von realen Personen erfassen zu können.

Synthetische Gesichter können das Training biometrischer Erkennungssysteme verbessern.

ABB.: ADOBE STOCK / STUDIO F.

Benchmark

In Anbetracht der oben genannten Herausforderungen führen wir ein Benchmarking verschiedener Modelle durch, die auf Generative Adversarial Networks (GANs) oder Diffusionsmodellen basieren, um die biometrische Qualität und Vielfalt zu bewerten. Zu diesem Zweck verwenden wir sowohl traditionelle Qualitätsmetriken wie BRISQUE als auch die Open Source Face Image Quality (OFIQ) des deutschen BSI, die demnächst in die ISO/IEC 19794-5 als Standardimplementierung von Qualitätsmetriken für Gesichtsbilder aufgenommen wird. Wir schätzen auch, wie viele Identitäten aus den verschiedenen Modellen generiert werden können. Die nächsten Schritte werden sich auf die besten Modelle konzentrieren, um einen großen synthetischen Datensatz zu generieren, den wir zur Verbesserung verschiedener Aspekte biometrischer Erkennungssysteme nutzen werden.

Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml

Biometrische Daten und Datenschutz

Wie man Deep Hashes aus Irisbildern extrahiert

Ein gängiger Ansatz zum Schutz von Passwörtern, sowohl für die Speicherung als auch für die Übertragung, verwendet kryptographische Hashes. Bei biometrischen Daten, wie z. B. Irisbildern, können wir aufgrund der verrauschten Natur biometrischer Daten keine gängigen Hash-Algorithmen wie die SHA- oder MD-Familien verwenden: ein einziger Bitwechsel führt zu völlig unterschiedlichen Hashes. Wir müssen daher andere Möglichkeiten zur Extraktion von Hashes aus Irisbildern erforschen.

Was ist der Schutz biometrischer Vorlagen?

Biometrische Daten werden in der Europäischen Datenschutzgrundverordnung (DSGVO) als sensible personenbezogene Daten eingestuft. Um biometrische Systeme einsetzen und nutzen zu können, müssen die Daten daher durchgängig geschützt werden: bei der Speicherung, der Übertragung und jeder Art der Verarbeitung. Die Norm ISO/IEC 24745 definiert die Eigenschaften, die so genannte biometrische Template-Protection-Schemata (BTP) erfüllen müssen, und die Norm ISO/IEC 30136 enthält Leitlinien für die Prüfung dieser Schemata im Hinblick auf den Schutz der Privatsphäre.

Deep Hashes

Unter den verschiedenen BTP-Methoden, die in den letzten zwei Jahrzehnten entwickelt wurden, gibt es einen neuen Trend, bei dem Deep-Learning-Algorithmen nicht nur für die biometrische Erkennung, sondern auch für den Schutz der zugrunde liegenden Daten eingesetzt werden. Wir haben uns insbesondere auf die Verwendung von binären Codes mit maximaler Entropie (MEB) konzentriert, die bereits aus Gesichtsbildern extrahiert wurden. Dieser Ansatz besteht aus drei Schritten: 1) Zunächst verwenden wir ein neuronales Faltungsnetzwerk (CNN), um Schablonen mit einer reduzierten Variabilität innerhalb der Klasse zu erzeugen (z. B. führen zwei Gesichtsbilder derselben Person zu sehr ähnlichen Schablonen); 2) dann kombinieren wir diese Schablonen mit vordefinierten MEB-Codes; und 3) wir wenden allgemeine kryptografische Hashes auf diese Codes an, um die endgültigen geschützten Schablonen zu erzeugen (ähnlich wie beim textbasierten Passwortschutz). Eine solche Methodik hat mehrere Vorteile: Die kryptografische Hash-Funktion ist

Um die Privatsphäre der Menschen zu schützen, können Deep Hashes von Iris-Bildern extrahiert werden.

nicht umkehrbar, und es sollte sehr schwierig sein, einen MEB-Code aus seinem Hash wiederherzustellen; selbst wenn ein MEB-Code wiederhergestellt wird, verrät er nicht die Gesichtsvorlage, der er zugewiesen wurde; und wir können im Falle einer Kompromittierung neue MEB-Codes zuweisen (denken Sie daran, dass wir ein Passwort ändern können, aber nicht unser Gesicht oder unsere Iris!). Die größte Herausforderung besteht in der Generierung von Vorlagen, die eine geringe Variation innerhalb der Klasse aufweisen.

Deep Iris-Hashes

Irisbilder weisen eine geringere Varianz zwischen den Aufnahmen auf als Gesichtsbilder. Daher haben wir uns bisher auf dieses biometrische Merkmal konzentriert. Mit einem leichtgewichtigen CNN haben wir 256-Bit MEB-Codes generiert und dann SHA-512 angewendet. In einer Datenbank mit 100 Probanden erreichten wir eine vielversprechende False Match Rate von 7 %. Dies ist natürlich höher als die Fehlerraten, die mit ungeschützten Daten erzielt werden: Wir werden weiter daran arbeiten, diese Fehler zu verringern und auch weitere Eigenschaften zum Schutz der Privatsphäre analysieren, wie z. B. die Unverknüpfbarkeit von Vorlagen, die in verschiedenen Anwendungen erfasst wurden.

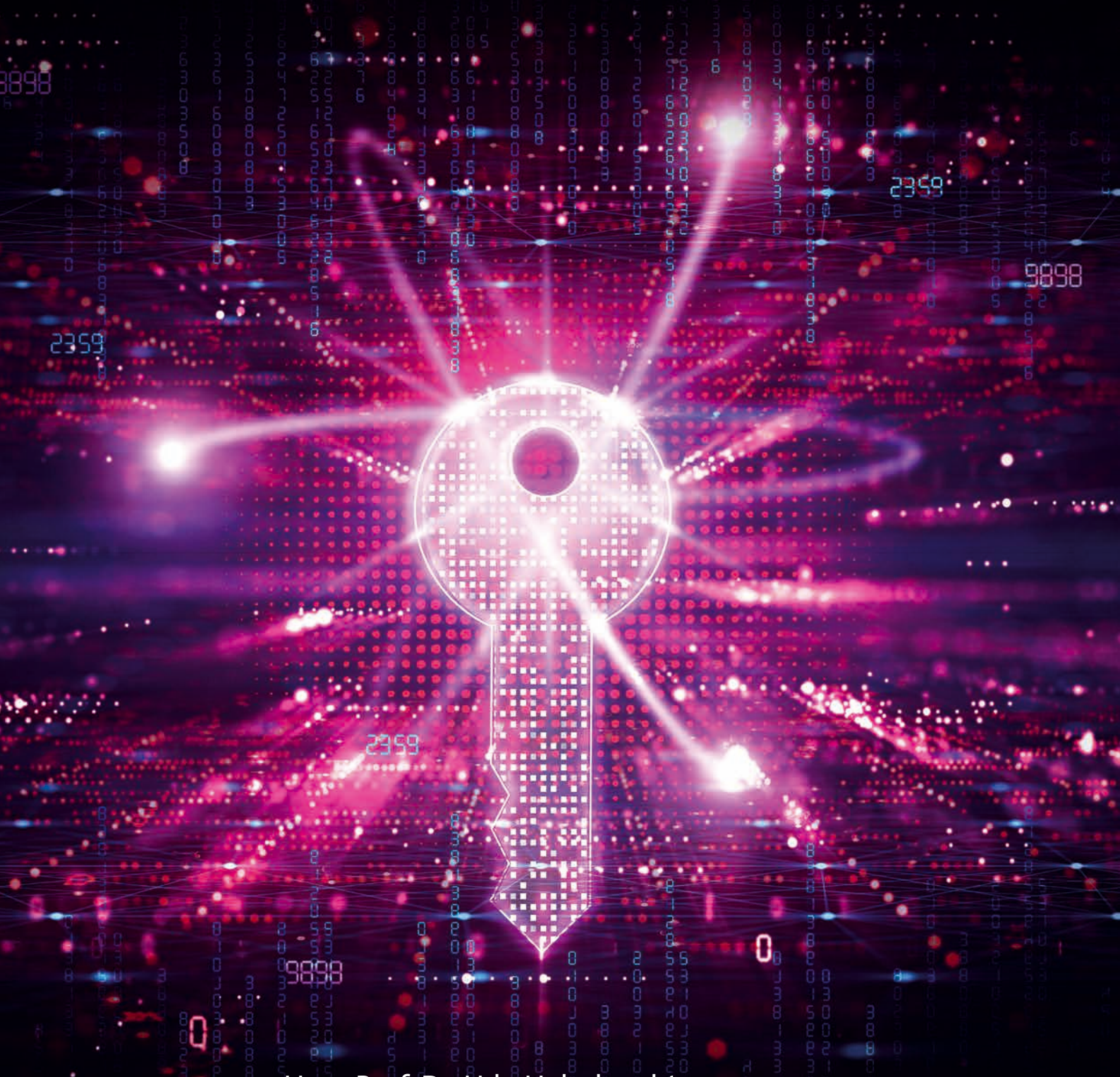
Prof. Dr. Marta Gomez-Barrero

+49 89 6004 7425

marta.gomez-barrero@unibw.de

www.unibw.de/bioml

ABB.: ADOBE STOCK / TANYA



Hon.-Prof. Dr. Udo Helmbrecht

Quantenkommunikation

Im Rahmen von dtec.bw wird im Projekt MuQuaNet ein Quantennetz im Großraum München mit akademischen und industriellen Partnern aufgebaut. Ziel ist der Test- und Forschungsbetrieb eines Quantenkommunikationsnetzes mit ausgewählten zivilen und militärischen Anwendungen.

MuQuaNet: Pionierarbeit für quantensichere Kommunikation im Großraum München

Im Rahmen des Forschungsprojekts MuQuaNet (Münchner Quantennetz) wird im Großraum München ein Quantennetz in Zusammenarbeit mit akademischen und industriellen Partnern aufgebaut. Dieses Vorhaben, das durch dtec.bw gefördert wird, verfolgt das Ziel, eine zukunftsweisende Kommunikationsinfrastruktur zu entwickeln, die auf quantenmechanischen Phänomenen beruht und Quantenobjekte nutzt um höchste Sicherheitsstandards zu erfüllen. Durch den Einsatz von Quantenschlüsselverteilung (QKD) soll die sichere Übertragung von Daten sowohl für zivile als auch militärische Anwendungen erforscht und getestet werden.

Ziele und Ansatz

Das Hauptziel von MuQuaNet ist der Aufbau, die Evaluation und der Testbetrieb eines Quantennetzes, das moderne Sicherheitsanforderungen erfüllt und innovative Ansätze zur Datenübertragung bietet. Dabei liegt ein Fokus auf der Erprobung der praktischen Anwendbarkeit von QKD in realen Szenarien, insbesondere in sicherheitskritischen Bereichen wie der Verteidigung. Die Infrastruktur verbindet verschiedene Standorte, darunter den Campus der Universität der Bundeswehr (UniBw), sowie Partnerinstitutionen wie das Deutsche Zentrum für Luft- und Raumfahrt (DLR), die Ludwig-Maximilians-Universität (LMU), Airbus und weitere Partner aus Industrie und Wissenschaft.

Schlüsselmanagement als Kernpunkt

Ein zentrales Element des Projekts ist das Management der Schlüssel, das die Basis für die Sicherheit in QKD-Systemen bildet. Herausforderungen wie fehlende Standards und die Zuverlässigkeit von Zwischenknoten werden durch innovative Ansätze wie das im Projekt entwickelte Multi-Path-Key-Reinforcement (MKR) adressiert. Dieses Verfahren verteilt Schlüsselmaterial über mehrere Pfade, um die Robustheit und Sicherheit in komplexen Netzen zu erhöhen.

Anwendungsbeispiel: VR-Fernwartung einer Fregatte

Ein prominenter Use Case des Projekts ist die Fernwartung von Fregatten mittels Virtual Reality (VR) über Satellitenlinks. Hierbei wird QKD eingesetzt, um die hohen Sicherheitsanforderungen dieser sensiblen Kommunikationsszenarien zu erfüllen. MuQuaNet entwickelte hierzu ein spezielles Freistrahl-QKD-System in Zusammenarbeit mit der LMU, und untersuchte zusammen mit dem DLR die Integration in Satellitenkommunikation. Diese Arbeiten unterstreichen die Bedeutung von QKD für sicherheitskritische militärische Anwendungen.

3D-gedrucktes Fregattenmodell mit Sensoren für die QKD-verschlüsselte Fernwartung via VR-Brille.

Perspektiven und Nutzen

MuQuaNet leistet einen wesentlichen Beitrag zur Entwicklung sicherer Quantenkommunikationssysteme und unterstützt die Bundeswehr sowie andere Behörden beim Schutz sensibler Daten. Die im Projekt gewonnenen Erkenntnisse und Technologien werden nicht nur den wissenschaftlichen Fortschritt vorantreiben, sondern auch die industrielle Innovationskraft stärken. Perspektivisch soll das Netz um weitere Standorte, Anwendungen und Partner erweitert werden, um die Praxistauglichkeit von QKD in verschiedenen Szenarien zu optimieren und die europäische Führungsposition im Bereich der quantensicheren Kommunikation zu festigen.

Prof. Dr. Wolfgang Hommel

wolfgang.hommel@unibw.de

+49 89 6004 2495

www.unibw.de/muquanet

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

ABB.: SHUTTERSTOCK / ARTEMISDIANA; FI CODE / S. KASTRUP

3-km-Freistrahl-QKD Testumgebung

Ein selbstentwickelter Decoy-State-Sender ermöglicht robuste QKD unter realistischen atmosphärischen Bedingungen.

Der 3-km-Freistrahl-QKD-Link von MuQuaNet zwischen ETTI und Airbus zeigt robuste QKD unter realistischen Outdoor-Bedingungen. Der von LMU und UniBw entwickelte Decoy-State-BB84-Sender (850 nm) benötigt minimalen SWaP, entscheidend für mobile QKD. Die Bodenstrecke ist Atmosphäreneffekte ausgesetzt, vergleichbar mit einem LEO (Low Earth Orbit) Satellit-zu-Boden-Downlink.

EIN SCHRITT IN Richtung praktischer Quantenkommunikation ist der 3 km lange Freistrahl-QKD-Link zwischen der Universität der Bundeswehr München und Airbus. Herzstück dieses selbst entwickelten Demonstrators ist ein 850-nm-Decoy-State-BB84-Sender, dessen minimales Größen-, Gewichts- und Leistungsprofil (SWaP) realen Anforderungen gerecht wird – von bodengestützten Outdoor-Anwendungen bis zu anderen möglichen Szenarien mit begrenztem Bauraum. Das System arbeitet mit einer Modulationsrate von 100 MHz und verwendet einen FPGA für die Signalerzeugung sowie zur präzisen Anpassung der Quantenprotokoll-Parameter.

Vorläufige Messungen bei Tageslicht (17 Uhr) ergaben etwa 500 Bit/s sichere Schlüsselrate, mit deutlichem Potenzial zur Steigerung durch Optimierungen an optischen Komponenten, Strahlausrichtung und QKD-Parametern. Es ist geplant schnelle Spiegel zu verwenden um Strahlabweichungen durch Turbulenzen, Vibrationen und Temperaturgradienten zu kompensieren. Zudem eröffnet die zusätzliche Nutzung des 1550-nm-Beacons für klassische Kommunikation die Möglichkeit eines komplett eigenständigen Systems. Aktuelle Weiterentwicklungen setzen auf höhere Stabilität, niedrigere Fehlerraten und bessere Wartbarkeit – allesamt entscheidend für reale Einsatzszenarien.

Offene Tests unter freiem Himmel zeigen, wie Luftfeuchtigkeit, Lichtverschmutzung und Temperaturschwankungen QKD-Experimente außerhalb streng kontrollierter Labore beeinflussen. Selbst kleine Umweltschwankungen können die optische Kopplung stören oder das Hintergrundrauschen verändern, was Anpassungen bei Strahlausrichtung und QKD-Parametern erfordert. Durch das Protokollieren dieser Faktoren zusammen mit Leistungsdaten können Hardware und Steuerungsalgorithmen gezielt verbessert werden, um das System langfristig robuster zu machen.

Obwohl dieser Link in erster Linie als Kurzstrecken-Demonstrator fungiert, leistet er auch einen Beitrag zu den Zielen von MuQuaNet, indem er Hinweise liefert, wie Freistrahl-QKD in größere Netzwerke eingebunden werden kann. Die dabei gewonnenen Daten helfen, Strategien zur Skalierung von QKD zu entwickeln, da die dichte Atmosphäre über 3 km ähnliche Effekte zeigt wie ein 500-km-Low-Earth-Orbit Satellit-zu-Boden-Downlink.

Dieser Freistrahl-QKD-Link dient als wichtige Testumgebung für die Integration von Quantensicherheit in reale Kommunikationsinfrastrukturen. Die Erkenntnisse sollen auch die Entwicklung von Satelliten-QKD voranbringen, wo eine Anpassung an atmosphärische Einflüsse essenziell ist, um eine robuste globale quantenkryptografische Abdeckung zu erreichen.

Michael Auer

michael.auer@unibw.de

+49 89 6004 7374

https://go.unibw.de/eq

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

Sicherheitsanalysen von QKD Geräten

Im Berichtszeitraum lag der Schwerpunkt der Arbeit auf der Evaluierung von Sicherheitsrisiken und der Entwicklung von Gegenmaßnahmen bei Angriffen auf QKD-Systeme. Die Analysen sind dabei in drei Bereiche einteilbar: Quantum Hacking, klassische IT-Angriffsvektoren und Analyse der elektromagnetischen Abstrahlung.

Quantum Hacking

Quantum Hacking beschreibt die Angriffe auf quantenoptische Komponenten um Schlüsselmaterial zu manipulieren oder den Schlüsselraum einzuschränken.

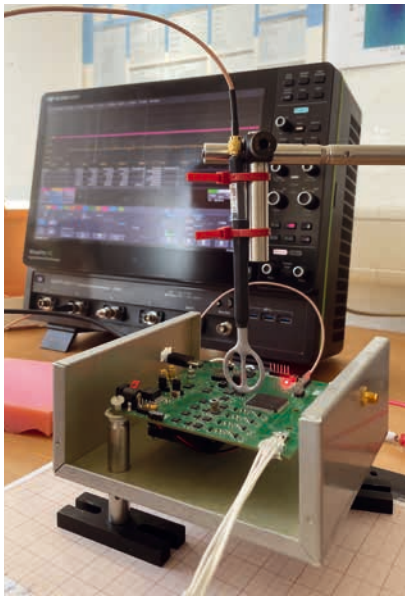
Grundlage hierfür ist der im Jahre 2023 veröffentlichte BSI Bericht „Implementation Attacks against QKD Systems“, in dem eine große Anzahl von quantenoptischen Angriffsvektoren aus wissenschaftlichen Veröffentlichungen systematisch zusammengefasst und kategorisiert wurden.

Zusammen mit einem Hersteller wurde der Angriff „Detector Efficiency Mismatch“ auf einem kommerziell verfügbaren QKD System durchgeführt.

Bei diesem Angriff werden manche der für die Technologie notwendigen Detektoren gezielt ausgeschaltet bzw. in der Effizienz eingeschränkt, um den Schlüsselraum zu beeinflussen. Das gewonnene Schlüsselmaterial wurde anschließend mit statistischen Methoden analysiert. Dabei konnten wir nachweisen, dass die vom Hersteller implementierte proprietäre Gegenmaßnahme diesen Angriff wirksam entkräftet.

Klassische IT-Angriffsvektoren

In dem Projektteil wurden klassische Penetrationstests auf die IT-Komponenten der QKD-Geräte durchgeführt.



Messung elektromagnetischer Emissionen einer QKD-Komponente.

Nach einer initialen Reconnaissance, konnte mithilfe von verschiedenen Scanningmethoden ein initialer Zugang identifiziert werden.

Mithilfe von Privilege Escalation konnten Adminrechte auf dem Gerät erhalten werden, um Persistenz herzustellen. Außerdem hätten Daten exfiltriert werden können.

In einem Responsible Disclosure Verfahren wurden gefundene Schwachstellen den jeweiligen Herstellern gemeldet und Hilfestellung bei ihrer Beseitigung gegeben.

Das Projekt trägt damit zur Stärkung der IT-Sicherheit deutscher QKD-Lösungen bei.

Analyse der elektromagnetischen Abstrahlung

QKD-Geräte können elektromagnetische Abstrahlung produzieren, welche mit speziellem Equipment gemessen werden kann. Die gesammelten Daten können korreliert werden und potentiell Rückschlüsse auf das generierte Schlüsselmaterial zulassen. In einem ersten Experiment konnte hier rohes Schlüsselmaterial ausgelesen werden. Weitere Experimente sowie Konzepte zum Schützen vor dieser Art von Angriffen sind hier aktuell in der Planung.

David Koch
david.koch@unibw.de
+49 89 6004 1728
https://go.unibw.de/em

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

dtec.bw Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union NextGenerationEU

ABB.: MUQUANET / M. KAACK

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

Das Team von Wolfgang Hommel forscht unter dem Leitmotiv „Entwicklung und Betrieb sicherer vernetzter Anwendungen“ an technischen und organisatorischen Sicherheitsmaßnahmen für komplexe IT-Infrastrukturen und Kommunikationsnetze mit erhöhtem Schutzbedarf sowie deren praktischem Einsatz.

DAS TEAM DER Professur für IT-Sicherheit von Software und Daten verfolgt das Ziel, Lösungen für praxisrelevante Security-Fragestellungen unter Berücksichtigung der im Betrieb komplexer IT-Infrastrukturen anzutreffenden operativen Randbedingungen zu erarbeiten.

Am Anfang der Forschungsarbeiten und Projekte mit Dritten steht deshalb meist eine umfassende empirische Analyse, bei der beispielsweise relevante Komponenten aus dem designierten Einsatzgebiet in virtuellen Umgebungen detailgetreu abgebildet oder zumindest in ihrem Kern modelliert und per Simulation nachgebaut und analysiert werden. Dieser Ansatz ermöglicht unter anderem die explorative Anwendung offensiver Testverfahren und somit die qualitative und quantitative Analyse von Schwachstellen in komplexen mehrstufigen Angriffsszenarien. Daraus können systematisch Sicherheitsanforderungen abgeleitet werden, die als Grundlage für die nachfolgenden konstruktiven Tätigkeiten und eine spätere praktische Evaluation erzielter Resultate dienen.

Die Konstruktion neuer und verbesserter IT-Sicherheitsmaßnahmen folgt einem Security-Engineering-Ansatz: Sie werden einerseits auf technischer Ebene konzipiert, modelliert und simuliert und andererseits unter organisatorischen Aspekten möglichst nahtlos in die Design-, Einführungs- und Betriebsprozesse der vorgesehenen Anwendungsgebiete integriert. Wesentlicher Anspruch ist die konkrete Implementierung mit anschließender Evaluation, die mindestens im Labor, möglichst aber auch in konkreten Pilotumgebungen und im Idealfall durch individuelle Einbettung in wissenschaftlich begleitete Projekte erfolgt. Ebenso werden die Rolle des Faktors Mensch in der Informationssicherheit, ökonomische und rechtliche Randbedingungen berücksichtigt.

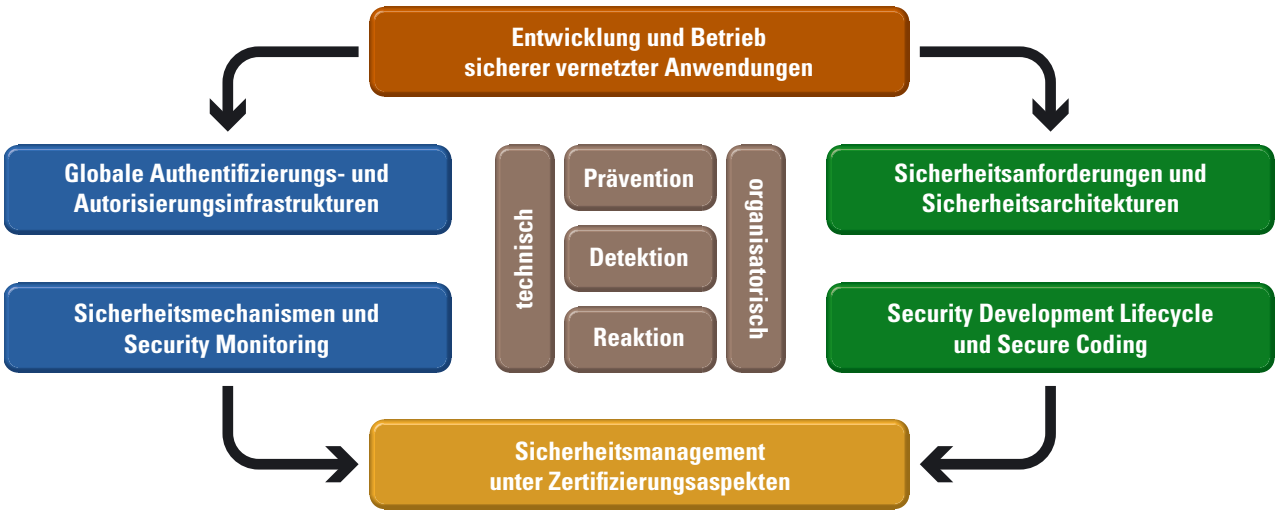
In laufenden Forschungsvorhaben und Projekten wurde 2024 unter anderem an der Adaption von Security Information & Event Management (SIEM) Systemen an Low-latency-Anforderungen und neuartige Bedrohungen gearbeitet. Innovative Ansätze zur Absicherung von Kommunikationsprotokollen, Security Monitoring und richtliniengesteuerten Automatisierungslösungen wurden auf das Management zukünftiger Energieversorgungsnetze angewandt. Der Transfer der Forschungsergebnisse in die Praxis wurde auch im Rahmen von dtec.bw-Projekten intensiviert: Beispielsweise wurden im Rahmen einer Kooperation mit der österreichischen Gemeinde Neuhaus die ersten fünf Standorte für den Testbetrieb eines energieautarken Blackout-Krisenkommunikationssystems auf Basis der Funktechnologie LoRa in Betrieb genommen.

Prof. Dr. Wolfgang Hommel

wolfgang.hommel@unibw.de

+49 89 6004 7355

www.unibw.de/software-security



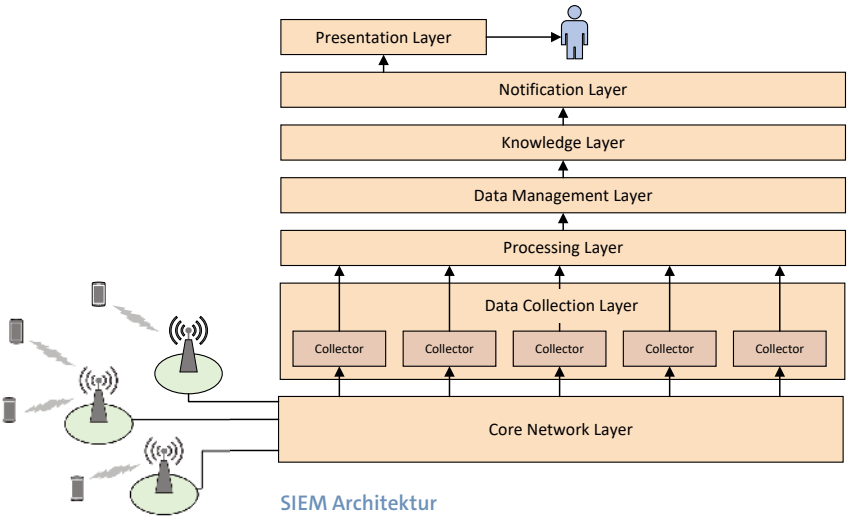
Forschungsschwerpunkte der Professur für IT-Sicherheit von Software und Daten.

ABB.: ISTOCK / VERTIGO3D; TAUSENDBLAUWERK, QUELLE: FI CODE / W. HOMMEL

Projekt 6G-life

Digitale Transformation und Souveränität zukünftiger Kommunikationsnetze

In dem Projekt 6G-life werden mit einem holistischen Ansatz innovative Konzepte im Bereich skalierbare Kommunikation, neuartige Methoden, flexible Softwarekonzepte und adaptive Hardware erforscht, die den Grundgedanken der Mensch-Maschine-Kollaboration unterstützen. In allen Forschungsfeldern werden die Anforderungen an Latenz, Resilienz, Sicherheit und Nachhaltigkeit als Querschnittsthemen stets parallel bearbeitet.



SIEM Architektur

6G: Zukunftsfähige Netz mit integrierter Sicherheit

Mit 5G wurde das Tor zur Digitalisierung in der Industrie weit aufgestoßen. Neben der Steuerung von Maschinen ermöglicht 5G das Internet der Dinge in Echtzeit. Ein wesentlicher Nachteil bei 5G-Kommunikationsnetzen ist jedoch der geringe Einsatz neuartiger Technologien, was die Zukunftsfähigkeit einschränkt. Durch die Integration neuartiger Technologien sollen den Anforderungen für hochpräzise Dienste in 6G-Netzen Rechnung getragen werden. Dies bringt jedoch sicherheitsrelevante Herausforderungen mit sich. Die Absicherung sowohl der Kommunikationsinfrastruktur als auch der Kommunikation sollen daher bei 6G von Anfang an mitgedacht werden, um eine native Integration in die Standards und Protokolle sicherzustellen.

SIEM Architektur

Im Rahmen des Projektes 6G-life werden mitunter Ansätze für ein verteiltes Security Information & Event Management (SIEM) System für 6G-Netze untersucht sowie prototypisch implementiert. Im Kontrast zum bisherigen Stand der Technik stellen dabei die Charakteristika von 6G-Netzen neue Herausforderungen dar, beispielsweise die Anforderungen an die Energieeffizienz von low-power Endgeräten, die weiter minimierten Latenzen und die nochmals deutlich erhöhten Datenraten. Während In-Network Computing gegenüber der herkömmlichen hierarchischen Datenaggregation und -auswertung neue Möglichkeiten zur dezentralen und latenzarmen Korrelation und Analyse von Daten bringt, muss die resultierende Dynamik z. B. von Netztopologien und stark verteilten Softwaresystemen im Kontext von IT-Sicherheitsanalysen und Lagebilddarstellungen berücksichtigt werden.

Die SIEM Architektur basiert auf unterschiedlichen, zusammenarbeitenden Ebenen, um sicherheitsrelevante Daten zu sammeln, zu verarbeiten, zu analysieren und darzustellen. Neben der SIEM-Gesamtarchitektur mit Konzepten für das verteilte Deployment umfassen die Arbeiten auch die Schnittstellen zur Erfassung relevanter Sicherheitsinformationen von den beteiligten Netzkomponenten und Endgeräten sowie deren lagebildartige Darstellung. Ein weiterer Fokus liegt auf der Entwicklung skalierbarer Mechanismen zur Verarbeitung großer Datenmengen, um die steigenden Anforderungen an Datenraten und Latenzen in 6G-Netzen zu erfüllen.

Tore Bierwirth
tore.bierwirth@unibw.de
+49 89 6004 7357
https://go.unibw.de/6g-life

Gefördert durch: Bundesministerium für Bildung und Forschung im Rahmen des Programms „Souverän. Digital. Vernetzt.“

ABB.: FI CODE / T. BIERWIRTH

Projekt DEFINE

DC-Netze für eine sichere Energieversorgung

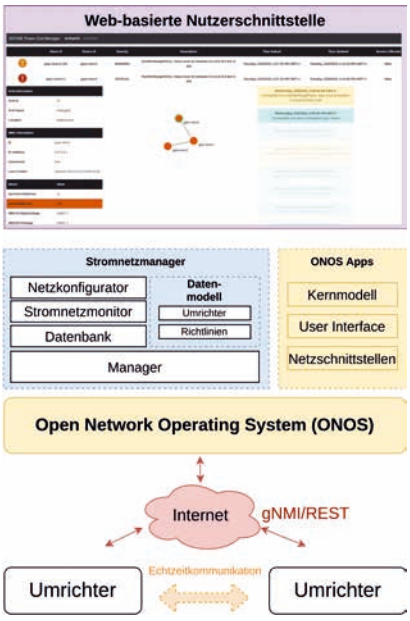
Das Projekt DEFINE erforscht stabile und sichere Strominfrastrukturen der Zukunft von der Komponenten- über die Container- und Stromnetzebene bis hin zur Netzfernüberwachung- und -steuerung von Grund auf neu. Ziel ist nicht nur die Gewährleistung eines stabilen Betriebs, sondern auch die Härtung der zur Steuerung der Netze notwendigen IT-Infrastruktur gegen Angriffe.

Ein zweischichtiger Managementansatz

Umrichterstationen halten das Stromnetz aufrecht und steuern aktiv Stromflüsse zur Deckung der Strombedarfe, auch im Fehlerfall. Ein Managementssystem in einer Netzleitstelle überwacht und steuert die Umrichterstationen. Dazu wird ein zweischichtiger Ansatz untersucht in dem Umrichterstationen einerseits in Echtzeit kontinuierlich ihren Zustand dezentral miteinander austauschen um auf Bedarfsänderungen und Fehler reagieren zu können. Andererseits erfasst eine zentrale Netzleitstelle den Zustand der Umrichterstationen, um eine langfristige Gesamtsicht aufzubereiten, Störungen und Angriffe zu erkennen und diese automatisch einzudämmen.

SDN-Technologie als Netzleitstelle

Software-Defined-Networking (SDN) lagert die Steuerungslogik aus der eigenlichen Netzkomponente aus. ONOS ist eine Managementplattform aus dem SDN-Bereich, die die zentrale Sammlung von Netzdaten und flexible Erweiterung um Managementanwendungen (Apps) erlaubt, um Netzdaten auszuwerten und das Netz auf dieser Basis zu steuern. In DEFINE wird dieser Ansatz für Stromnetze untersucht und eine App zum Management moderner Umrichterstationen und von Stromnetzen konzipiert und prototypisch implementiert. Auf Basis hochflexibler Protokolle wie dem gRPC Network Management Interface (gNMI) und REST können bedarfsabhängig Kennzahlen von Umrichterstationen erhoben werden. Die Erhebung erfolgt dabei über abgesicherte Kommunikationstunnel (z. B. über TLS). Die Kennzahlen werden zentral gespeichert und auf Störungen oder Angriffe untersucht.



SDN-basierte Netzleittechnik für moderne Stromnetze.

Wird eine Störung erkannt, dann wird ein Alarm auf einer Web-basierten Nutzeroberfläche angezeigt. Die Nutzeroberfläche zeigt stets eine aktuelle Lagebilddarstellung des Stromnetzes, der darin aktiven Umrichterstationen und der aktuellen Kennzahlen jeder Umrichterstation. Die Ansicht kann sowohl in einem zentralen Kontrollzentrum aber auch auf mobilen Geräten wie Tablets für unterwegs aufgerufen werden. Die Netzleitstelle erlaubt aber nicht nur die Darstellung, sondern auch eine automatisierte und/oder ferngesteuerte Reaktion auf Störungen und Angriffe.

Angriffserkennung und Härtung

Die Managementplattform muss nicht nur Verfahren zur Angriffserkennung (z. B. Korrelation von Ereignissen) umsetzen. Schutz vor unberechtigem Zugriff oder einer Kompromittierung der Netzleitstelle sind ebenfalls Forschungsgegenstand um sichere und fernwartbare Stromnetze der Zukunft gewährleisten zu können.

Dr. Michael Steinke
michael.steinke@unibw.de
+49 89 6004 4825
https://go.unibw.de/inf24define

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.

dtec.bw
Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr

Finanziert von der Europäischen Union
NextGenerationEU

ABB.: FI CODE / M. STEINKE

Prof. Dr.-Ing. Mark Manulis

Forschungsgruppe Privacy and Applied Cryptography Lab

PACY Lab, geleitet vom Inhaber der Professur für Privacy, Prof. Dr.-Ing. Mark Manulis, erforscht Technologien zur Verbesserung der Privatsphäre basierend auf modernen kryptographischen Methoden. Im Fokus stehen Design, Analyse und Entwicklung von kryptographischen Verfahren zum Schutz von Benutzern, Daten und Nachrichten, sowie deren praktischer Einsatz im Umfeld von Web, Cloud, IoT und Blockchain.

Forschungsschwerpunkte am PACY Lab

PACY Lab wurde im März 2022 eingerichtet und ist Teil des Forschungsinstituts CODE. Die Mitarbeitende verfügen über tiefe Kenntnisse aus Kryptographie, Informatik und Mathematik, die sie für Grundlagen- und Anwendungsforschung erfolgreich einsetzen.

Die Schwerpunkte liegen in der Erforschung von Methoden und Verfahren auf dem Gebiet der Privacy Enhancing Cryptography (PEC) – dabei handelt es sich generell um kryptographische Verfahren mit speziellen Anforderungen an Vertraulichkeit und Privatheit.

Im Fokus von PACY Lab stehen Design und praktischer Einsatz von diversen PEC-Verfahren, darunter erweiterter Verschlüsselungs- und Signaturverfahren sowie Protokollen. Die Gruppe beschäftigt sich mit Modellierung und Analyse von funktionellen Eigenschaften und Schutzzielen. Erforscht werden Zusammenhänge zwischen Verfahren/Eigenschaften, um das allgemeine Verständnis zu verbessern und neue Konstruktionswege zu finden. PACY Lab entwickelt neue PEC-Verfahren und nutzt diese zur Konstruktion von kryptographischen Protokollen zur Authentisierung und Zugangskontrolle, Verarbeitung von Daten und Transaktionen sowie zum Nachrichtenaustausch.

Beim Design und Implementierung von neuen PEC-Verfahren werden am PACY Lab alle gängigen mathematischen Techniken der Kryptographie eingesetzt, darunter auch Kryptographie mit elliptischen Kurven und bilinearen Abbildungen. Am PACY Lab wird zurzeit auch viel mit den Techniken der gitterbasierten Kryptographie gearbeitet, um die gewünschte kryptographische Sicherheit gegenüber von künftigen Quantenrechnern zu realisieren. Zu weiteren eingesetzten PEC-Techniken zählen Secret Sharing und Zero-Knowledge-Beweise.

PEC für Daten: Zugangskontrolle und Datenverarbeitung

Traditionelle Verschlüsselungsverfahren können Geheimhaltung gewährleisten, jedoch nicht direkt für die Verarbeitung von verschlüsselten Daten eingesetzt werden. Moderne PEC-Verfahren ermöglichen eine Vielzahl von Operationen auf verschlüsselten Daten, ohne dass diese während der Verarbeitung entschlüsselt werden müssen. PACY Lab arbeitet an funktionalen Verschlüsselungsverfahren, die mehr Flexibilität bei Zugangskontrolle im Datenaustausch ermöglichen bzw. eine direkte Verarbeitung von verschlüsselten Daten in verteilten und Mehrnutzer-Anwendungen bieten. Zu den laufenden Forschungsarbeiten gehören Ansätze zur vollständig homomorphen Verschlüsselung und zur attributbasierten Verschlüsselung sowie kryptografische Protokolle, die Operationen (z. B. Suchabfragen) auf verschlüsselten Daten unterstützen, sowie deren Einsatz in verteilten Anwendungen.

PEC für Benutzer: Authentisierung und Nachrichtenaustausch

Digitale Signaturen bilden das Rückgrat moderner PKI. Damit können Benutzer sich authentisieren bzw. Ende-zu-Ende sichere Verbindungen aufbauen. Die Verifikation von PKI basierten Signaturen gibt viele sensible Informationen preis, wie z. B. Identitäten, öffentliche Schlüsseln und sämtliche Attribute. PACY Lab erforscht fortgeschrittene Signaturtechniken, um Authentifizierung mit Anonymität oder Unverfolgbarkeit zu kombinieren. Zu den laufenden Forschungsarbeiten gehören attributbasierte Signaturverfahren und damit zusammenhängende Konzepte für Anonymous-Credentials-Systeme. Darüber hinaus erforscht PACY Lab Protokolle für sicheres und privates Messaging und für verteilte und delegierbare Authentifizierung, zum Beispiel in Verbindung mit dem neuen FIDO2-Standard für Web-Authentifizierung.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

ABB.: ADOBE STOCK / A. YALANSKYI; FI CODE

Rechnen auf verschlüsselten Daten mit voll homomorpher Verschlüsselung

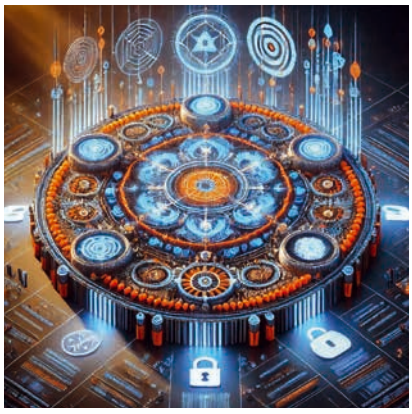
Datenverarbeitung mit verbessertem Datenschutz und Integrität

Die voll homomorphe Verschlüsselung (Fully Homomorphic Encryption, FHE) ist eine bahnbrechende kryptografische Technik, die es ermöglicht, Berechnungen mit verschlüsselten Daten durchzuführen, ohne dass diese zuvor entschlüsselt werden müssen. Auf diese Weise können sensible Informationen sicher verarbeitet werden, wobei der Datenschutz auch in nicht vertrauenswürdigen Umgebungen gewahrt bleibt. Die Anwendungen von FHE reichen von der Verbesserung der Datensicherheit beim Cloud-Computing bis hin zur Ermöglichung von datenschutzfreundlichem maschinellem Lernen, usw.

Voll Homomorphe Verschlüsselung (FHE)

Die Berechnung verschlüsselter Daten mit FHE erfordert komplexe mathematische Strukturen, wie z. B. gitterbasierte Kryptographie, um Operationen an Chiffretexten zu ermöglichen, die den Operationen an den Klartexten entsprechen. Im Wesentlichen ermöglichen FHE-Verfahren die Auswertung beliebiger Schaltkreise, die aus mehreren Arten von Gattern bestehen, so dass jede Berechnung mit verschlüsselten Daten so durchgeführt werden kann, als ob sie unverschlüsselt wären.

Trotz ihres Potenzials steht FHE vor erheblichen Herausforderungen in der Forschung. Eine Herausforderung ist der Rechenaufwand, da FHE-Operationen im Vergleich zu Operationen an unverschlüsselten Daten viel langsamer sind. Auch der Speicherbedarf von FHE ist erheblich, da die Chiffretexte oft viel größer sind als die Klartexte. Neben der Verbesserung der Effizienz und Praktikabilität konzentriert sich die aktuelle Forschung auf die Integritäts- und Überprüfbarkeitsgarantien für FHE-Berechnungen, die in einer nicht vertrauenswürdigen Umgebung durchgeführt werden.



Unsere Forschung zur Integrität und Überprüfbarkeit von FHE-Berechnungen

Seit 2023 erforscht das PACY Lab Sicherheitseigenschaften, die für FHE-Schemata zur Verfügung stehen, sowie mit deren Beziehungen und Realisierbarkeit. Unser Ziel war es, eine gemeinsame Sichtweise auf die Hierarchie bestehender Eigenschaften zu entwickeln und die stärkste noch realisierbare Definition von Sicherheit für beliebige FHE-Schemata zu finden. Stärkere Eigenschaften sind eindeutig solche, die die Integrität der zugrundeliegenden Klartexte schützen können, da die FHE-Berechnungen an den Chiffretexten von einer nicht vertrauenswürdigen Partei durchgeführt werden. Intuitiv ergibt sich der stärkste Integritätsschutz aus der Möglichkeit, das Ergebnis von FHE-Berechnungen zu verifizieren.

In unserer Arbeit, die auf der renommierten EUROCRYPT 2024 veröffentlicht wurde, haben wir einen neuen Begriff entwickelt, den wir „indistinguishability against verified chosen ciphertext-attack“ (IND-vCCA) nennen. Wir haben bewiesen, dass diese Eigenschaft die bisher stärksten Integritätsgarantien für FHE-Berechnungen bietet, und zwei allgemeine Transformationen vorgeschlagen, mit denen viele der bestehenden FHE-Verfahren durch die Verwendung sogenannter zero-knowledge SNARKs auf IND-vCCA-Sicherheitsniveau angehoben werden können. Seit ihrer Veröffentlichung hat unsere Arbeit die kryptographische Gemeinschaft dazu angeregt, die IND-vCCA-Sicherheit von spezielleren FHE-Konstruktionen, die in der Praxis verwendet werden, zu untersuchen.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

ABB.: GENERIERT BY DALL-E 3

Schnelle und aussagekräftige attributbasierte Verschlüsselung

Ermöglichung einer schnellen, feinkörnigen Zugriffskontrolle auf verschlüsselte Daten.

Die attributbasierte Verschlüsselung (ABE) ist eine kryptografische Technik, die eine fein abgestufte Zugangskontrolle zu verschlüsselten Daten ermöglicht. Im Gegensatz zu herkömmlichen Verschlüsselungsmethoden, ermöglicht ABE den Zugang auf der Grundlage der Attribute des Benutzers. ABE ist besonders nützlich in Szenarien, in denen Daten sicher von einer großen und dynamischen Gruppe von Benutzern gemeinsam genutzt werden müssen.

Herausforderungen bei der attributbasierten Verschlüsselung

Die attributbasierte Verschlüsselung (ABE) ist ein faszinierendes Gebiet mit mehreren Forschungsherausforderungen. Eine der wichtigsten Herausforderungen bei ABE ist die Verwaltung der Schlüssel. Jeder Benutzer benötigt einen privaten Schlüssel, der zu seinen Attributen oder seiner Zugriffsstruktur passt. Mit zunehmender Anzahl von Benutzern und Attributen muss das System mehr Schlüssel und komplexere Zugangsrichtlinien verwalten. Es ist eine große Herausforderung, sicherzustellen, dass das System effizient und skalierbar bleibt. Die Ver- und Entschlüsselungsprozesse in ABE können sehr rechenintensiv sein. Die Verbesserung der Effizienz dieser Prozesse ohne Beeinträchtigung der Sicherheit ist ein wichtiger Forschungsbereich. Von besonderer praktischer Bedeutung ist der Entwurf aussagekräftiger ABE-Schemata, die komplexe Zugriffsstrukturen unterstützen, wie z. B. AND-, OR- und Schwellenwert-Gatter, die eine differenziertere und detailliertere Zugriffskontrolle auf verschlüsselte Daten ermöglichen.

Aufbau schneller und aussagekräftiger ABE-Schemata

PACY Lab arbeitet an der Entwicklung praktischer ABE-Verfahren, die in der Lage sind, ausdrucksstarke Zugriffsrichtlinien zu verarbeiten, die durch konjunktive, disjunktive oder beliebige monotone boolesche Formeln dargestellt werden können, um den praktischen Einsatz in realen Anwendungen zu ermöglichen.

Zu diesem Zweck haben wir in Zusammenarbeit mit der University of Surrey (UK) mehrere effiziente ABE-Verfahren mit den oben genannten Eigenschaften entwickelt und implementiert. Die Ergebnisse unserer Arbeit wurden auf der renommierten Konferenz ACM CCS 2025 veröffentlicht.

ABB.: : GENERIERT BY DALL·E 3

Unsere ABE-Verfahren ermöglichen die Einbettung von Attributen in private Benutzerschlüssel und Zugriffsrichtlinien in Chiffretexte oder umgekehrt, je nach den Anforderungen einer bestimmten Anwendung. Darüber hinaus verfügen einige unserer ABE-Verfahren über die zusätzliche Eigenschaft der Anonymität, durch die Benutzerattribute verborgen werden.

Prof. Dr.-Ing. Mark Manulis

+49 89 6004 7365

mark.manulis@unibw.de

www.unibw.de/pacy

Prof. Dr. Daniel Slamanig

Kryptologie

Das Quantum Safe & Advanced Cryptography (QuSAC) Lab unter der Leitung von Prof. Dr. Daniel Slamanig beschäftigt sich mit beweisbar sicherer quantenresistenter asymmetrischer sowie fortgeschrittener Kryptographie. Unsere Forschung ist motiviert durch die steigenden Sicherheitsanforderungen, die zunehmende digitale Vernetzung und rasante technologische Entwicklungen mit sich bringen.

DAS QUSAC LAB FORSCHT an Grundlagen und Anwendungen der Kryptographie. Unser Hauptaugenmerk liegt auf quantenresistenter asymmetrischer Kryptographie und fortgeschrittenen Primitiven. Dabei betrachten wir sowohl modulare Konstruktionen auf Basis generischer Bausteine als auch solche, die auf konkreten mathematischen Annahmen beruhen. Hierbei stellt beweisbare Sicherheit einen zentralen Aspekt unserer Arbeit dar.

Relevanz von Kryptographie

Kryptographie ist ein zentrales Element von Cybersicherheit. Sie verbessert die Sicherheit und den Datenschutz der meisten modernen digitalen Dienste und Anwendungen und ist von hoher gesellschaftlicher Relevanz. Die Komplexität moderner Szenarien stellt jedoch auch hohe Anforderungen an die Sicherheit und Funktionalität der Kryptographie.

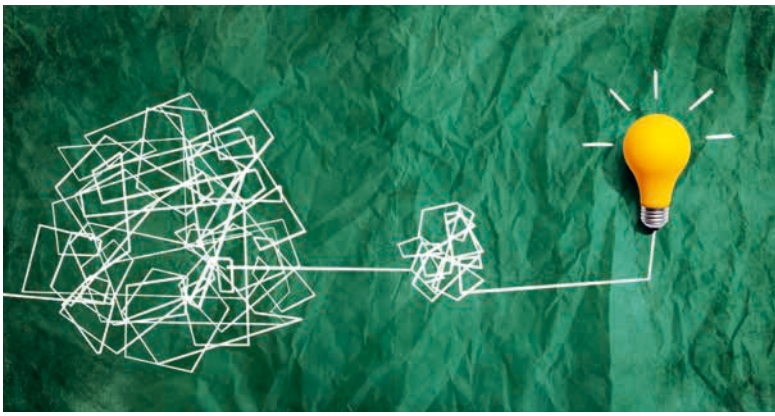
Stärkere Sicherheit: Quantencomputer und mehr

Potenzielle Fortschritte auf dem Gebiet der Quantencomputer würden die derzeit verwendete asymmetrische Kryptographie unsicher machen. Diesem Risiko kann durch den Einsatz von quantenresistenter (oder Post-Quanten-) Kryptographie entgegnet werden. Wir forschen an Klassen von geeigneten mathematischen Problemen (z. B. isogeniebasierte Kryptographie), sowie an der Entwicklung darauf basierender Primitive. Insbesondere war Prof. Slamanig an der Entwicklung des Picnic Post-Quanten-Signaturverfahren beteiligt. Picnic wurde bei dem wohl wichtigsten internationalen Post-Quanten-Kryptographie-Standardisierungsprojekt des NIST eingereicht und erreichte dort die dritte und finale Runde.

Ungeachtet dieser bedeutenden Herausforderung werden erforderliche Sicherheitsgarantien für moderne Szenarien oft nicht von kryptographischen Basisprimitiven angeboten. Hier arbeiten wir zum Beispiel an der Entwicklung von asymmetrischen Verschlüsselungsprimitiven, die die erforderlichen starken Sicherheitsgarantien bieten, sowie an den theoretischen Grundlagen Privatsphäre-freundlicher Kryptographie.

Mehr Funktionalität bei gleichzeitiger Sicherheit

Moderne Anwendungen werden immer komplexer und erfordern fortgeschrittene Funktionalität bei gleichzeitiger Gewährleistung hoher Sicherheit. Dies erfordert kryptographische Verfahren, deren Funktionalität weit über die von Basisprimitiven hinausgeht. Hier forschen wir etwa an nicht-interaktiven Zero-Knowledge-Beweisen und ihren kompakten Varianten (so genannte SNARKs), die aktuell die wohl meistverwendete fortgeschrittene Kryptographie in der Praxis darstellen.



Die Herausforderung in der Kryptographie ist das Lösen von oft paradox scheinenden Problemen.

Beitrag zur akademischen Gemeinschaft

Im Jahr 2024 wurde Prof. Slamanig eingeladen in Programmkomitees folgender internationaler Top-Konferenzen zu dienen: 44th Annual International Cryptology Conference (CRYPTO 2024), 31st und 32nd Annual ACM Conference on Computer and Communications Security (ACM CCS 2024 und ACM CCS 2025) sowie die 28th IACR International Conference on Practice and Theory of Public-Key Cryptography (PKC 2025). Darüber hinaus wurde er ins Editorial Board des IACR Communications in Cryptology (CiC) Journals eingeladen.

Entwicklung der Forschungsgruppe

Das QuSAC Lab wurde im November 2023 gegründet und beherbergt derzeit zwei Doktoranden und einen Post-Doc-Forscher. Die Gruppe verfügt über ein starkes nationales und internationales wissenschaftliches Netzwerk, unterhält zahlreiche internationale Kooperationen und empfängt regelmäßig internationale Gastwissenschaftler.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

www.unibw.de/crypto

ABB.: ADOBE STOCK / ANNIKA; ADOBE STOCK / TIERNEY

Fortschritte in der Isogeniebasierten Kryptographie

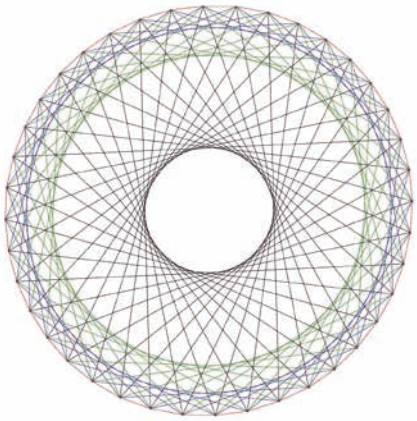
Neue Tools für Isogeniebasierte Kryptographie

Vor über zwanzig Jahren schlugen Couveignes, Rostovstev und Stolbunov das vor, was heute als isogeniebasierte Kryptographie bekannt ist. Dieses Konzept ist interessant, weil das Problem der Ermittlung einer geheimen Isogenie selbst für Quantencomputer als schwierig gilt und die daraus resultierenden privaten/öffentlichen Schlüssel bemerkenswert kompakt sind. Es handelt sich um ein sehr aktives Forschungsgebiet mit vielen kryptographischen Anwendungen und vielen interessanten Verbindungen zur Zahlentheorie.

WÄHREND isogeniebasierte Kryptographie ein junges Gebiet darstellt, geht die Verwendung elliptischer Kurven in der Kryptographie, so genannte Elliptic Curve Cryptography (ECC), in die achtziger Jahre zurück; ihre mathematische Untersuchung begann hingegen bereits in der Antike mit Diophantus und wurde in jüngerer Zeit von Fermat, Jacobi, Weierstraß und vielen anderen fortgesetzt. Einfach ausgedrückt ist eine elliptische Kurve eine Menge von Punkten, deren Koordinaten eine kubische Gleichung erfüllen. Auf dieser Punktmenge kann man eine Gruppenstruktur definieren, für die das so genannte diskrete Logarithmusproblem (DLP) schwer zu berechnen ist – dies ist der Kern der ECC. Shor hat jedoch in den neunziger Jahren gezeigt, dass es einen effizienten Quantenalgorithmus zur Lösung des DLP gibt, wodurch die ECC für Quantenangriffe anfällig wird. Während leistungsstarke Quantencomputer noch nicht existieren, gibt es einen weltweiten Trend zur Post-Quanten-Kryptographie, um diesem Risiko vorzubeugen.

Elliptische Kurven in einem Post-Quanten Setting

Im Gegensatz zur ECC nutzt die isogeniebasierte Kryptographie Abbildungen zwischen elliptischen Kurven, so genannte Isogenien, um eine Trapdoor-Einwegfunktion zu realisieren. Genauer gesagt betrachtet



Veranschaulichendes Beispiel eines Isogeniegraphen über einem Primkörper.

man Graphen deren Knoten Klassen von elliptischen Kurven und deren Kanten Isogenien darstellen. Die Ermittlung einer geheimen Isogenie (d. h. eines Pfades im Graphen) zwischen zwei gegebenen elliptischen Kurven gilt selbst für Quantencomputer als schwierig. Im Jahr 2022 wurde gezeigt, dass eine Abweichung von diesem Problem, z. B. durch die Veröffentlichung von Hilfsinformationen darüber, wie die geheime Isogenie bestimmte Punkte abbildet, gefährlich ist – es wurde nämlich ein verheerender Angriff gegen SIKE, ein zur Standardisierung in Betracht gezogenes Verschlüsselungsverfahren, demonstriert. Dieser Angriff betrifft jedoch nicht die zentrale Trapdoor-Funktion. Ganz im Gegenteil hat er die Forschung auf diesem Gebiet durch die Einführung neuer Ideen und Techniken signifikant vorangetrieben.

Kenntnis von geheimen Isogenien beweisen

Wenn isogeniebasierte Kryptographie praktisch und in komplexeren Protokollen verwendet wird, ist es erforderlich zu beweisen, dass öffentlichen Schlüssel wohlgeformt sind. Darüber hinaus ist es in zunehmend dezentralisierten Anwendungen oft erforderlich, dass viele Parteien gemeinsame Parameter, wie etwa spezifische elliptische Kurven, verwenden müssen. Hier muss garantiert sein, dass niemand die geheime Isogenie kennt, die als Hintertür angesehen werden kann. Im QuSAC Lab arbeiten wir beispielsweise an der Entwicklung von Zero-Knowledge-Beweisen für den effizienten Nachweis der Kenntnis von Isogenien. Dies ermöglicht es, die oben genannten Probleme zu lösen und viele zusätzliche Anwendungen zu realisieren. Derzeit sind wir besonders daran interessiert, solche Zero-Knowledge-Beweise über Arithmetisierungen zu realisieren, die Varianten so genannter modularer Polynome verwenden, welche unterschiedliche, aber äquivalente Darstellungen von Isogenien zwischen elliptischen Kurven erlauben.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

ABB.: FI CODE / D. SLAMANIG

Kryptographische Grundlagen der Datenschutzfreundlichen Authentifizierung

Digitale Signaturen mit besonderen Eigenschaften und Zero-Knowledge-Beweise

Mit der zunehmenden Nutzung von Online-Diensten gewinnt der Schutz der Privatsphäre immer mehr an Bedeutung. Dies ist besonders kritisch, da Authentifizierung, wie sie heutzutage im Internet erfolgt, in der Regel auf zentralisierten Identitätsmanagementlösungen beruht. Diese sind zwar sehr benutzerfreundlich, aus Sicht des Datenschutzes sind sie jedoch ziemlich „Privatsphäre-unfreundlich“ und weit davon entfernt, das Konzept der Datenminimierung umzusetzen.

GLÜCKLICHERWEISE bietet die Kryptographie einen Werkzeugkasten um so genannte Anonyme Credential Systeme (ACS) zu realisieren. Mit solchen Primitiven lässt sich Online-Authentifizierung mit einem hohen Maß an eingebautem Datenschutz realisieren.

Abstrakt betrachtet erhält in einem ACS ein Benutzer von einem Aussteller eine Signatur für eine Reihe von Benutzerattributen. Um eine Authentifizierung durchzuführen, muss der Benutzer nachweisen, dass er im Besitz einer solchen gültigen Signatur des Ausstellers ist, dessen Attribute eine bestimmte, vom Verifizierer geforderte Policy erfüllt. Dabei kann es sich um einzelne Attribute oder um eine komplexere Relation handeln, z. B. für das Attribut ‚Geburtsdatum‘ soll gelten, dass der Inhaber über 18 Jahre alt ist. Entscheidend ist, dass der Prozess weder direkt die Original-Signatur des Ausstellers noch Information über verbleibende Attribute preisgibt, was starke Datenschutzgarantien bietet. Außerdem sind alle Informationen, die während verschiedenen Authentifizierungen preisgegeben werden, nicht miteinander verknüpfbar.

Spezifische Signaturverfahren

Eine Konstruktionsart von ACS stützt sich auf spezielle Signaturverfahren. Im QuSAC Lab haben wir ein neues

Heutzutage sind „datenschutzunfreundliche“ Authentifizierungsmethoden noch weit verbreitet.

Signaturparadigma vorgeschlagen, die so genannten Äquivalenzklassensignaturen. Dabei handelt es sich um Signaturverfahren, die sowohl eine Randomisierung von Signaturen als auch eine kontrollierte öffentliche Randomisierung der signierten Nachricht ermöglichen, ohne die Signatur ungültig zu machen. Dieses Konzept wurde später auf so genannte Mercurial Signaturen erweitert, die zusätzlich eine Schlüsselrandomisierung unterstützen. Letztere ermöglichen ACS mit Delegationsmöglichkeiten. Kürzlich haben Mitglieder des QuSAC Labs derartige Signaturen mit starken Unverknüpfbarkeitseigenschaften entwickelt. Leider erfordern diese Konzepte eine reichhaltige algebraische Struktur, und es ist bisher unklar, ob oder wie sie basierend auf Post-Quanten-Annahmen konstruiert werden können. Um dennoch quantenresistente ACS zu ermöglichen, hat das QuSAC Lab vor kurzem damit begonnen, die Konstruktion anderer spezifischer Signaturschemata zu untersuchen, die als Baustein dienen können – insbesondere auf isogeniebasierten Annahmen beruhende blinde Signaturen.

Zero-Knowledge Beweise

Eine zweite und generische Möglichkeit ACS zu konstruieren, besteht darin ein beliebiges Signaturschema, z. B. ein weit verbreitetes Verfahren wie den Elliptic Curve Digital Signature Algorithm (ECDSA), und ein nicht-interaktives Zero-Knowledge Beweissystem (NIZK) zu kombinieren. Jüngste Fortschritte bei der Entwicklung sehr kompakter NIZK-Beweise, so genannter zk-SNARKs, machen solche Verfahren praktikabel, und es gibt erste sehr aktuelle Arbeiten durch Teams von Google und Microsoft, die planen, diese auch praktisch einzusetzen. Auch hier gibt es für Post-Quanten-Konstruktionen viele Herausforderungen zu lösen. Das QuSAC Lab arbeitet an deren Grundlagen und insbesondere an der Entwicklung von Post-Quanten-zk-SNARKs.

Prof. Dr. Daniel Slamanig

daniel.slamanig@unibw.de

+49 89 6004 7430

ABB.: ADOBE STOCK/ KIATTISAK

Prof. Dr. Arno Wacker

Datenschutz und Compliance

Datenschutz und IT-Sicherheit nicht nur lehren, sondern auch leben!

EINES UNSERER wichtigsten Ziele ist es, Datenschutz und IT-Sicherheit nicht nur zu erforschen und zu lehren, sondern auch im Alltag zu leben. Nur so können diese Themenkomplexe den Studierenden überzeugend und authentisch vermittelt werden. Darüber hinaus wollen wir auch der breiten Öffentlichkeit zeigen, dass datenschutzfördernde Technologien in den Alltag integriert werden können, sowohl im privaten als auch im geschäftlichen Bereich.

Lehre

Die Lehre in der Professur unterteilt sich in Datenschutz, Privacy Enhancing Technologies, Pentesting, Kryptologie sowie Sichere Netze und Protokolle. Datenschutz und Privacy Enhancing Technologies vermitteln den Studierenden unter anderem, was Privacy ist und warum sie sowohl für den Einzelnen als auch für demokratische Gesellschaften wichtig ist. Pentesting behandelt das Testen einzelner Systeme, komplexerer IT-Dienste und ganzer IT-Infrastrukturen sowie praxisrelevante Angriffsvarianten mit Orientierung an erprobten Best-Practice-Dokumentationen. Kryptologie vermittelt Grundlagen der Kryptographie sowie Kenntnisse über die verschiedenen Verfahren zur sicheren Datenübertragung in modernen Kommunikationsnetzen.

Forschung

Ein besonderer Schwerpunkt der Professur liegt auf Methoden und Mechanismen zur Unterstützung der Privatsphäre und des Datenschutzes und gliedert sich in drei verschiedene Forschungsschwerpunkte:

- Privatheitsunterstützende Mechanismen zielen auf die Stärkung der Privatheit des Einzelnen sowie auf die Erforschung von Kommunikationsregeln für das Internetzeitalter.

- Die Erhöhung des IT-Sicherheitsbewusstseins (Awareness) befasst sich unter anderem mit dem Bereich Selbstdatenschutz. Dazu entwickelt und erforscht die Professur u. a. Verfahren und Werkzeuge zur Erhöhung des Sicherheitsbewusstseins bei der Entwicklung von Softwarewerkzeugen bzw. im Umgang mit diesen.

- Die Kryptoanalyse klassischer Chiffren untersucht das Gebiet klassischer Verschlüsselungsverfahren mit Hilfe moderner (meta-)heuristischer Verfahren. Dabei werden unter anderem die Effizienz der Analysen sowie die Sicherheit der Algorithmen untersucht.

Wissenstransfer

Ein besonderes Anliegen unserer Professur ist es, interessierte Bürgerinnen und Bürger in Fragen der IT-Sicherheit zu schulen, aufzuklären und zu informieren. Dieses Ziel verfolgen wir mit Vorträgen und Workshops, die sich beispielsweise mit Pentesting, sicherem E-Mail-Verkehr im Alltag und dem Aufspüren von Sicherheitslücken beschäftigen.

Prof. Dr. Arno Wacker

arno.wacker@unibw.de

+49 89 6004 7325

www.unibw.de/datcom

ABB.: ISTOCK / MATEJMO; FI CODE / DATCOM

Starke Authentifizierung mit UniBwM-ID und SecureID

Mehr Sicherheit und Komfort durch die Einführung der UniBwM-ID.

Seit April 2024 bietet die Universität der Bundeswehr München eine neue zweistufige Anmeldelösung: die UniBwM-ID mit Passkeys und die besonders sichere UniBwM-SecureID mit hardwarebasierten Schlüsseln. Ziel des Projekts war die Kombination hoher IT-Sicherheitsstandards mit maximalem Komfort für die Nutzerinnen und Nutzer.

DAS PROJEKT WURDE im April 2024 durch das Rechenzentrum (RZ) der Universität angestoßen. Unter der Leitung von Professor Wacker, der sowohl die Professur für Datenschutz und Compliance als auch das RZ führt, entstand ein durchdachtes Konzept, das hohe Sicherheitsanforderungen mit praktischer Benutzerfreundlichkeit vereint. Professor Wacker lieferte die Kernidee, das Konzept und wesentliche Teile der Architektur, während sein Team am RZ die Umsetzung operativ vorantrieb. Pünktlich zum Trimesterstart am 1. Oktober 2024 war das Projekt erfolgreich abgeschlossen.

Mit diesem Projekt wollte die Universität den klassischen, zunehmend unsicheren Ansatz von Benutzername und Passwort ablösen. Die neue Authentifizierungsarchitektur soll sicherstellen, dass gestohlene Zugangsdaten für Angreifer wertlos bleiben. Dazu wurden zwei Sicherheitsstufen entwickelt: Die UniBwM-ID ermöglicht den Einsatz von Passkeys für „normale“ Dienste wie ILIAS oder GIT, während die UniBwM-SecureID für besonders sensible Bereiche konzipiert ist, in denen die Benutzerinnen und Benutzer ihre Uni-Zugangsdaten verwalten und ändern können. In diesen sensiblen Diensten bleibt der Einsatz hardwarebasierter Sicherheitsschlüssel verpflichtend.

Ein zentraler Aspekt war es, Sicherheit und Komfort zu vereinen. Passkeys, basierend auf dem FIDO2-Standard, erlauben eine passwortfreie Anmeldung, wobei die Authentifizierung gerätegebunden erfolgt, beispielsweise über Apple Face ID oder Windows Hello. Die UniBwM-ID erlaubt so einen schnellen und einfachen Zugang zu universitären Diensten ohne administrative Berechtigungen, wie ILIAS. Für Dienste mit besonders

UniBwM-Authentifizierung: UniBwM-ID und -SecureID vereinen Komfort und Sicherheit.

schützenswerten Daten, wie das Nutzermanagement unter nutzer.unibw.de, ist hingegen die UniBwM-SecureID erforderlich, die hardwarebasierte Schlüssel wie YubiKeys verlangt. Diese Kombination aus Passkeys und Hardware-Sicherheitsschlüsseln stellt sicher, dass Anmeldedaten umfassend vor Phishing und Datendiebstahl geschützt sind.

Mit dieser Authentifizierungslösung konnte die Professur ihr Leitmotto „Datenschutz und Compliance nicht nur lehren, sondern auch leben“ verwirklichen. Die moderne Sicherheitsarchitektur verhindert Anmeldungen ohne Hardware-Schlüssel in sensiblen Bereichen und bietet gleichzeitig eine komfortable Lösung für „normale“ Dienste. Dank der Expertise der Professur für Datenschutz und Compliance konnte das RZ mit der UniBwM-ID eine zukunftssichere Authentifizierungslösung an der Universität etablieren. Bis Oktober 2024 wurden alle Universitätsmitglieder mit einem YubiKey ausgestattet, und die Anmeldung über Benutzername und Passwort für die betroffenen Dienste wurde ab dem 1. Oktober 2024 vollständig abgelöst. Dieses Projekt markiert einen bedeutenden Meilenstein für die IT-Sicherheit der Universität und zeigt, wie theoretisches Wissen erfolgreich in der Praxis angewendet wird – ein Beispiel für die enge Verbindung zwischen universitärer Forschung und operativer Praxis.

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

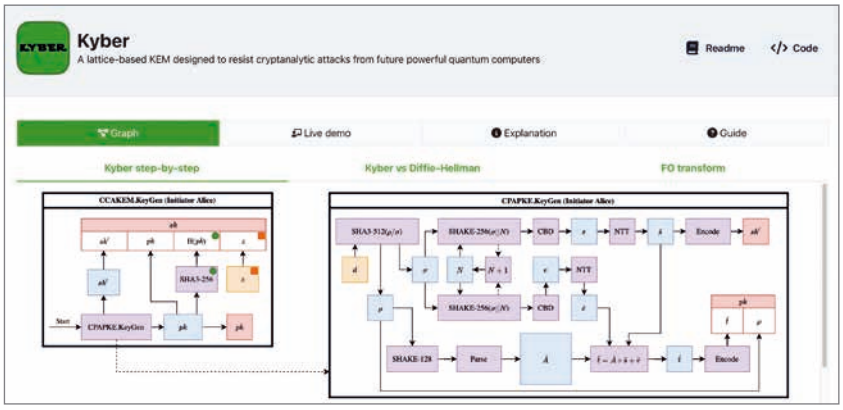
ABB.: FI CODE / A. WACKER

Projekt CrypTool

Neue WebApps für Kryptografie und Kryptoanalyse

Das Projekt CrypTool (www.cryptool.org) mit seinem seit 1998 aufgebauten Bestand an Softwareanwendungen, Lehr- und Lernmaterial zum Thema Kryptografie war im Jahr 2023 von der Universität Siegen an die Professur für Datenschutz und Compliance von Herrn Prof. Wacker umgezogen. Neben der Pflege des Bestands wurden seitdem mehrere WebApps neu entwickelt, Öffentlichkeitsarbeit betrieben und Kontakte geknüpft, um Schwerpunkte für die künftige Ausrichtung des Projekts mit der Bundeswehr als Zielgruppe zu finden.

NEBEN KLEINEREN APPS wie z. B. der Enigma-App, die ein Student der UniBw im Rahmen seiner BA entwickelte (https://www.cryptool.org/de/cto/enigma/), gab es die folgenden größeren Teilprojekte:



Interaktive Kyber WebApp.

1. Lernprogramm

Es wurde eine Lern-WebApp entwickelt, die auf den Kryptografieteil des neuen Bayerischen Gymnasiallehrplans zugeschnitten ist: https://learn.cryptool.org.

Die App befindet sich als Public Beta seit November 2024 im Einsatz. In Abstimmung mit dem Staatsinstitut für Schulqualität und Bildungsforschung München wird die App nach Einarbeitung der Rückmeldungen aus den Schulen voraussichtlich im sog. Lehrplan-Informationssystem verlinkt werden. Auf diese Weise könnte es uns gelingen, dass künftig jeder Schüler, der sein Abitur in Bayern absolviert, unsere App und damit auch CODE kennenlernt.

2. KI

Im Projekt CrypTool wurde KI erfolgreich für die Kryptoanalyse klassischer/historischer Chiffren angewandt, indem man das Verschlüsselungsverfahren bestimmte, wenn nur Geheimtext vorliegt. Dazu wurden eigene Modelle (neuronale Netze) trainiert. Das klappt ganz gut mit einer limitierten Anzahl von rund 50 Verfahren und wurde auch öffentlich über die NCID-App innerhalb von CrypTool-Online zugänglich gemacht (https://www.cryptool.org/en/cto/ncid/). Unsere aktuelle Forschung testet die Grenzen von bestehenden LLMs aus, indem man alternativ Code-basiertes Prompt Engineering nutzt, statt eigene Modelle zu trainieren.

3. Post-Quanten-Kryptografie

Das bisher als Kyber bekannte Schlüsselkapselungsverfahren wurde vom NIST im August 2024 standardisiert (https://csrc.nist.gov/pubs/fips/203/final). Eine CrypTool-WebApp, die dieses Verfahren u. a. mit Hilfe von interaktiven Graphiken erläutert, befindet sich seit 2023 in Entwicklung und wird derzeit überarbeitet, um die letzten Änderungen des NIST einzupflegen. Sie wird demnächst als CrypTool-Online App verfügbar sein: https://www.cryptool.org/de/cto/kyber/.

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

ABB.: FI CODE / CRYPTOOL / A. WACKER

Prof. Dr. Gabi Dreo Rodosek

Kommunikationssysteme und Netzsicherheit

Die Professur befasst sich mit dem Einsatz von generativer KI/ML in Netzsicherheit und Social Media Analytics, Software-Defined Networking, 5G/6G-Netzen sowie die Erkennung, Bewertung und Mitigation von Cyberrisiken.

Projekt 6G-life

Digitale Transformation und Souveränität künftiger Kommunikationsnetze

6G-life treibt die Spitzenforschung für 6G-Kommunikationsnetze mit dem Fokus auf die Zusammenarbeit von Mensch und Maschine voran. 6G-life bietet neue Ansätze für Nachhaltigkeit, Sicherheit, Resilienz und Latenz und wird die Wirtschaft und damit die digitale Souveränität in Deutschland nachhaltig stärken.

AN DEM PROJEKT, das von der TU Dresden und der TU München koordiniert wird, sind rund 162 Forscher und 19 Start-ups beteiligt. Das Projekt wird mit 70 Millionen Euro gefördert. Im Folgenden wird nur auf die Forschung im Bereich Netzsicherheit eingegangen.

Die Sicherheit von 6G-Netzen ist für den Aufbau hochvertrauenswürdiger cyber-physischer Systeme unerlässlich. In der Forschung werden verschiedene Aspekte der 6G-Netzsicherheit untersucht, wobei der Schwerpunkt auf der sich entwickelnden Bedrohungslandschaft, fortschrittlichen Verfahren zur Erkennung von Anomalien, der Anwendung der Zero Trust Architecture (ZTA) und vertrauenswürdigen Ausführungsumgebungen (TEEs) liegt.

Es wurde eine umfassende Bedrohungsanalyse durchgeführt, die sich mit 6G-spezifischen Schwachstellen, insbesondere in der Lieferkette, und neuen Angriffsvektoren befasst, die durch künstliche Intelligenz (KI) und maschinelles Lernen (ML) angetrieben werden. Um die Erkennung von Bedrohungen zu verbessern, werden KI-gestützte Verfahren zur Erkennung von Anomalien, wie z. B. Temporal Graph Neural Networks (TGNNs), auf ihre Fähigkeit untersucht, Abweichungen in dynamischen Netzumgebungen zu erkennen. Darüber hinaus wurde das Potenzial von Large Language Models (LLMs) zur Verbesserung der Netzsicherheit im Hinblick auf die automatische Erkennung von Bedrohungen und Anomalien analysiert.

Die Lösungen von 6G-Life werden neue Formen der Mensch-Maschine-Interaktion ermöglichen.

Security-by-Design ist ein zentrales Prinzip, insbesondere in servicebasierten Architekturen (SBAs), die Authentifizierung, Autorisierung und robuste Verschlüsselung für alle Netzinteraktionen gewährleisten. Darüber hinaus wird die Relevanz wichtiger Komponenten wie Network Repository Function (NRF), Service Communication Proxy (SCP) und Network Exposure Function (NEF) im Hinblick auf ihre Rolle bei der Gewährleistung eines sicheren Netzbetriebs analysiert.

Prof. Dr. Gabi Dreo Rodosek

gabi.dreo@unibw.de

+49 89 6004 7360

https://6g-life.de

Gefördert durch: Bundesministerium für Bildung und Forschung im Rahmen des Programms „Souverän. Digital. Vernetzt.“. Joint-Projekt 6G-life, Projektkennzeichen: 16KISK002.

ABB.: ADOBE STOCK / DENIS PUTILOV; ADOBE STOCK / SERGEY NIVENS

Prof. Dr. Ulrike Lechner

Forschungsgruppe Wirtschaftsinformatik

Die Forschungsgruppe Wirtschaftsinformatik unter der Leitung von Prof. Dr. Ulrike Lechner untersucht Sicherheit aus einer interdisziplinären Perspektive, die technologische, organisatorische und menschliche Aspekte einbezieht. Ein zentraler Forschungsschwerpunkt liegt auf der Entwicklung von Lernspielen im Bereich Cybersicherheit, mit dem Ziel, das Bewusstsein für Risiken, Mitigationsstrategien sowie Incident-Response-Maßnahmen zu schärfen.

Projekt CONTAIN

Effektive Reaktionen auf Bedrohungen aus dem digitalen Raum

Das Forschungsprojekt CONTAIN verfolgt das Ziel, die Effektivität und Effizienz bei der Reaktion auf Bedrohungen aus dem digitalen Raum zu steigern. Im Fokus steht dabei insbesondere Ransomware, die sowohl persönliche Endgeräte als auch Unternehmensnetzwerke mit betrieblichen Informationssystemen, Produktionsanlagen sowie Partner in der Lieferkette betreffen kann.

CONTAIN IST EIN deutsch-österreichisches Forschungsprojekt, das in einem interdisziplinären Konsortium innovative Konzepte und Verfahren zur Abwehr und Bewältigung von Ransomware-Angriffen untersucht.

Forschungsansatz von CONTAIN

Zur Stärkung der Resilienz gegenüber Cyberangriffen entwickelt CONTAIN Szenarien, Serious Games sowie Simulationen und führt eine Demonstrationsübung durch. Dabei steht der kontinuierliche Dialog mit Anwendern im Mittelpunkt. Drei zentrale Szenarien werden betrachtet:

1. Ransomware auf persönlichen Endgeräten
2. Ransomware-Angriffe auf Unternehmensnetzwerke
3. Ransomware in der digitalen Lieferkette

Serious Games: Sensibilisierung und Handlungsvorbereitung

Die Serious Games von CONTAIN verfolgen das Ziel, das Bewusstsein für Incident Response und Business Continuity zu schärfen und gleichzeitig auf adäquates Handeln in Krisensituationen vorzubereiten.

„Eine Frage der Sicherheit“: Dieses Spiel thematisiert Ransomware-Angriffe auf privat und beruflich genutzte Endgeräte. Die Spielenden lernen, die richtigen Fragen zu stellen, um zurück zur Arbeitsfähigkeit zu finden und reflektieren aus verschiedenen Perspektiven – etwa als Familienmitglied, Freund, Vorgesetzter, IT-Sicherheitsbeauftragter, Datenschutzbeauftragter oder Vertreter einer Sicherheitsbehörde – worauf es den Beteiligten im Ernstfall ankommt.

„Operation Raven“: Dieses Serious Game simuliert einen Ransomware-Vorfall im Netzwerk eines Betreibers Kritischer Infrastrukturen. Die Spielenden entwickeln rundenbasiert Strategien, um die Übernahme des Netzwerks durch Ransomware zu verhindern.

„CopyCat“: Das Spiel „CopyCat“ adressiert Bedrohungen in der digitalen Supply Chain und behandelt insbesondere Cloud-spezifische Angriffsvektoren sowie die geteilte Verantwortung bei Sicherheitsmaßnahmen in Cloud-Diensten. Die Zielgruppe sind Softwareentwicklerinnen und -entwickler aus der Industrie.

„Hack-Mich-Nicht“: Dieses Spiel richtet sich an Mitarbeitende und Entscheidungsträger in der Logistikbranche. Es sensibilisiert für Bedrohungen in der Lieferkette und ermöglicht den Spielenden, Sicherheitsmaßnahmen zu entwickeln und zu erproben.

Zentrale Forschungsergebnisse

Im Rahmen von CONTAIN wird ein IT-Sicherheitsrahmenwerk entwickelt, das sich insbesondere an kleine und mittlere Unternehmen (KMU) richtet. Die erarbeiteten Konzepte und Maßnahmen werden in einer föderierten Übung demonstriert. Detaillierte Informationen und Forschungsergebnisse sind auf der Projektwebseite verfügbar.

Projektpartnerschaft und Förderung

CONTAIN wird im Rahmen der deutschen zivilen Sicherheitsforschung (SIFO) und des österreichischen KIRAS-Programms durchgeführt. Unternehmen und Behörden aus beiden Ländern arbeiten gemeinsam an innovativen Lösungen zur Erhöhung der Cyberresilienz.

Das Konsortium dankt dem Bundesministerium für Bildung und Forschung (BMBF, FKZ 13N16581-13N16587), dem Bundesministerium der Finanzen (BMF, FO999902707) sowie der Österreichischen Forschungsförderungsgesellschaft für die Förderung dieses Projekts.

Prof. Dr. Ulrike Lechner
ulrike.lechner@unibw.de
+49 89 6004 2504
www.contain-projekt.de

Gefördert durch:
BMBF, BMF, Österreichische Forschungsförderungsgesellschaft (FFG)

ABB.: ADOBE STOCK / USAMA

Juniorprof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

Juniorprof. Molls Forschung konzentriert sich zum einen auf Reinforcement Learning, wobei ihn besonders die Kombinationsmöglichkeiten mit klassischem Operations Research sowie die Anwendungsmöglichkeiten im Prescriptive Analytics und Prescriptive Intelligence interessieren. Zum anderen forscht er an den Schnittstellen von Quantum Computing zu Optimierung und Machine Learning.

Quantum Machine Learning für das Future Combat Air System

Bewertung des Potenzials von Quantum Machine Learning als Ergänzung zu klassischen KI-Tools

Die Weiterentwicklung von Quantencomputern verspricht Lösungen für Probleme, die klassische Systeme nicht bewältigen, und eröffnet neue Möglichkeiten in Datenanalyse, Optimierung und Mustererkennung. In einer datengesteuerten Welt, in der Machine Learning (ML) Technologien in zahlreichen Bereichen antreibt, untersuchte diese Studie das Quantum Machine Learning (QML) als zukunftsweisende Alternative zum klassischen ML.

IN EINEM GRÖSSEREN Projekt entwickelt IBM das KI-Backbone für das Future Combat Air System und stellt eine zentrale Infrastruktur sowie algorithmische Werkzeuge für die Datenanalyse bereit. Diese einjährige Studie untersuchte, ob QML eine vielversprechende Ergänzung zu klassischen Werkzeugen sein könnte.

Das Projekt umfasste einen Überblick über den Stand der Technik, Experimente auf IBM-Quantenhardware sowie eine Einführung in die Quanteninformatik und bestehende Algorithmen und Hardware-Optionen.

Quantum Machine Learning in der Forschung

Wie klassisches ML lässt sich QML in Ansätze mit oder ohne neuronale Netze unterteilen. Dabei nutzen einige Quanten-Variationsschaltungen (QVCs) als Quantenanaloga zu neuronalen Netzen, andere nicht. Die Literatur zu Nicht-QVCs fokussiert sich auf Quantenversionen klassischer ML-Algorithmen, die oft ein nicht vorhandenes Quanten-RAM für Geschwindigkeitssteigerungen voraussetzen.

Die QVC-Literatur behandelt vor allem die Nachbildung neuronaler Netzarchitekturen, wobei der Schwerpunkt auf Bildklassifizierung liegt. QVCs erzielen häufig konkurrenzfähige Ergebnisse und übertreffen klassische neuronale Netze in einigen Fällen.

Durch den Wechsel vom Bit zum QBit besteht die Chance auf Vorteile im QML.

Erforschung von QVCs: Experimente auf IBM-Hardware

Im zweiten Teil des Projekts wurden Experimente zur Zeitreihenklassifizierung anhand eines von IBM vorgeschlagenen Datensatzes durchgeführt. Diese Untersuchungen sind nicht nur projektrelevant, sondern haben auch wissenschaftlichen Wert, da Zeitreihenklassifizierung mit Quantenmethoden kaum erforscht ist. Daher wurden zwei klassische, neuronale Methoden mit ihren hybriden Quantenvarianten verglichen - ergänzt durch eine Analyse der Leistung auf Simulatoren und realer Quantenhardware.

Während Quantenalgorithmen in Simulationen mit klassischen Methoden mithalten konnten, verschlechterte sich ihre Performanz auf echter Quantenhardware deutlich – im Gegensatz zu früheren Studien zu Nicht-Zeitreihenproblemen. Zudem bleibt die Skalierbarkeit kritisch, da einzelne Berechnungen auf Quantencomputern mehrere Stunden dauerten.

Zusammenfassend zeigt QML großes Potenzial für verschiedene Anwendungen, insbesondere durch geringere Parameteranforderungen und konkurrenzfähige Leistung. Allerdings bleiben erhebliche Hardware-Herausforderungen bestehen, insbesondere die hohe Anfälligkeit aktueller Quantenhardware für Rauschen.

Juniorprof. Dr. Maximilian Moll

maximilian.moll@unibw.de

+49 89 6004 2248

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

Wir entwickeln intelligente Methoden, um reale Datenherausforderungen wie Ungleichgewichte und sich verändernde Datensätze zu bewältigen und das Gemeinwohl zu fördern. Unsere Forschung konzentriert sich auf verantwortungsvolle KI (Fairness, Erklärbarkeit, Robustheit), adaptives Lernen und generative KI, um neue Lösungen zu schaffen, einschließlich der Generierung von Daten zur Verbesserung der KI-Qualität. Anwendungen finden sich in zentralen Bereichen wie Bildung, Landwirtschaft, Banken und Ingenieurwesen.

DIE GRUPPE FÜR Künstliche Intelligenz und Maschinelles Lernen (AIML) konzentriert sich auf die Erforschung und Entwicklung intelligenter Algorithmen, die reale Datenprobleme lösen und zum gesellschaftlichen Wohl beitragen. Unsere Arbeit wird von drei Kernfragen geleitet: Wie können wir intelligente Maschinen für die reale Welt bauen? Welche Art von Intelligenz streben wir an, zu erschaffen? Und kann KI Kreativität zeigen – und wie können wir diese Kreativität für sinnvolle Anwendungen nutzen? Unsere Forschung konzentriert sich auf verantwortungsvolle KI (Fairness, Erklärbarkeit, Robustheit), adaptives Lernen und generative KI. Diese Bereiche decken mehrere Anwendungsdomänen ab, einschließlich Bildung, soziale Netzwerke, Banken, Landwirtschaft, Fertigung und Ingenieurwesen.

Forschungshighlights

Im 2024 hat unsere Gruppe bedeutende Beiträge im Bereich der KI geleistet. Zu den Höhepunkten gehört TABCF, eine neuartige Methode für kontrafaktische Erklärungen für tabellarische Daten mithilfe eines transformer-basierten VAE (ACM ICAIF 2024) und eine transparente Nachbarschafts-Näherungsmethode für Texterklärungen (EEE DSAA 2024). Wir haben auch FairBranch entwickelt, eine bias-empfindliche Methode für das Multi-Task-Lernen zur Minderung negativer und bias-bezogener Übertragungen zwischen Aufgaben (IEEE IJCNN 2024) sowie eine Methode für fairen Graph-Clustering mithilfe kontrastiver Regularisierung (PAKDD 2024).

Projekthighlights

Das EU-Projekt MAMMOTH förderte KI mit Fairness-Bewusstsein, indem es Werkzeuge zur Minderung von Vorurteilen über verschiedene Datentypen und multidimensionale Identitäten entwickelte, mit Anwendungen im Finanzwesen und der Identitätsverifikation. Das EU-Projekt STELAR entwickelte ein Wissenssee-Management-System für FAIR- und KI-fähige Daten, das im Agrar- und Lebensmittelsektor pilotiert wurde. Das DFG-Projekt HEPHAESTUS verbesserte die adaptive Prozessplanung für 5-Achs-Fräsen, erhöhte die Genauigkeit und reduzierte manuelle Anpassungen. Schließlich wurde das DFG SFB1463 erfolgreich abgeschlossen, das Simulationen und KI zur Optimierung des Designs und Betriebs von Offshore-Megastrukturen integrierte. Unsere Beiträge umfassen einen neuartigen Datensatz für das datengestützte konzeptionelle Design von Offshore-Jacket-Substrukturen (veröffentlicht in *Ocean Engineering*), der die Bedeutung hochwertiger Daten im Ingenieurwesen unterstreicht.

Internationale Präsenz

Unsere Gruppe förderte ihre Arbeit auf internationalen und regionalen Foren und erreichte ein breites Publikum. Ein bedeutendes Ereignis war die Einführungsveranstaltung des AI Fairness Cluster & Workshop zum Thema KI-Vorurteile in Amsterdam, bei dem über 50 Institutionen zusammenkamen, um KI-Vorurteile zu thematisieren. Beim Versus Festival in Österreich trugen wir zur Podiumsdiskussion „AI vs. Mensch“ bei, und auf der Intl. Conf. on Web Engineering in Finnland nahmen wir an der Diskussion „Weaving an Ethical and Human-Centric Web“ teil. Prof. Ntoutsi fungierte als Programm-Co-Chair der ECML PKDD 2024 in Litauen, einer der führenden Konferenzen im Bereich Maschinelles Lernen, und organisierte gemeinsam den ReAI-Workshop auf SETN in Griechenland, bei dem die Zukunft der KI diskutiert wurde. Außerdem boten wir einen fortgeschrittenen Kurs zum Thema „Fairness und Erklärbarkeit – Modelle, Messungen und Minderungstechniken“ auf der ESSAI 2024 in Athen an und leiteten einen Ferienworkshop für Mädchen im Rahmen von UniBw M: Starke Mädchen machen MI(N)T!, um sie in verantwortungsvolle KI einzuführen.

Mit Blick auf 2025 konzentrieren wir uns darauf, die komplexen Herausforderungen zu bewältigen, die durch die rasche technologische, gesellschaftliche und rechtliche Entwicklung entstehen, mit innovativen und verantwortungsvollen KI-Lösungen.

Prof. Dr. Eirini Ntoutsi

eirini.ntoutsi@unibw.de

+49 89 6004 7420

https://www.unibw.de/aiml

ABB.: ADOBE STOCK / LUCEGRAFIAR; ADOBE STOCK / STARLIGHT

Prof. Dr. Stefan Pickl

Operations Research – Forschungsgruppe COMTESSA

Die Professur für Operations Research hat in den letzten Jahren das Kompetenzzentrum COMTESSA (Core Competence Center for Operations Research, Management Intelligence Tenacity Excellence, Safety & Security ALLIANCE) begleitend entwickelt. Im wissenschaftlichen Interesse stehen die Analyse und Simulation komplexer Systeme sowie die Entwicklung von datengetriebenen Optimierungsverfahren zur IT-basierten Entscheidungsunterstützung. Seit 2023 ist Prof. Dr. Stefan Pickl ordentliches Mitglied der Deutschen Akademie der Technikwissenschaften (acatech).

Projekt REAVRS

Identifikation komplexer Angriffspotentiale für das System Bahn

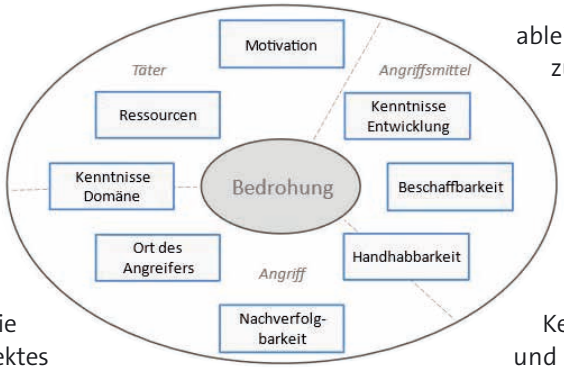
Basierend auf der zunehmenden Anwendung von Digitalisierungsaspekten wie Big Data, IT etc., weist das System Bahn eine erhöhte Vulnerabilität gegenüber Angriffen von Dritten auf. Ein generelles Vorgehen bzgl. einer einheitlichen Angriffssicherheit hat sich bis dato nicht durchgesetzt. REAVRS entwickelt ein komplexes Vulnerabilitätsmodell des Systems Bahn, um anschließend intelligente (AI-basierte) Maßnahmen gegen physische- als auch Cyber-Gefahren zu entwickeln.

Zielsetzung

Ziel des Projekts REAVRS – einem Forschungsvorhaben vom Deutschen Zentrum für Schienenverkehrsforschung (DZSF) – ist die Charakterisierung und Analyse der aktuellen Vulnerabilität des deutschen Eisenbahnsystems. Die teilnehmenden Partner des Projektes sind die Universität der Bundeswehr München, Fakultät für Informatik – Institut 1, Chair for Operations Research, Forschungsgruppe COMTESSA (Projektleitung) in Kooperation mit dem Forschungsinstitut CODE sowie der Ingenieurgesellschaft für Verkehrs- und Eisenbahnwesen mbH (IVE mbH), der CreaLab GmbH und dem Institut für Verkehrswesen, Eisenbahnbau und -betrieb (IVE) an der TU Braunschweig.

OR-basierte Systemanalyse

Der Fokus des Projekts liegt auf der Entwicklung eines komplexen Vulnerabilitätsmodells. Eine funktionale systematische Abbildung des (deutschen) Eisenbahnsystems wird entwickelt, gefolgt von einer präzisen Charakterisierung und Analyse erfolgter Angriffe sowie einer Beschreibung typischer Systemumgebungen. Angriffsmöglichkeiten bzw. Bedrohungsszenarien werden systematisiert, und eine Gefährdungsidentifikation wird auf Basis einer OR-basierten Systemanalyse zur Risikoanalyse erstellt.



Identifikation von Kenngrößen für die Bedrohung.

Cyber-Vignetten und Angriffsszenarien

Nach Vorauswahl von Angriffspunkten werden diese zu beispielhaften Modell-Vignetten entwickelt. Bei der Systematisierung der Angriffsmittel wurden mehr als 500 physische und fast 1000 mögliche Cyberangriffe identifiziert. Eine Ursachenanalyse wird mit einer Selektion und auch Neugenerierung von repräsentativen Vignetten durchgeführt. Im finalen Schritt wird die entwickelte Methodik in eine komfortable IT-basierte Entscheidungsunterstützung Umgebung und ein zukunftsweisendes Managementcockpit eingebettet.

Identifikation von Kenngrößen

Werden die Vignetten im Detail betrachtet, so lassen sich die in der Abbildung dargestellten Kenngrößen ableiten. Sie sind die Grundlage eines zu entwickelnden Management Cockpits (Comtessa Suite).

Safety & Security Living Lab

Nach der Identifikation der Kenngrößen für die Bedrohung werden die einzelnen Kenngrößen quantitativ bewertet und in eine Sicherheitsarchitektur eingebettet. Diese detaillierte Ursachenanalyse geht in die anschließende komplexe Risikoanalyse ein. Aktuell wird auch eine automatisierte Version des Bedrohungsmodells sowie ein unterstützendes Management Cockpit erarbeitet, um ein Lagebild für die Vulnerabilität des deutschen Eisenbahnsystems zu entwickeln und eine Integration des „Safety & Security“ Living-Lab am House of Logistics and Mobility (HOLM) zur Sicherheitsanalyse vorzubereiten.

Prof. Dr. Stefan Pickl
stefan.pickl@unibw.de
+49 89 6004 2400
https://go.unibw.de/reavrs

Gefördert durch: Deutsches Zentrum für Schienenverkehrsforschung (DZSF)

PD Dr. Corinna Schmitt

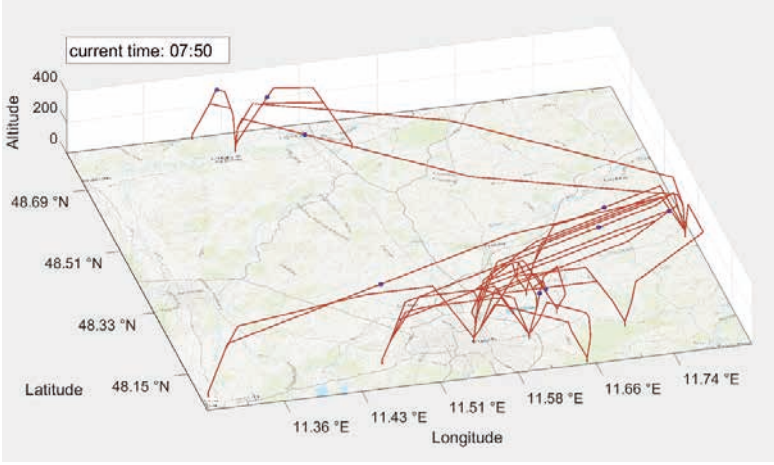
Projekt AMIUS

Das Forschungsinstitut CODE ist Partner im Projekt AMIUS – Air Mobility Integration U-Space. Ziel ist die Schaffung des ersten integrierten bayerischen U-Raums, der die Stadt Ingolstadt mit dem Flughafen Manching verbindet. Zusammen mit regionalen Industriepartnern werden entsprechende Kommunikationskonzepte und modellbasierte Umsetzbarkeitsansätze spezifiziert und ein erster Prototyp entwickelt.

DAS AMIUS PROJEKT ist eines der zahlreichen geförderten Projekte des Förderprogramms „Air Mobility“ durch das Bayerische Staatsministerium für Wirtschaft, Landesentwicklung und Energie. Ziel ist die Schaffung des ersten integrierten bayerischen U-Space (Urban-Space = Verkehrsmanagement für unbemannte Luftfahrzeuge), der die Stadt Ingolstadt mit dem Flughafen Manching bzw. mit der Metropole München verbindet. Das Konsortium setzt sich aus regionalen Industriepartnern (u. a. Airbus Defence and Space, Airbus Urban Mobility und SkyFive) sowie akademischen Einrichtungen (UniBw M/FI CODE und TU München) zusammen. Das FI CODE wird mit Expertisen des assoziierten Partners Institut für Lufttransportsysteme (ILT) der TU Hamburg (TUHH) unterstützt.

Neben den hier beschriebenen Aktivitäten steht der geschaffene U-Space als reales Testfeld für die Nutzung durch bayerische Unternehmen der elektrischen Senkrechtstarter (eVTOLs, bspw. Lufttaxis oder Helikopter) und unbemannte Luftfahrzeugsysteme (UASs; bspw. Drohnen oder Luftschiffe) - Industrie zur Verfügung. Im Projekt wird untersucht, wie ein auf digitalen Diensten basierender U-Raum den heutigen Luftverkehr mit seinen Prozessen und Technologien mit zukünftigen Einsatzszenarien von UASs und eVTOLs in einem gemeinsamen Luftraum integrieren kann. Zu diesem Zweck werden die erforderlichen Flugverkehrsmanagementfunktionen für einen sicheren, integrierten und effizienten Betrieb durch die von der Europäischen Agentur für Flugsicherheit (EASA) definierten U-Raum-Dienste bereitgestellt und demonstriert. Basierend auf diesen digitalen Diensten sind Flüge innerhalb der Kontrollzone Manching, z. B. vom Drohnenzentrum zum Hauptbahnhof Ingolstadt, als konkrete Anwendungsfälle geplant. Diese praktischen Demonstrationen werden durch entsprechende wissenschaftliche modellbasierte Voruntersuchungen, multimodale Simulationen mit verschiedenen Verkehrssystemen, Machbarkeitsstudien sowie Kostenanalysen der beteiligten Hochschulen unterstützt.

Um in Zukunft einen sicheren und effizienten integrierten Betrieb von UASs, eVTOLs und allgemeiner Luftfahrt zu gewährleisten, sind neuartige Verkehrskonzepte erforderlich. Dazu muss das bestehende Luftraummanagement durch ein integriertes UAS Traffic Management System (UTM) ergänzt und damit um die Dimension des bisher unkontrollierten Luftraums erweitert werden. Der Fokus liegt auf der Konzeption und technischen Umsetzung des Demonstrators mit einem UTM-System und entsprechenden Bodeninfrastrukturen, ergänzt durch innovative Kommunikationstechnologien und eine zentrale Kontrollstation. Im Rahmen des Projekts wird auch untersucht, wie einerseits der Datenfluss zwischen den beteiligten Luftraumnutzern und andererseits die Speicherung relevanter Daten gegen unbefugte externe Eingriffe gesichert werden kann.



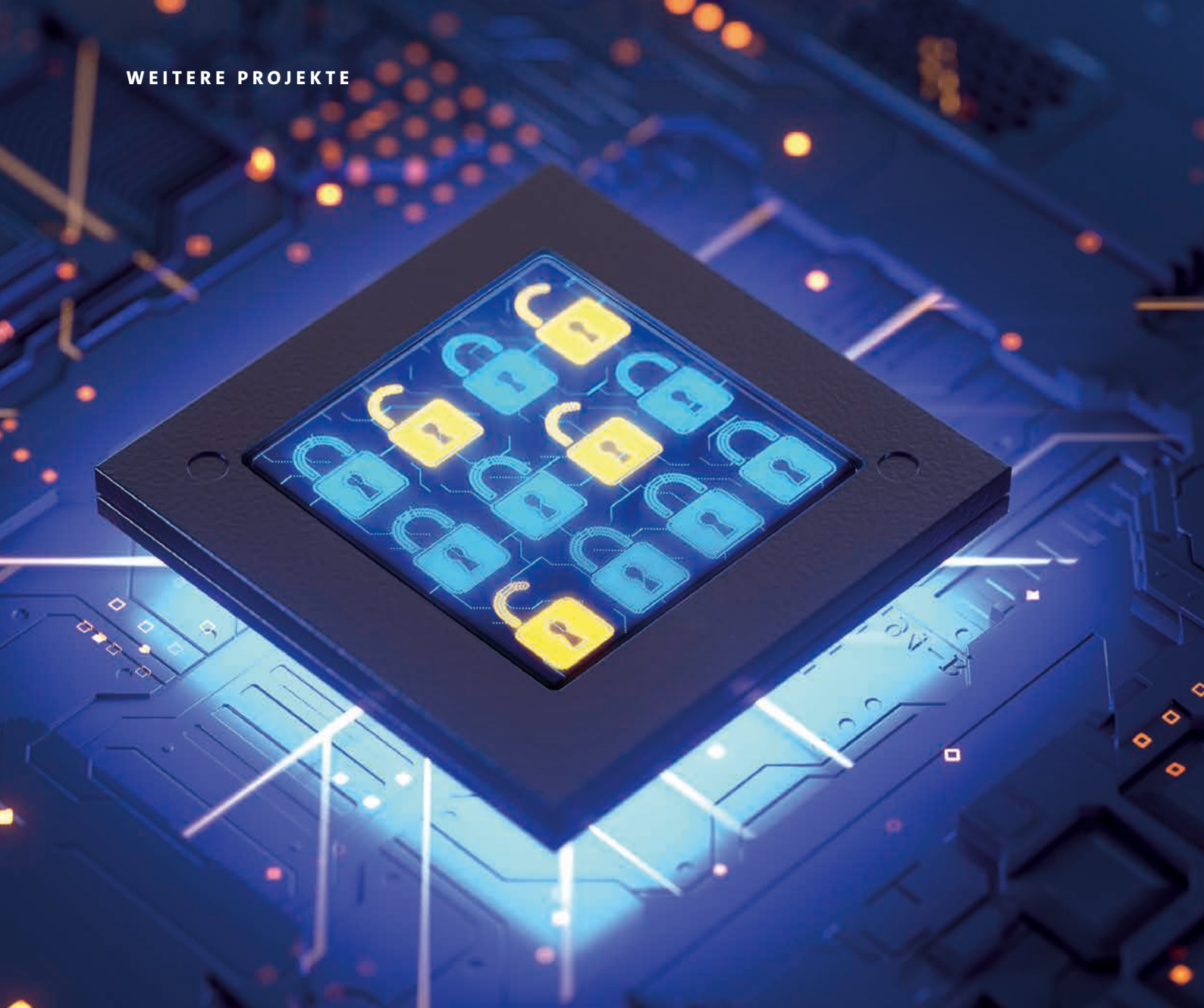
Simulation geflogener Trajektorien im AMIUS U-Space Ingolstadt – München.

Im Rahmen des Verbundprojekts AMIUS verfolgt das FI CODE zusammen mit dem ILT der TUHH zwei Ziele im Bereich der UAS-Forschung: (1) Auf Basis eines skalierbaren modellbasierten Ansatzes und in enger Verbindung mit realen Testansätzen der Projektpartner sollen belastbare Aussagen zur Realisierung der notwendigen Führungs- und Kommunikationsinfrastruktur für die urbane Luftmobilität getroffen werden. (2) Es werden Lösungen für eine sichere Cloud-basierte Datenspeicherung im Betrieb und über den Lebenszyklus erarbeitet, um die Verzögerung der Datenanalyse und -kommunikation zu reduzieren. Die entwickelten Simulationen, Kosten- und Infrastrukturabschätzungen sowie die Cloud-Konzepte und Standardanalysen werden für die technische Entwicklung eines Prototyps zur Verfügung gestellt.

PD Dr. Corinna Schmitt
corinna.schmitt@unibw.de
+49 89 6004 7314
https://go.unibw.de/amius

Gefördert durch: Bayerisches Staatsministerium für Wirtschaft, Landesentwicklung und Energie (Nr. ROB-2-3410.20-04-11-15/HAMI-2109-001)

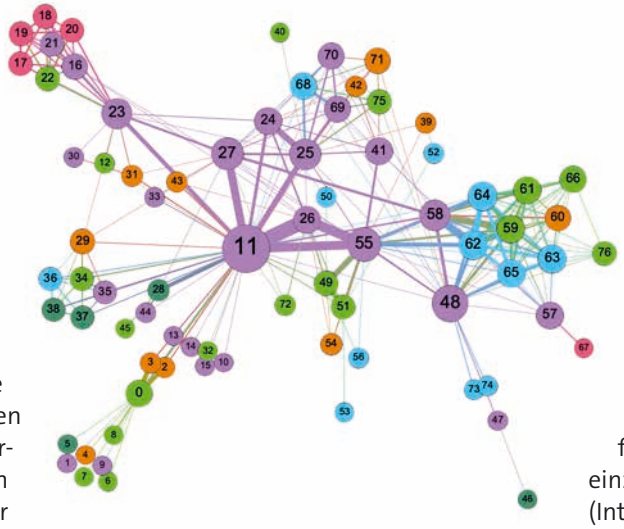
ABB.: AIRBUS HELICOPTERS / CHRISTIAN KELLER; AMIUS REPORT



Prof. Dr. Gunnar Teege

Formale Methoden für die Sicherheit von Dingen (FOMSET)

Die Forschungsgruppe FOMSET verwendet formale Methoden, um IT-Sicherheit im Bereich eingebetteter und cyberphysischer Systeme zu erreichen. Beispiele sind formale Softwareverifikation für Betriebssysteme und die graphenorientierte Modellierung von IoT-Netzwerken. Die Forschung erfolgt im Rahmen von Doktorarbeiten und Industrieprojekten.



Ein Graph-Modell eines IoT-Netzes aus Geräten mit unterschiedlichen Eigenschaften.

DAS ZIEL der Forschungsgruppe von Prof. Dr. Gunnar Teege ist es, den Einsatz formaler Methoden für die Absicherung von IT-Systemen zu erhöhen. Dazu werden verschiedene Arten von Systemen betrachtet und jeweils für spezifische Sicherheitseigenschaften passende Methoden untersucht.

Formale Verifikation von Systemsoftware

Systemsoftware wie Gerätetreiber und andere Betriebssystem-Komponenten ist häufig besonders kritisch für die Sicherheit des gesamten darauf aufbauenden IT-Systems, daher ist der formale Nachweis, dass keine Fehler oder Schwachstellen enthalten sind, hier besonders relevant. Gleichzeitig wird Systemsoftware auch heute noch häufig in Programmiersprachen wie C oder C++ oder sogar in Assemblersprachen implementiert, dies macht den Zugang für formale Verifikation besonders schwierig und aufwändig. Hier ist das Ziel der Gruppe, den Automatisierungsgrad für formale Nachweise mit Hilfe von mathematischen Beweisassistenten wie Isabelle oder Coq zu erhöhen.

Attestierung von Cloud-Systemen basierend auf Mikrokernen

Nutzer eines Cloud-Systems müssen sich darauf verlassen können, dass für ihre Anwendungen Sicherheitseigenschaften wie Integrität und Vertraulichkeit gewahrt bleiben. Dies setzt voraus, dass das Cloud-System keine Verletzung dieser Eigenschaften ermöglicht und dem Nutzer manipulationssichere Nachweise darüber geben kann („Attestierung"). Hierzu wird in der Gruppe untersucht, wie sich solche Nachweise auf Basis von Mikrokernen wie dem formal verifizierten seL4 erstellen lassen.

Graphbasierte Modellierung von Malware-Infektionen in IoT-Netzen

Die große Anzahl und häufig schlechte Absicherung der einzelnen Geräte in IoT-Netzen (Internet of Things) macht es kaum möglich, solche Netze mit herkömmlichen Maßnahmen wie Sicherheitsupdates vor Angriffen zu schützen. In der Gruppe werden graphbasierte Modelle der Geräte und ihrer Verbindungen verwendet, um sicherheitsrelevante Strukturen in den Netzen zu erkennen und auszunutzen. Dabei werden Methoden, die im Bereich sozialer Netze für die Verbreitung von Informationen und auch für Infektionskrankheiten entwickelt wurden, auf IoT-Netze übertragen.

Absicherung von Fahrzeug-Netzen mittels Blockchain-Technologie

Vernetzte Fahrzeuge tauschen Informationen untereinander und mit der Verkehrs-Infrastruktur aus. Dieser Austausch ist umso effektiver, je mehr Instanzen daran teilnehmen können, gleichzeitig erhöht dies die Gefahr von Angriffen auf Integrität, Verfügbarkeit und ggf. Vertraulichkeit der Informationen. Die Blockchain-Technologie wurde entwickelt für Krypto-Währungen und wird auch eingesetzt für die Nachverfolgung von Gütern, für die Anwendung in Fahrzeug-Netzen muss sie modifiziert werden. In der Gruppe wird untersucht, welche Modifikationen erforderlich sind, um verifizierbare Sicherheitseigenschaften für Fahrzeug-Netze zu erhalten.

Prof. Dr. Gunnar Teege

gunnar.teege@unibw.de

+49 89 6004 3353

www.unibw.de/fomset

ABB.: [M] SHUTTERSTOCK / BLUE ANDY, ISTOCK / MATEJMO; FARELL FOLLY

ABB.: ADOBE STOCK / KILLYKOON

Kooperationen

Deutschland und die Welt

Nationale Partner

Das FI CODE arbeitet in Deutschland mit 68 Partnern in 40 Städten und Gemeinden zusammen.

DIE ZUSAMMENARBEIT mit anderen Universitäten, öffentlichen Einrichtungen und Wirtschaftsunternehmen gehört zum Selbstverständnis von CODE: Mit und von unseren Partnern lernen wir und können erste Schritte in Richtung der Umsetzung unserer Forschungsergebnisse in der Praxis gehen.

Gleichzeitig sorgt der enge Austausch dafür, dass wir die konkreten Frage- und Problemstellungen unserer Partner verstehen und aus wissenschaftlicher Perspektive betrachten können.

Innerhalb von Deutschland ist unser Netzwerk besonders eng. Als Teil der Universität der Bundeswehr München arbeiten wir bundesweit mit 68 Institutionen in 40 Städten und Gemeinden zusammen. Besondere Schwerpunkte liegen dabei auf Bayern bzw. dem Münchner Raum, Nordrhein-Westfalen und Hessen. ■

	Partner	Ort
1	Rheinisch-Westfälische Technische Hochschule Aachen (RWTH Aachen)	Aachen
2	Landkreis Bad Kissingen	Bad Kissingen
3	Akhetonics GmbH	Berlin
4	Deutsches Institut für Normung (DIN)	Berlin
5	Freie Universität Berlin (FU)	Berlin
6	Hochschule für Wirtschaft und Recht Berlin (HWR Berlin)	Berlin
7	Verein zur Förderung eines Deutschen Forschungsnetzes e. V. (DFN)	Berlin
8	Hochschule Bielefeld (HSBI)	Bielefeld
9	IDEMIA Identity & Security Germany AG	Bochum
10	Ruhr-Universität Bochum (RUB)	Bochum
11	Bundesamt für Sicherheit in der Informationstechnik (BSI)	Bonn
12	Zentrum Digitalisierung der Bundeswehr und Fähigkeitsentwicklung Cyber- und Informationsraum (ZDigBw)	Bonn
13	Technische Universität Chemnitz	Chemnitz
14	Fraunhofer-Institut für Graphische Datenverarbeitung (IGD)	Darmstadt
15	GSI Helmholtz-Zentrum für Schwerionenforschung	Darmstadt
16	Hochschule Darmstadt (h_da)	Darmstadt
17	Nationales Zentrum für angewandte Cybersicherheit ATHENE	Darmstadt
18	Technische Universität Darmstadt	Darmstadt
19	RapidMiner GmbH	Dortmund
20	Helmholtz-Zentrum Dresden-Rossendorf (HZDR)	Dresden
21	Technische Universität Dresden (TUD)	Dresden
22	Landeskriminalamt Nordrhein-Westfalen (LKA NRW)	Düsseldorf
23	Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)	Erlangen/Nürnberg
24	Cyber Security Operations Centre der Bundeswehr (CSOCBw)	Euskirchen
25	Frankfurt University of Applied Sciences	Frankfurt a. M.
26	nuix	Frankfurt a. M.
27	Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ)	Garching
28	Wehrtechnische Dienststelle für Informationstechnologie und Elektronik (WTD 81)	Greding
29	Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur)	Halle/Saale
30	Führungsakademie der Bundeswehr (FüAkBw)	Hamburg
31	Helmut-Schmidt-Universität/Universität der Bundeswehr Hamburg (HSU/UniBw H)	Hamburg
32	Gottfried Wilhelm Leibniz Universität Hannover (LUH)	Hannover
33	Medizinische Hochschule Hannover (MHH)	Hannover
34	Fraunhofer-Institut für Digitale Medientechnologie (IDMT)	Ilmenau

	Partner	Ort
35	Karlsruher Institut für Technologie (KIT)	Karlsruhe
36	Christian-Albrechts-Universität zu Kiel (CAU)	Kiel
37	Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw)	Koblenz
38	Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)	Köln/Oberpfaffenhofen
39	Universität Konstanz	Konstanz
40	Minol-ZENNER-Gruppe	Leinfelden-Echterdingen
41	Otto-von-Guericke-Universität Magdeburg (OVGU)	Magdeburg
42	BWI GmbH	Meckenheim
43	Bayerisches Landeskriminalamt (BLKA)	München
44	ESG Elektroniksystem- und Logistik-GmbH	München
45	FAST-DETECT GmbH	München
46	Ludwig-Maximilians-Universität München (LMU)	München
47	MTU Aero Engines AG	München
48	Polizeipräsidium München	München
49	Siemens Energy AG	München
50	Technische Universität München (TUM)	München
51	VISTA Geowissenschaftliche Fernerkundung GmbH	München
52	Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)	München
53	Infineon Technologies AG	Neubiberg
54	Bayerisches Landesamt für Sicherheit in der Informationstechnik (LSI)	Nürnberg
55	Carl von Ossietzky Universität Oldenburg	Oldenburg
56	Universität Potsdam (UP)	Potsdam
57	Marinekommando (MarKdo)	Rostock
58	CISPA Helmholtz-Zentrum für Informationssicherheit	Saarbrücken
59	Leibniz-Institut für Neue Materialien (INM)	Saarbrücken
60	Landeskriminalamt Baden-Württemberg (LKA BW)	Stuttgart
61	Airbus Defence and Space GmbH	Taufkirchen
62	Airbus Protect GmbH	Taufkirchen
63	Hensoldt Cyber GmbH	Taufkirchen
64	Eberhard Karls Universität Tübingen	Tübingen
65	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)	Wachtberg/Bonn
66	Hessisches Landeskriminalamt (HLKA)	Wiesbaden
67	Hessisches Polizeipräsidium für Technik (HPT)	Wiesbaden
68	Bundeskriminalamt (BKA)	Wiesbaden/Berlin

ABB.: TAUSENDBLAUWERK.DE


36 Kiel
Rostock
57
30
31
Hamburg
3
4
5
6
7
68
Berlin
55
Oldenburg
32
33
Hannover
56 Potsdam
8
Bielefeld
41 Magdeburg
9
10
Bochum
Dortmund
19
Halle/Saale 29
20
21
Dresden
22 Düsseldorf
13
Chemnitz
Köln 38
11
12
1 Aachen
34 Ilmenau
Bonn
65
24 Euskirchen
Meckenheim
Wachtberg
42
37 Koblenz
25
26
Frankfurt/Main
2
Bad Kissingen
66 67 68 Wiesbaden
Darmstadt
14
15 16
17 18
Erlangen 23
Nürnberg 54
58
59
Saarbrücken
Greding 28
35
Karlsruhe
43 44
45 46
47 48
49 50
51 52
60
Stuttgart
Leinfelden-
Echterdingen
64 Tübingen
40
27
Garching
München
Neubiberg 53
Oberpfaffenhofen
38
Taufkirchen
61 62 63
39
Konstanz
Legende
1 Standortnummer der Partner
Standorte der Partner

Internationalität

Auch international pflegt das FI CODE ein großes Netzwerk. Im Jahr 2024 stammten die Mitarbeitenden aus 17 Ländern. In 26 Ländern gab es 76 Kooperationspartner.

ABB.: ISTOCK / BLUE PLANET STUDIO

Mitarbeitende

Nationalität	Anzahl
argentinisch	1
brasilianisch	1
bulgarisch	1
deutsch	111
finnisch	1
französisch	4
griechisch	2
indisch	6
italienisch	2
kosovarisch	1
kroatisch	1
niederländisch	1
österreichisch	10
polnisch	1
slowenisch	1
spanisch	2
südkoreanisch	1
Gesamt	**147**

Internationale Kooperationspartner

Land	Partner
Australien	CSIRO Data61
	Royal Melbourne Institute of Technology (RMIT)
Belgien	KU Leuven
Dänemark	Technical University of Denmark
Estland	eu-LISA
Finnland	Tampere University
Frankreich	Air and Space Force Academy Research Center (CREA)
	ARIADNEXT
	EURECOM
	Telecom SudParis
	Grenoble Alps University (UGA)
Griechenland	Agroknow IKE
	Athena Research and Innovation Center (ARC)

Land	Partner
Griechenland	Centre for Research and Technology Hellas (CERTH)
	EXUS Software
	Harokopio University of Athens
	IASIS NGO
	University of Athens (UoA)
	Ubitech
	University of Ioannina
	University of Piraeus
Irland	Trilateral Research Limited Ireland (TRI-IE)
Israel	Ben-Gurion University of the Negev
Italien	Abaco S.p.A.
	Fondazione Bruno Kessler (FBK)
	University of Bologna
	University of Genoa
	University of Roma Tre
	University of Trento
	University of Turin
Japan	Kyoto University
	National Institute of Information and Communications Technology (NICT)
	NTT Social Informatics Laboratories
Liechtenstein	University of Liechtenstein
Luxemburg	University of Luxembourg
Neuseeland	University of Auckland
Niederlande	Eindhoven University of Technology (TU/e)
	University of Groningen
	University of Twente
Norwegen	Norwegian University of Science and Technology (NTUT)
	University of Oslo
Österreich	Austrian Institute of Technology (AIT)
	Austrian Armed Forces
	Carinthia Emergency Services
	Complexity Science Hub Vienna (CSH)
	Johannes Kepler University Linz (JKU)

Land	Partner
Österreich	Kelag-Konzern
	Municipality of Neuhaus, Carinthia
	P.SYS Caring Systems
	Software Competence Center Hagenberg
	University of Applied Sciences Campus Vienna
	Paris Lodron University of Salzburg (PLUS)
	Vienna University of Technology
Polen	Wroclaw University of Science and Technology (WUST)
Schweiz	EPFL
	Idiap Research Institute
	University of St. Gallen (HSG)
Serbien	Foodscale Hub
Spanien	Association Fòrum Dona Activa 2010
	Autonomous University of Madrid (UAM)
Südkorea	Korea Institute of Science and Technology Information (KISTI)
	University of Science and Technology (UST)
Tschechien	Center for Environmental and Technology Ethics
	Masaryk University (MU)
USA	Auburn University, College of Engineering
	Brave Software
	Brown University
	City University of New York (CUNY)
	Michigan State University
	Naval Postgraduate School (NPS)
	University of Arizona, College of Engineering
Vereinigtes Königreich	Imperial College London
	Trilateral Research Limited UK (TRI-IE)
	University of Sheffield
	University of Surrey
Zypern	Centre for Social Innovation Ltd. (CSI)

ABB.: ADOBE STOCK / ALFASMART

Nachwuchs-förderung

Chancen und Angebote

Studienpreis des Forschungsinstituts CODE 2024

Szenarioanalyse im Projekt NEWSROOM

Das Forschungsinstitut Cyber Defence (CODE) zeichnet gemeinsam mit der Firma Giesecke+Devrient GmbH die Abschlussarbeit von Annika S. mit dem CODE-Studienpreis 2024 aus. In ihrer Masterarbeit befasste sie sich mit Cybersicherheitsszenare und ging methodisch dabei innovative Wege. Der CODE-Studienpreis wurde im Rahmen der großen Masterfeier am 14. Dezember 2024 auf dem Campus der Universität der Bundeswehr München verliehen.

DIE ZUNAHME VON Cyberangriffen auf kritische Infrastrukturen oder die Cyberangriffe im Zusammenhang mit dem Ukraine-Krieg sind nur zwei Beispiele für die zahlreichen Herausforderungen, denen sich Regierungen und Staaten derzeit gegenübersehen. Gleichzeitig wird die Cybersicherheit in ganz Europa dank der von der Europäischen Union (EU) formulierten Richtlinien stetig verbessert. Um jedoch das Ziel eines einheitlichen Sicherheitsniveaus zu erreichen, ist u. a. auch die Förderung des Austauschs und der Zusammenarbeit zwischen den europäischen Ländern zu allen Themen der Cybersicherheit entscheidend.

Im Rahmen des vom European Defence Fund geförderten Forschungsprojekts NEWSROOM werden Systeme und Methoden für das Cyber-Situationsbewusstsein entwickelt. Vor diesem Hintergrund war das Ziel der Arbeit, Workshops zu konzipieren, durchzuführen und auf der Grundlage der Workshop-Ergebnisse verschiedene Szenarios der Cybersicherheit in der EU zu entwickeln.

Als methodischer Rahmen der Arbeit diente der Design-Science-Ansatz für die Entwicklung eines innovativen Workshop-Formats. Aufbauend auf einer State-of-the-Art Analyse wurden innovative effektive, ansprechende Workshops konzipiert und durchgeführt. Aus den Ergebnissen der Workshops wurden wiederum verschiedene Angriffsvektoren und Mitigationsmaßnahmen abgeleitet. Im Ergebnis präsentiert die Arbeit eine Sammlung von acht verschiedenen, neuartigen Cybersicherheits-Szenarios.

In ihrer Masterarbeit „Szenarioanalyse im Rahmen des Projekts NEWSROOM“ hat Annika S. ein innovatives Format entworfen, das die Entwicklung von Cybersicherheits-Szenarios in einem kollaborativen Setting ermöglicht. Das Format ist dabei auf die Anforderungen des Forschungsprojekts NEWSROOM abgestimmt ist: es adressiert die Sicherheit kritischer Infrastrukturen, die militärische Domäne, Angreifer- und Verteidigersicht und vor allem die Zusammenarbeit auf europäischer Ebene. Auch zeigt ihr Format auf, wo Expertinnen und Experten potenzielle Bedrohungen vermuten und wie schwierig es ist, auf europäischer Ebene eine Kooperation zu definieren.

Annika S. hat mit internationalen Partnern des Forschungsprojekts NEWSROOM Szenario-Workshops durchgeführt und diese moderiert, hat die Ergebnisse gesichert und analysiert, um letztendlich die Szenarien zu entwickeln. In ihrer Arbeit hat sie konzeptionelles Neuland betreten und konnte durch Kreativität, Kompetenz und ihre Fähigkeiten in der Moderation sowie der Analyse und dem Design der Szenarien überzeugen. Ihre Masterarbeit gibt der Cybersicherheits-Forschung – nicht nur im Projekt NEWSROOM – neue Impulse. ■

Prof. Geralt Siebert (l.), Prof. Karl-Heinz Renner (2. v. l.), Präsidentin Eva-Maria Kern (3. v. l.) und die Preisträgerinnen und Preisträger der diesjährigen Studien- und Sonderpreise nach der Preisverleihung.

ABB.: ADOBE STOCK / CREATIVE BRINGER; UNIVERSITÄT DER BUNDESWEHR MÜNCHEN / SIEBOLD

Studienpreise der Universität der Bundeswehr München

Die Universität der Bundeswehr München vergibt jedes Jahr mehrere Studienpreise, die von unterschiedlichen Partnern gestiftet werden. Mit dem Studienpreis des Forschungsinstituts CODE werden seit 2018 herausragende Master-Absolventinnen und -Absolventen mit einer einschlägigen Arbeit aus dem Themenspektrum Cyber Defence ausgezeichnet. Er wird gestiftet von der Giesecke+Devrient GmbH und ist mit 1.000 € dotiert. ■

Die Preisträger der letzten Jahre

Jahr	Preisträger	Schwerpunkt der Arbeit
2018	Christian Siegert	Automatisiertes Aufspüren von IT-Sicherheitslücken
2019	Philipp Sammeck	Sicherheitsanalyse eines elektronischen Tresorschlosses
2020	Robert Jurisch-Eckardt	Entwicklung eines Systems zur Bekämpfung von Cybercrime
2021	Martin Lukner	Synthetisierung von Malware-Spuren für die digitale Forensik
2022	Lars Fuchs	Effiziente Nutzbarmachung von Schwachstellen in Telekommunikationsendgeräten
2023	Hannes Ludwig	An Approach to Creating Adversarial Samples
2024	Annika S.	Szenarioanalyse im Rahmen des Projekts NEWSROOM

Studieren am Forschungsinstitut CODE

Der **Masterstudiengang Cyber-Sicherheit** am FI CODE der Universität der Bundeswehr München befasst sich mit Informationsverarbeitungs-Prozessen, deren Planung, formaler Modellierung, Implementierung und Einsatz mit einem Fokus auf technische und organisatorische Informationssicherheit. Neben fundierten theoretischen Methoden werden insbesondere auch praxisrelevante Fähigkeiten – etwa zur Identifizierung und Beseitigung von sicherheitsrelevanten Schwachstellen, zur Entwicklung und Implementierung von Sicherheitskonzepten und zur Erkennung und Abwehr von Angriffen auf IT-Systeme – vermittelt. Zudem werden rechtliche und ethische Fragestellungen sowie ausgewählte Themen rund um den Faktor Mensch in der Informationssicherheit behandelt.

Die Bundeswehr fördert zivile Studierende mit einem **Stipendium für den Masterstudiengang Cyber-Sicherheit** an der UniBw M. Voraussetzungen für die Förderung sind ein Studium (Bachelor oder FH) im MINT-Bereich sowie die erfolgreiche Teilnahme an einem Auswahlverfahren des Assessment-Centers für Führungskräfte der Bundeswehr. Neben Studiengängen auf Exzellenzniveau und einer hervorragenden Betreuungsquote durch Lehrpersonal bietet die UniBw M ihren Studierenden eine Vielzahl von Freizeitaktivitäten und Annehmlichkeiten. Günstige Wohnmöglichkeiten in einer der lebenswertesten und vielseitigsten Städte Deutschlands runden die Vorzüge ab.

Weitere Informationen

Master Cyber-Sicherheit:
https://go.unibw.de/mcyb

Stipendium der Bundeswehr:
https://go.unibw.de/stipendium-mcyb

ABB.: CLAUS SCHUNK

PROMOTIONEN UND

Klement Hagenhoff

„A Framework for Controller-Based Multi-Flow Routing in MANETs“

IN MOBILEN Ad-hoc-Netzwerken wird das Routing und die Datenübertragung von den Teilnehmenden übernommen. Aufgrund der Mobilität der Teilnehmenden basieren Rountingentscheidungen oft auf veralteten Verbindungsinformationen. Die Doktorarbeit stellt angepasste und selbst entwickelte Ansätze zur Berechnung langlebiger Routen vor, um verlässliche Datenübertragungen unter Berücksichtigung der bestehenden Übertragungskapazität zu ermöglichen. Darüber hinaus werden Techniken vorgestellt, die mithilfe eines Controllers eine schnelle Erfassung der Netztopologie ermöglichen und Routingtechniken mit aktuellen Verbindungsinformationen versorgen.

Klement Hagenhoff wurde im März 2024 bei Prof. Dr. Gabi Dreo Rodosek promoviert. Derzeit ist er am IT-Dienstleistungszentrum des Freistaats Bayern als IT-Projektkoordinator tätig. ■

Julius Hermelink

„Seitenkanal- und Fehlerangriffe auf moderne gitterbasierte kryptographische Verfahren“

DIE ENTWICKLUNG VON Quantencomputern bedroht die aktuell verwendete asymmetrische Kryptographie – Shors Algoritmus könnte weit verbreitete kryptographische Verfahren brechen. In seiner Arbeit stellt er mehrere Strategien vor, mit denen gitterbasiere Verfahren angegriffen werden können. Seine Angriffsstrategien kombinieren Chosen-Ciphertext Angriffe mit Seitenkanalanalyse und Fehlerangriffen und zielen auf zwei Hauptkomponenten der Decapsulation-Routine ab. Außerdem präsentiert er Techniken, mit denen der geheime Schlüssel aus den in den Angriffen gewonnen Informationen gewonnen werden kann und zeigt, wie diese Methoden mit algebraischen Ansätzen kombiniert werden können.

Julius Hermelink wurde im März 2024 bei Prof. Dr. Gabi Dreo Rodosek promoviert. Derzeit ist er am Max-Planck-Institut für Sicherheit und Privatssphäre in Bochum als Postdoctoral Researcher beschäftigt. ■

ABB.: FI CODE / ANGELIKA WAGENER FOTOGRAFIE (1); PRIVAT (3)

HABILITATION 2024

Daniela Pöhn

„Identity Management Framework“

DER FOKUS DER ARBEIT ist ein ganzheitliches Identitätsmanagement-Framework zur Verbesserung der Interoperabilität und Sicherheit des Identitätsmanagements, bestehend aus Architektur, IT-Sicherheit und Identitätsmanagementprozesse. Das Kernelement der Architektur ist das Referenzmodell für verschiedene Identitätsmanagementprotokolle. Im Bereich der IT-Sicherheit werden Methoden, Gegenmaßnahmen und Schulungsmöglichkeiten vorgeschlagen. Die Identitätsmanagementprozesse umfassen z. B. organisationsübergreifende Prozesse passend zur Architektur und ein Rahmenwerk für kontinuierliche Verbesserungen.

Daniela Pöhn hat sich im Juni 2024 bei Prof. Dr. Wolfgang Hommel habilitiert. Derzeit ist sie an der Professur für IT-Sicherheit von Software und Daten als wissenschaftliche Mitarbeiterin beschäftigt. ■

Nils Rodday

„Improving Internet Routing Security: From Origin Validation to Path Validation“

DAS INTERNET IST ein Netz von Netzen welches als de-facto Standard das Border-Gateway-Protokoll (BGP) zum Austausch von Routing Informationen nutzt. Ursprungsvalidierung bietet die Möglichkeit den korrekten Absender einer Nachricht zu identifizieren, während Pfadvalidierung es ermöglicht, den gesamten Routing Pfad nachzuvollziehen. Die vorliegende Dissertation stellt neue Messmethoden zur Bestimmung des Verbreitungsgrades bestehender Ursprungsvalidierung vor und entwickelt Vorschläge wie Pfadvalidierung als Mittel größerer Sicherheit bestmöglich nutzbar gemacht werden kann.

Nils Rodday wurde im März 2024 bei Prof. Dr. Gabi Dreo Rodosek promoviert. Derzeit ist er als selbstständiger IT-Sicherheitsberater aktiv. ■

Capture the Flag 2024

Spannende Challenges beim zehnten „Capture the Flag“ des FI CODE

Seit 2015 zieht das „Capture the Flag“-Event des Forschungsinstituts CODE jedes Jahr Hacking-Begeisterte an die Universität der Bundeswehr München. In zahlreichen spannenden Challenges stellen die Teilnehmenden ihr Können unter Beweis und messen sich mit Gleichgesinnten. Dabei kommt auch der Spaß nicht zu kurz. Kein Wunder also, dass sich dieses Eventformat einer stetigen Beliebtheit erfreut und 2024 zum insgesamt zehnten Mal stattfand.

NACHDEM CODE IM letzten Jahr bereits sein zehnjähriges Bestehen feierte, stand in diesem Jahr ein weiteres Jubiläum an. Zum insgesamt zehnten Mal wurde das „Capture the Flag“ (CTF) ausgerichtet und ist damit mittlerweile ein fester Bestandteil im Kalender von CODE. Jedes Jahr im November zieht die Veranstaltung zahlreiche Teilnehmende auf den Campus der Universität der Bundeswehr München. So auch in diesem Jahr. Nach einer Qualifizierungsrunde im Oktober, bei der fast 80 Teams teilgenommen haben, konnten sich am Ende die besten 24 von ihnen über eine Einladung zur Hauptrunde in Neubiberg freuen.

Schnelligkeit zahlt sich aus

Bei einem CTF handelt es sich um einen speziellen Cybersicherheits-Wettbewerb, bei dem Teams gegeneinander antreten und verschiedene Aufgaben – oder „Challenges“, wie sie im CTF-Fachjargon bezeichnet werden – gelöst werden müssen. Der Faktor Zeit spielt eine entscheidende Rolle, denn wer die Challenges schnell löst und die Flags sammelt, bekommt mehr Punkte. Wer es sogar schafft, als erstes eine Lösung zu finden, bekommt Extra-Punkte („First Blood“). Ein wertvoller Bonus auf dem hartumkämpften Weg an die Spitze des Scoreboards. Die Challenges sind dabei in verschiedene Kategorien unterteilt (Web Hacking, Forensic, Cryptography, Binary Exploitation, Virtual Reality etc.). Damit keine Langeweile aufkommt stehen die Aufgaben jedes Jahr unter einem anderen Leitthema.

Beim Theme des CTF 2024 orientierte man sich an dem Film „Predator“, einem Actionfilm-Klassiker aus dem Jahr 1987, in dem ein Söldnerkommando im südamerikanischen Dschungel auf einen hochtechnisierten, feindseligen Außerirdischen trifft. Wie in den Vorjahren, schaffte es das Organisations-Team von CODE, Team localos und der xo Dynamics GmbH basierend auf Rahmenhandlung der Filmvorlage ein Event auf die Beine zu stellen, welches zumindest in München und Umgebung seinesgleichen sucht.

Bei der VR-Challenge mussten die Teilnehmenden den Predators entkommen und dabei eine Reihe von Rätseln lösen.

ALLE ABB.: FI CODE / B. BELLGRAU

Herausfordernde Challenges

So gab es beispielsweise eine Virtual Reality Challenge, bei der die Spieler in einem Urwald wiederfinden und dort von Predators „gejagt“ werden. Um zu entkommen, galt es in der ersten Phase der Challenge zunächst möglichst schnell eine Reihe von Logik-Rätseln zu lösen und einen sicheren Unterschlupf zu erreichen. Dort fanden die Spieler eine Art Computer Terminal der Predators vor, über welches durch Manipulation diverser mechanischer Komponenten ein Selbstzerstörungsbefehl für die Predators erzeugt werden musste. Nach der Zerstörung der Predators konnte der Weg durch den virtuellen Urwald fortgesetzt und die Flag gefunden werden. In einer weiteren Challenge aus der Kategorie „Cryptography“ war eine Verschlüsselung zu brechen, die auf der Predator-Sprache „Yautja“ basiert. Die Zeichen des Yautja-Alphabets bestehen aus Strichen, welche um zwei Mittelpunkte pro Zeichen in verschiedenen Winkeln angeordnet sind. Die Verschlüsselung bestand in der Transposition der eingegebenen zeichen. Zudem änderte sich der verwendete Schlüssel mit jeder Eingabe nach einem Muster, welches in Form eines Initialisierungsvektors einzugeben war. Den Spieler wurde dabei eine „Verschlüsselungsmaschine“ bereitgestellt, die als eine Art „Orakel“ bei der Lösung der Challenge unterstützen sollte. War der Code geknackt, konnte eine verschlüsselte Nachricht (Chiffrat) gelesen und die Flag geholt werden.

Spaß und Wettbewerb

Nachdem die Veranstaltung am Freitagabend pünktlich um 18 Uhr gestartet wurde, lieferten sich die 24 Teams aus dem In- und Ausland die ganze Nacht hindurch einen spannenden Wettkampf, der den Teilnehmenden einiges abverlangte. Nach insgesamt 18 Stunden stand dann am Samstagmittag das Siegerteam fest. Mit 1524 Punkten konnte sich das Team „Winnie the pwnd“ behaupten und die Teams „SIGCONT“ (1356 Punkte) und „Nop(e)“ auf die Plätze 2 und 3 verweisen. Bei der Siegerehrung gratulierte CODEs Leitender Direktor Prof. Dr. Wolfgang Hommel den drei bestplatzierten Teams und überreichte die Zertifikate. Auch wenn sich am Ende nur die Sieger auf der „Flag of Fame“ mit ihren Unterschriften verewigen durften, als Gewinner können sich diesem Tag alle Teilnehmenden fühlen. Sind es doch vor allem der Spaß sowie das Austesten und Ausbauen der eigenen Fähigkeiten, die bei einem derartigen Veranstaltungsformat im Vordergrund stehen. ■

Mehr Informationen:

www.unibw.de/code/events/ctf

ctf@unibw.de

ABB.: ADOBE STOCK / ADRIAN GROSU

Addendum

Publikationen, Aktivitäten und Organisation

Prof. Dr. Harald Baier

Digitale Forensik

PUBLIKATIONEN

DEMMEL, M., GÖBEL, T., GONÇALVES, P., BAIER, H.: Data Synthesis is Going Mobile – On Community-driven Dataset Generation for Android Devices. Digital Threats: Research and Practice, 2024, doi: 10.1145/3688807.

DEUTSCHMANN, M., BAIER, H.: Flash-Dateisysteme im Kontext der digitalen Forensik. In: Polizei-Informatik 2024, D. Honekamp Wilfried Labudde, Ed., Remscheid: Rediroma-Verlag, 2024, pp. 115–126.

DEUTSCHMANN, M., BAIER, H.: Ubi est indicium? On forensic analysis of the UBI file system. Forensic Science International: Digital Investigation, vol. 48, no. Supplement, DFRWS EU 2024 – Selected Papers from the 11th Annual Digital Forensics Research Conference Europe, p. 301689, 2024, [Online]. doi: 10.1016/j.fsidi.2023.301689.

GÖBEL, T., BAIER, H., TÜRR, J.: Generating Usable and Assessable Datasets Containing Anti-Forensic Traces at the Filesystem Level. In: Advances in Digital Forensics XX : 20th IFIP WG 11.9 International Conference, New Delhi, India, January 4–5, 2024, Revised Selected Papers, S. Kurkowski Elizabeth Shenoi, Ed., in IFIP Advances in Information and Communication Technology, vol. 724. Cham: Springer, 2024.

GÖBEL, T., BAIER, H., WOLF, D.: Scenario-based Data Set Generation for Use in Digital Forensics: A Case Study: 4. International Workshop on Digital Forensics (IWDF4). In: INFORMATIK 2024: Lock in or log out? Wie digitale Souveränität gelingt, Gesellschaft für Informatik e.V., Ed., in GI-Edition Lecture Notes in Informatics (LNI), vol. P352. Bonn; Berlin: Gesellschaft für Informatik, 2024, pp. 355–370. doi: 10.18420/inf2024_25.

KLIER, S., BAIER, H.: Beware of the Rabbit Hole – A Digital Forensic Case Study of DIY Drones. In: Secure IT Systems: NordSec 2024, Horn Iwaya, Leonardo; Kamm, Liina; Martucci, Leonardo; Pulls, Tobias, Ed., in Lecture Notes in Computer Science, vol. 15396. Cham: Springer, 2024, pp. 325–344. doi: 10.1007/978-3-031-79007-2_17.

KLIER, S., BAIER, H.: Scalable Image Clustering to screen for self-produced CSAM. EAI Endorsed Transactions on Internet of Things, vol. 10, pp. 1–14, 2024, doi: 10.4108/eetiot.6631.

MUNDT, M.: Die Synergie von GIS und KI. In: Polizei-Informatik 2024, D. Honekamp Wilfried Labudde, Ed., Remscheid: Rediroma-Verlag, 2024, pp. 20–29.

MUNDT, M., BAIER, H.: Adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik. Linux-Magazin, no. 2, 2024, [Online]. Available: https://www.linux-magazin.de/ausgaben/2024/02/bedrohungen-erkennen/.

MUNDT, M., BAIER, H.: Gib dem Dino Futter – adaptive Detektion von Bedrohungen in KRITIS-Netzwerken mittels Open-Source-Forensik. In: 31. DFN-Konferenz „Sicherheit in vernetzten Systemen“, DFN-Cert, Ed., Springer, 2024.

MUNDT, M., BAIER, H., RAAB-DÜSTERHÖFT, A.: Towards Reducing Business-Risk of Data Theft Implementing Automated Simulation Procedures of Evil Data Exfiltration. In: ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security, New York, NY: Association for Computing Machinery, 2024, pp. 1–12. doi: 10.1145/3664476.3664483.

RZEPKA, L., OTTMANN, J., FREILING, F., BAIER, H.: Causal Inconsistencies Are Normal in Windows Memory Dumps (too). In: Digital Threats: Research and Practice, ACM, 2024. [Online]. doi: 10.1145/3680293.

TWENNING, L., BAIER, H.: Towards arbitrating in a dispute – on responsible usage of client-side perceptual hashing against illegal content distribution. In: EICC '24: Proceedings of the 2024 European Interdisciplinary Cybersecurity Conference, K. S. Li Shujun Coopamootoo, Ed., New York: Association for Computing Machinery, 2024, pp. 105–114. doi: 10.1145/3655693.3655712.

WOLF, D., GÖBEL, T., BAIER, H.: Hypervisor-based data synthesis: On its potential to tackle the curse of client-side agent remnants in forensic image generation. Forensic Science International: Digital Investigation, vol. 48, no. Supplement DFRWS EU 2024 – Selected Papers from the 11th Annual Digital Forensics Research Conference Europe, p. 301690, 2024, doi: 10.1016/j.fsidi.2023.301690.

LEHRE

1162	**Erweiterte Digitale Forensik (WT)**
3824	**Digitale Forensik (HT)**
5001/1009	**Seminar Digitale Forensik (WT + FT)**
5501/1009	**Seminar Forensische Methoden der Informatik (HT)**
5505	**IT-Forensik (FT)**

WEITERE FUNKTIONEN

- Gutachter für Journal of Digital Investigation und Computers & Security
- Conference Co-Chair of 13th International Conference on IT Security Incident Management & IT Forensics
- Gutachter für IFIP WG11.9 International Conference on Digital Forensics 2024
- Gutachter für DFRWS EU 2024
- Gutachter für GI Sicherheit
- Gutachter für International Conference on IT Security Incident Management & IT Forensics 2024
- Gutachter für DFRWS APAC 2024
- Gutachter für German Cybersecurity PhD Award

Prof. Dr. Stefan Brunthaler

Sichere Software-Entwicklung

PUBLIKATIONEN

BERLAKOVICH, F., BRUNTHALER, S.: Cross Module Quickening – The Curious Case of C Extensions. In: Proceedings of the 38th European Conference on Object-Oriented Programming.

BERNAD, M., BRUNTHALER, S.: HOBBIT: Hashed OBject Based InTegrity. In: Proceedings of the 38th European Conference on Object-Oriented Programming.

MECHELINCK, R., DORFMEISTER, D., FISCHER, B., VOLCKAERT, S., BRUNTHALER, S.: GlueZilla: Efficient and Scalable Software to Hardware Binding using Rowhammer. In: Proceedings of the 21st Conference on Detection of Intrusions and Malware & Vulnerability Assessment.

SARAFOV, V., MARKVICA, D., BERLAKOVICH, F., BERNAD, M., BRUNTHALER, S.: Understanding and Improving Coverage Tracking with AFL++ (Registered Report). In: Proceedings of the 3rd International Fuzzing Workshop.

FORSCHUNGSPROJEKTE

APERITIF – Analysis Pipeline for Effective Vulnerablity Identification Through Fuzzing

Im Rahmen des Projekts APERITIF erforscht µCSRL gemeinsam mit der Forschungsgruppe PATCH von Prof. Dr. Kinder neue, hochskalierende und automatische Schwachstellenanalyse-Verfahren durch Fuzzing auf Datacenter-Ebene. Unterstützt durch einen eigenen Cluster analysiert das Team neue Möglichkeiten zur Parallelisierung und Optimierung von einzelnen Fuzzern.

Gefördert durch: BMVg/BAAINBw
Laufzeit: 2021–2025

DEMISEC – Detecting Malicious Implants in Source Code

Moderne Software enthält eine Reihe von externen Open-Source-Komponenten, die von vielen verschiedenen Personen entwickelt wurden. Beinhaltet auch nur eine dieser Komponenten potenziell bösartigen Code, ist die Sicherheit des gesamten Produkts gefährdet. Im Projekt DEMISEC wird untersucht, wie sich böswillige Änderungen an Quellcode erkennen lassen, bevor sie den Entwicklungsprozess unterwandern können

Gefördert durch: BMVg/BAAINBw
Laufzeit: 2021–2025

DEPS – Dependable Production Environments with Software Security

Das Projekt DEPS erforscht neuartige Techniken, um Software effizient an Hardware zu binden. Die dadurch geschützten Systeme sind zum einen deutlich resilienter gegenüber regulären Angriffen und erschweren zum anderen gängige Reverse-Engineering-Techniken, um geistigen Diebstahl entweder ganz zu verhindern oder durch Kostenexplosionen unökonomisch werden zu lassen.

Gefördert durch: Österreichische Forschungsförderungsgesellschaft (FFG), Software Competence Center Hagenberg
Laufzeit: 2022–2025

LEHRE

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

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

1010 **Maschinennahe Programmierung (WT)**

3647 **Compilerbau (HT + WT)**

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

MESSEN, TAGUNGEN, SEMINARE

- 33rd ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2024), Wien, Österreich (Session Chair und Panel Member beim Doctoral Symposium)
- Kolloquium mit Prof. Dr. Shriram Krishnamurthi, Brown University, RI, USA
- 38th European Conference on Object-Oriented Programming (ECOOP 2024), Wien, Österreich
- 3rd International Fuzzing Workshop (FUZZING) 2024, Wien, Österreich
- 40th Workshop der GI-Fachgruppe Programmiersprachen und Rechenkonzepte, Bad Honnef
- DWT SWG Konferenz „Software Defined Defense“, Bonn

PREISE UND AUSZEICHNUNGEN

- Distinguished Reviewer Award, IEEE SecDev 2024

WEITERE FUNKTIONEN

- Chair Area Board „System Security“ of the Journal of Systems Research (JSYS)

Mitglied des Programmkomitees

- Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA 2024), Pasadena, CA, USA

Prof. Dr. Michaela Geierhos

Data Science

PUBLIKATIONEN

BÄUMER, F. S., SCHULTENKÄMPER, S., GEIERHOS, M., LEE, Y.S. Mirroring Privacy Risks with Digital Twins: When Pieces of Personal Data Suddenly Fit Together. SN Computer Science Vol. 5, 1109. 2024. https://doi.org/10.1007/s42979-024-03413-z

CIMITAN, A., ALVES PINTO, A., GEIERHOS, M.: Curation of Benchmark Templates for Measuring Gender Bias in Named Entity Recognition Models. In: Calzolari, N., Kan, M.-Y., Hoste, V., Lenci, A., Sakti, S., Xue, N. (Hrsg.). Proceedings of the 2024 Joint International Conference on Computational Linguistics, Language Resources and Evaluation (LREC-COLING 2024). ELRA and ICCL. 2024. S. 4238–4246.

GEIERHOS, M.: Täuschend echt? Fake News! Identifikation von Desinformationskampagnen in Social Media. prmagazin Vol. 54. No. 2. Medienhaus Rommerskirchen GmbH. 2024. S. E1–E7.

HENNEN, M., BABL, F., GEIERHOS, M.: ITER: Iterative Transformer-based Entity Recognition and Relation Extraction. In: Al-Onaizan, Y., Bansal, M., Chen, Y.-N. (Hrsg.). Findings of the Association for Computational Linguistics: EMNLP 2024. Association for Computational Linguistics. 2024. S. 11209–11223.

MAORO, F., GEIERHOS, M.: Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen: Wie kann Künstliche Intelligenz in der Polizeiarbeit unterstützend eingesetzt werden und dabei sowohl fair als auch nachvollziehbar sein? Kongress KI@HSBI2023: Solutions im Fokus. Schriftenreihe des Institutes for Data Science Solutions 1. 2024. S. 22–23.

MAORO, F., GEIERHOS, M.: FICODE at GermEval 2024 GerMS-Detect closed ST1 & ST2: Ensemble- and Transformer-Based Detection of Sexism and Misogyny in German Texts. In: Krenn, B., Petrak, J., Gross, S. (Hrsg.). Proceedings of GermEval 2024 Task 1 GerMS-Detect Workshop on Sexism Detection in German Online News Fora (GerMS-Detect 2024). Association for Computational Linguistics. 2024. S. 21–25.

MAORO, F., VEHMEYER, B., GEIERHOS, M.: Leveraging Semantic Search and LLMs for Domain-Adaptive Information Retrieval. In: Lopata, A., Gudoniene, D., Butkiene, R. (Hrsg.). Information and Software Technologies. 29th International Conference ICIST. Springer Nature Switzerland. 2024. S.148–159.

MURAUER, J., STAUDACHER, K., GEHRKE, W., GEIERHOS, M.: Towards Masked Language Modeling in Quantum Natural Language Processing. 21st International Conference on Quantum Physics and Logic (QPL). 2024.

PRITZKAU, A., WALDMÜLLER, J., BLANC, O., GEIERHOS, M., SCHADE, U.: Current language models' poor performance on pragmatic aspects of natural language. In: Ghosh, K., Mandl, T., Majumder, P., Mitra, M. (Hrsg.). Working Notes of FIRE 2023 - Forum for Information Retrieval Evaluation (FIRE-WN 2023). 2024. S. 159–169.

RÖSCH, P. J., OSWALD, N., GEIERHOS, M. LIBOVICKY, J.: Enhancing Conceptual Understanding in Multimodal Constrastive Learning through Hard Negative Samples. In: Gu, J., Fu, T-J., Hudson, D., Celikyilmaz, A., Wang, W. (Hrsg.). Proceedings of the 3rd Workshop on Advances in Language and Vision Research (ALVR). Association for Computational Linguistics. 2024. S. 102–115.

SCHULTENKÄMPER, S., BÄUMER, F. S., BELLGRAU, B., LEE, Y. S., GEIERHOS, M.: From Digital Tracks to Digital Twins: On the Path to Cross-Platform Profile Linking. In: Sales, T. P., de Kinderen, S., Proper, H. A.., Pufahl, L., Karastoyanova, D., van Sinderen, M. (Hrsg.). Enterprise Design, Operations, and Computing. EDOC 2023 Workshops: IDAMS, iRESEARCH, MIDas4CS, SoEA4EE, EDOC 2023 Workshops. EDOC 2023. Lecture Notes in Business Information Processing Vol. 498. Springer Nature Switzerland. 2024. S. 158–171.

SOARES DE SOUZA, A., MEIßNER, A., GEIERHOS, M. (2025). Combining Frequency-Based Smoothing and Salient Masking for Performant and Imperceptible Adversarial Samples. In: Antonacopoulos, A., Chaudhuri, S., Chellappa, R., Liu, CL., Bhattacharya, S., Pal, U. (eds) Pattern Recognition. ICPR 2024. Lecture Notes in Computer Science, Vol. 15322. Springer, Cham. doi: 10.1007/978-3-031-78312-8_19.

WINKEL, F., GEIERHOS, M., FINK, J.: Evaluating Embedding Models for Retrieving ESG Information from Annual Business Reports. ICIS 2024 Proceedings. Association for Information Systems (AIS). 2024.

FORSCHUNGSPROJEKTE

KIMONO – Kampagnenidentifikation, -monitoring und -klassifikation mittels Methoden des Social Media Mining zur Integration in ein KI-basiertes Frühwarnsystem

Ziel des KIMONO-Projekts ist die Erkennung und Modellierung von kurz- und langfristigen Desinformations- und Beeinflussungskampagnen in Sozialen Medien wie X (ehemals Twitter) und Facebook. Insbesondere Kampagnen, die von staatlichen Akteuren vorangetrieben werden, stehen im Fokus.

Gefördert durch: BMVg/BAAINBw
Laufzeit: 09/2021–12/2024

MuQuaNet – Quanten-Internet im Großraum München
TP: „Authority-Dependent Risk Identification and Analysis in online Networks“

Ziel ist es, ausgewählte Apps zu überwachen und deren gesammelte Daten zu analysieren, mit Social-Media-Profilen zu korrelieren und Personennetzwerke zu bilden, um potenzielle Ziele zu identifizieren und ihr Gefährdungspotenzial aufgrund der gegebenen Datenlage einzustufen.

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 10/2020–12/2026

NAWI – News-Artikel und Wissen

Das Projekt NAWI beschäftigt sich mit der Wissensgewinnung und -modellierung aus News-Artikeln.

Laufzeit: 12/2021–11/2026

Synthetische Daten-Generierung und -Detektion

Das Projekt beschäftigt sich mit der Erforschung von Methoden zur Erzeugung und Detektion von synthetisch erstelltem bzw. manipuliertem Datenmaterial mithilfe Künstlicher Intelligenz. In diesem Kontext sollen Verfahren entwickelt werden, die in der Lage sind, synthetisch erstellte und manipulierte Bilder, Videos und Audiodateien zuverlässig zu erkennen.

Gefördert durch: Zentrale Stelle für Informationstechnik im Sicherheitsbereich
Laufzeit: 06/2022–11/2025

TACR – Technische Adaption von Cyber-Ranges für die militärische Nutzung

In der F&T Studie Technische Adaption von Cyber-Ranges für die militärische Nutzung wird untersucht, wie der Bedarf von Dienststellen in der Bundeswehr an Trainingsanlagen für das digitale Umfeld, sogenannten Cyber Ranges, gedeckt werden kann. Dazu werden verschiedene Use-Cases und Cyber-Range-Produkte geprüft und evaluiert. Zusätzlich werden ebenso Szenare im militärischen Kontext entwickelt und in einer Übung praktisch geprobt.

Gefördert durch: Wehrtechnische Dienststelle für Informationstechnologie und Elektronik in der Bundeswehr (WTD81)
Laufzeit: 10/2023–06/2025

VIKING – Vertrauenswürdige Künstliche Intelligenz für polizeiliche Anwendungen

Das Teilprojekt „Erklärbarkeit vertrauenswürdiger KI-Sprachmodelle für den transparenten Gebrauch bei Sicherheitsbehörden zur Textklassifikation“ widmet sich im Rahmen des Verbundprojekts VIKING der Erforschung vertrauenswürdiger KI-Methoden zur Textklassifikation.

Gefördert durch: Bundesministerium für Bildung und Forschung (BMBF)
Laufzeit: 01/2022–03/2025

LEHRE

1144 **Knowledge Discovery in Big Data (FT + HT)**

3850 **Natural Language Processing (WT + FT)**

3851 **Information Retrieval (WT)**

3852 **Anwendungsgebiete der Data Science (HT + WT + FT)**

MESSEN, TAGUNGEN, SEMINARE

- DeepLearn 2024 (Universität Maia, Portugal)
- KI@BW 2024 (HSU, Hamburg)

PREISE UND AUSZEICHNUNGEN

Studienpreis der AFCEA Bonn e.V.
Hannes Jost Ludwig erreichte den ersten Platz für seine Masterarbeit „An Approach to Creating Adversarial Samples“.

WEITERE FUNKTIONEN

- Mitglied im Fakultätsrat INF (bis 09/2024)
- Mitglied in der Studiengangskommission Master Cyber-Sicherheit
- Mitglied im Beirat „Deutsche Biographie“ der Historischen Kommission bei der BAdW (bis 10/2024)
- Projektleitung der „Deutschen Biographie“ der Historischen Kommission bei der BAdW (seit 10/2024)
- Gutachterin für die Europäische Kommission
- Gutachterin für VDI/VDE Innovation + Technik

Mitglied im Programmkomitee

- NAACL 2024 – Annual Conference of the North American Chapter of the Association for Computational Linguistics
- LREC-COLING 2024 – Joint International Conference on Computational Linguistics, Language Resources and Evaluation
- PATTERNS 2024 – International Conference on Pervasive Patterns and Applications
- EMNLP 2024 – Conference on Empirical Methods in Natural Language Processing
- WiNLP 2024 – Widening Natural Language Processing

Prof. Dr. Marta Gomez-Barrero

BioML: Biometrics and Machine Learning Lab

LEHRE

10112 **Einführung in Datenbanken (FT)**

42121 **Deep Learning (FT)**

42122 **Selected Topics in Deep Learning for IT-Security (FT)**

42111 **Biometric Recognition (HT)**

42112 **Selected topics in Biometric Recognition (HT)**

MESSEN, TAGUNGEN, SEMINARE

- IEEE Int. Conference of the Biometrics Special Interest Group (BIOSIG) – General Chair
- IEEE Int. Joint Conference on Biometrics (IJCB) – Program Co-Chair
- IEEE Int. Workshop on Biometrics and Forensics (WIFS) – Special Session Chair Co-Chair

WEITERE FUNKTIONEN

- General Chair der International Conference of the Biometrics Special Interest Group (BIOSIG)
- Vorsitzende der BIOSIG Special Interest Group der Gesellschaft für Informatik (GI)
- Stellvertretende Vorsitzende der European Association for Biometrics (EAB)
- Mitglied des IARP TC4 Conference Committee, des IEEE Biometrics Council Security and Privacy Technical Committee, und des IEEE Information and Forensics Technical Committee
- Delegierte des Deutschen Instituts für Normung (DIN) in ISO/IEC SC37 JTC1 SC37 für Biometrie
- Co-Affiliation Norwegian University of Science and Technology (NTNU)

Prof. Dr. Wolfgang Hommel

IT-Sicherheit von Software und Daten

PUBLIKATIONEN

BIERWIRTH, T., PFÜTZNER, S., SCHOPP, MA., STEININGER, C.: Design and Evaluation of Advanced Persistent Threat Scenarios for Cyber Ranges. IEEE Access. Vol. 12. 2024. pp. 72458–72472.

FRANK, A., STEINKE, M., HOMMEL, W.: Lowcaf: A Low-Code Protocol Analysis Framework. In: 20th International Conference on Network and Service Management (CNSM). Prague, Czech Republic: IFIP, IEEE, 2024.

FRIES, I., GRABATIN, M., HOFMEIER, M.: Sovereign by Design: The LIONS Approach to Digital Sovereignty. Logos Verlag Berlin, 2024 – ISBN 978-3-8325-5834-5.

GEISLER, M., PÖHN, D., HOMMEL, W.: Hooked: A Real-World Study on QR Code Phishing. DFN-Konferenz Sicherheit in vernetzten Systemen (31., 2024, Hamburg). 2024.

HOFMEIER, M., GRABATIN, M., HOMMEL, W.: System Design for Electronic Signatures within Supply Chains using Blockchain Technology and Self-Sovereign Identities. In: Sovereign by Design: The LIONS Approach to Digital Sovereignty (2024), pp. 143–160.

HOFMEIER, M., PÖHN, D., HOMMEL, W.: DistIN: Analysis and Validation of a Concept and Protocol for Distributed Identity Information Networks. ARES '24: Proceedings of the 19th International Conference on Availability, Reliability and Security. New York, NY, USA. Association for Computing Machinery. 2024.

LESCHKE, N., PÖHN, D., PALLAS, F.: How to Drill into Silos: Creating a Free-to-Use Dataset of Data Subject Access Packages. In: Jensen, Meiko; Laurasoux, Cédric; Rannenberg, Kai (Ed.). Privacy Technologies and Policy. 12th Annual Privacy Forum, APF 2024, Karlstad, Sweden, September 4–5, 2024, Proceedings. Cham. Springer. 2024.

MAUL, D., STIEMERT, L., PÖHN, D.: Evaluation of Basic Methods to Bypass Recent Antivirus Systems in Windows Environments. DFN-Konferenz Sicherheit in vernetzten Systemen (31., 2024, Hamburg). 2024.

PÖHN, D., GRABATIN, M., HOMMEL, W.: Analyzing the Threats to Blockchain-Based Self-Sovereign Identities by Conducting a Literature Survey. Applied Sciences. Vol. 14. 2024. No. 1.

PÖHN, D., GRUSCHKA, N.: Past and Present: A Case Study of Twitter's Responses to GDPR Data Requests. In: Rannenberg, Kai; Drogkaris, Prokopios; Lauradoux, Cédric (Ed.). Privacy Technologies and Policy. 11th Annual Privacy Forum, APF 2023, Lyon, France, June 1–2, 2023, Proceedings. Cham. Springer. 2024. pp. 57–84. Lecture Notes in Computer Science.

PÖHN, D., HOMMEL, W.: Digital Skills and Technology to Empower Women. In: Krishnan, Saravanan; Anand, A. Jose; Kumar, Raghvendra (Ed.). Sustainable Development Goals. Technologies and Opportunities. Boca Raton. CRC Press. 2024.

FORSCHUNGSPROJEKTE

6G-life

Im Projekt 6G-life werden mit einem holistischen Ansatz innovative Konzepte im Bereich skalierbare Kommunikation, neuartige Methoden, flexible Softwarekonzepte und adaptive Hardware erforscht, die den Grundgedanken der Mensch-Maschine-Kollaboration unterstützen. In allen Forschungsfeldern werden die Anforderungen an Latenz, Resilienz, Sicherheit und Nachhaltigkeit als Querschnittsthemen stets parallel bearbeitet.

Gefördert durch: BMBF (Unterauftrag der TU München)
Laufzeit: 12/2022–08/2025

ACSE LTE – Airborne Cybersecurity Enhancement Long Term Evolution

Airborne Cybersecurity Enhancement (ACSE) LTE (Long Term Evolution) ist das Folgeprojekt des Ende 2023 abgeschlossenen ACSE-Projekts. Wie sein Vorgänger ist ACSE LTE Teil der Forschungskooperation zwischen dem FI CODE und Airbus Defence and Space. Der Fokus dieses Projekts liegt auf der Anwendung der im Vorgänger gewonnen Erkenntnisse zu sicherer Flugzeugkommunikation für taktische Datenlinks.

Gefördert durch: Airbus Defence and Space
Laufzeit: 01/2024–12/2025

Anwendungsorientierte Technologiepotentiale für Cyber/IT

Das Ziel der F&T-Maßnahme „Anwendungsorientierte Technologiepotentiale für Cyber/IT“ ist es, Forschungsideen und Innovationen zu identifizieren, divergierende Interessen, Ziele und Methoden im Bereich der Forschung von Cybersicherheit und Cyberverteidigung zusammenzuführen sowie die Sektoren-übergreifende Kooperation im Bereich Technologiemonitoring im Cyber-Cluster voranzutreiben.

Gefördert durch: Wehrtechnische Dienststelle für Informationstechnologie und Elektronik in der Bundeswehr (WTD81)
Laufzeit: 07/2024–12/2026

DEFINE – DC-Netze für eine sichere Energieversorgung

Moderne Stromnetze werden u. a. aus regenerativen Stromquellen wie Solar- oder Windenergie gespeist und bedienen immer anspruchsvollere Bedarfe wie die Elektromobilität. Gleichstromverteilnetze versprechen hier gegenüber herkömmlichen AC-Netzen einen Vorteil in Effizienz und Kontrolle. Das FI CODE forscht an gehärteten IT- und geeigneten Überwachungs- und Steuerungslösungen für diese Energieversorgungsnetze der Zukunft.

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 01/2021–12/2026

LIONS – Ledger Innovation and Operation Network for Sovereignty

Das Projekt LIONS baut eine Forschungsplattform zur Erhöhung von Resilienz und Digitaler Souveränität in der Digitalisierung mittels Distributed-Ledger-Technologien auf. Als Teil des interdisziplinären Forschungsprojekts steht für die Forschungsgruppe dabei das Thema Self-Sovereign Identity Management und die technische Unterstützung der Projektpartner im Mittelpunkt.

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 01/2021–12/2026

ROLORAN – Resilient Operation of LoRa Networks

Dieses Projekt evaluiert die Nutzbarkeit der weitreichenden, energieeffizienten und robusten Funktechnologie LoRaWAN. Neben Softwareanalysen zur Protokollhärtung und Messreihen zu Sendereichweite, Stör- und Ortbarkeit werden prototypische Einzelgeräte und Gesamtsysteme entwickelt. Augenmerk liegt hierbei auf Kooperationen zu den Szenarien Sturzflutfrühwarnung und Krisenkommunikation.

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 01/2021–12/2026

TACR - Technische Adaption von Cyber-Ranges für die militärische Nutzung

In der F&T Studie Technische Adaption von Cyber-Ranges für die militärische Nutzung wird untersucht, wie der Bedarf von Dienststellen in der Bundeswehr an Trainingsanlagen für das digitale Umfeld, sogenannten Cyber Ranges, gedeckt werden kann. Dazu werden verschiedene Use-Cases und Cyber-Range-Produkte geprüft und evaluiert. Zusätzlich werden ebenso Szenare im militärischen Kontext entwickelt und in einer Übung praktisch geprobt.

Gefördert durch: Wehrtechnische Dienststelle für Informationstechnologie und Elektronik in der Bundeswehr (WTD81)
Laufzeit: 10/2023–06/2025

LEHRVERANSTALTUNGEN

1006 **Einführung in die Informatik 1 (HT)**

1007 **Einführung in die Informatik 2 (WT)**

3459 **Ausgewählte Kapitel der IT-Sicherheit (WT+FT)**

5501 **Seminar Anwendungs- und Softwaresicherheit (FT)**

5501 **Seminar Informationssicherheitsmanagement (HT)**

5507 **Sichere vernetzte Anwendungen (FT)**

5508 **Sicherheitsmanagement (FT)**

MESSEN, TAGUNGEN, SEMINARE

- Workshop Chair von EDId @ ARES 2024 (Dr. Daniela Pöhn)

PREISE UND AUSZEICHNUNGEN

ITIS e.V. Forschungspreis
Auszeichnung auf dem Dies Academicus für Dr. Michael Grabatin mit der Dissertation "Architecture and Tools for Self-sovereign Identity Management on Distributed Ledgers".

WEITERE FUNKTIONEN

- Dekan der Fakultät für Informatik
- Prüfungsausschuss Master of Intelligence & Security Studies
- Mitglied im Betriebsausschuss des Deutschen Forschungsnetzes
- Gutachter im Forschungsförderprogramm „Sparkling Science 2.0“

Mitglied des Programmkomitees

- IEEE/IFIP International Symposium on Integrated Network Management
- IEEE/IFIP Network Operations and Management Symposium
- IEEE International Conference on Communications
- DFN-Konferenz Sicherheit in vernetzten Systemen
- Workshop on Avionics Systems and Software Engineering
- International Workshop on Frontiers in Availability, Reliability and Security
- International Journal of Critical Infrastructure Protection
- International Journal of Electronic Government
- International Journal of Innovation and Technology Management

Prof. Dr. Ulrike Lechner

Forschungsgruppe Wirtschaftsinformatik

PUBLIKATIONEN

BECHARA, J., LECHNER, U. (2024). Digital sovereignty and open-source software–A discussion paper. In: International Conference on Innovations for Community Services (pp. 397–407). Springer Nature Switzerland Cham.

ESPINHA GASIBA, T., IOSIF, A.-C., KESSBA, I., AMBURI, S., LECHNER, U., PINTO-ALBUQUERQUE, M. (2024). May the source be with you: On ChatGPT, cybersecurity, and secure coding. Information, 15(9), 572.

FAHRNBERGER, G., SCHAUER, S., LECHNER, U. (2024). Check for scared? Prepared? Toward a ransomware incident response scenario 9. In: Innovations for Community Services: 24th International Conference, I4CS 2024, Maastricht, The Netherlands, June 12–14, 2024, Proceedings (Vol. 2109, p. 289). Springer Nature.

FRIES, I., GRABATIN, M., HOFMEIER, M. (eds.) (2024). Sovereign by Design. The LIONS Approach to Digital Sovereignty. Logos Verlag Berlin.

GREINER, M., SEIDENFAD, K., LANGEWISCH, C., HOFMANN, A., LECHNER, U. (2024). The digital product passport: Enabling interoperable information flows through blockchain consortia for sustainability. In: International Conference on Innovations for Community Services (pp. 377–396). Springer Nature Switzerland Cham.

GREINER, M., STRUSSENBERG, J., SEILER, A., HOFBAUER, S., SCHUSTER, M., STANO, D., FAHRNBERGER, G., SCHAUER, S., LECHNER, U. (2024). Scared? Prepared? Toward a ransomware incident response scenario. In: International Conference on Innovations for Community Services (pp. 289–320). Springer Nature Switzerland Cham.

GREINER, M., ZEISS, C., NEIS, N., SEIDENFAD, K., LECHNER, U., WINKELMANN, A. (2024). Governance Requirements for Decentralized Blockchain-based Supply Chain Consortia. Wirtschaftsinformatik 2024 Proceedings. 58. https://aisel.aisnet.org/wi2024/58.

IOSIF, A.-C., ESPINHA GASIBA, T., LECHNER, U., PINTO-ALBUQUERQUE, M. (2024). To kill a mocking bug: Open source repo mining of security patches for programming education. In: 5th International Computer Programming Education Conference (ICPEC 2024) (pp. 16:1–16:12). Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

IOSIF, A. C., LECHNER, U., PINTO-ALBUQUERQUE, M., ESPINHA GASIBA, T. (2024). Code review for cybersecurity in the industry: Insights from gameplay analytics. In: 5th International Computer Programming Education Conference (ICPEC 2024) (pp. 14:1–14:11). Schloss Dagstuhl–Leibniz-Zentrum für Informatik.

IOSIF, A.-C., LECHNER, U., PINTO-ALBUQUERQUE, M., ESPINHA GASIBA, T. (2024). Cybersecurity awareness training for industrial software developers via a serious game for code review.

IOSIF, A.-C., LECHNER, U., PINTO-ALBUQUERQUE, M., GASIBA, T. E. (2024). Serious game for industrial cybersecurity: Experiential learning through code review. In: 2024 36th International Conference on Software Engineering Education and Training (CSEE&T) (pp. 1–6). IEEE

KLARE, M., LECHNER, U. (2024). A reference model to strengthen digital sovereignty in companies. The 15th International Conference on Software Business (ICSOB 2024), November 18–20, 204, Utrecht, the Netherlands.

LIONS Monitor. Individuals Perspectives on Information Technology and E-Signatures. Universität der Bundeswehr München, 2024.

MÜLLER, K., KOLB, L., LECHNER, U., BODENDORF, F. (2024). Ethical AI principles for enterprise collaboration in federated learning networks.

REINHARD, P., NEIS, N., KOLB, L., WISCHER, D., LI, M. M., WINKELMANN, A., TEUTEBERG, F., LECHNER, U., LEIMEISTER, J. M. (2024). Augmenting frontline service employee onboarding via hybrid intelligence: Examining the effects of different degrees of human-GenAI interaction. In International Conference on Design Science Research in Information Systems and Technology (pp. 384–397).

REINHARD, P., NEIS, N., KOLB, L., WISCHER, D., WINKELMANN, A., TEUTEBERG, F., LECHNER, U. (2024). Check for updates: Augmenting frontline service employee onboarding via hybrid intelligence: Examining the effects of different degrees. In: Design Science Research for a Resilient Future: 19th International Conference on Design Science Research in Information Systems and Technology, DESRIST 2024, Trollhättan, Sweden, June 3–5, 2024, Proceedings (Vol. 14621, p. 384). Springer Nature.

SEIDENFAD, K., GREINER, M., BIERMANN, J., DANNENBERG, D., KEINEKE, S., LECHNER, U. (2024). Check for greenhouse gas emissions as commons: A community service approach with blockchain on the edge. In: Innovations for Community Services: 24th International Conference, I4CS 2024, Maastricht, The Netherlands, June 12–14, 2024, Proceedings (Vol. 2109, p. 351). Springer Nature.

SEIDENFAD, K., GREINER, M., BIERMANN, J., DANNENBERG, D., KEINEKE, S., LECHNER, U. (2024). Greenhouse gas emissions as commons: A community service approach with blockchain on the edge. In: International Conference on Innovations for Community Services (pp. 351–376). Springer Nature Switzerland Cham.

SEIDENFAD, K., GREINER, M., BIERMANN, J., LECHNER, U. (2024). Blockchain-based monitoring, reporting and verification of GHG emissions on the network edge – a system integration study in the artisan coffee industry. In: 2024 IEEE/SICE International Symposium on System Integration (SII) (pp. 1227–1228).

SEILER, A., LECHNER, U., STRUSSENBERG, J., HOFBAUER, S. (2024). Operation Raven: Design of a cyber security incident response game. In: International Conference on Innovations for Community Services (pp. 337–347). Springer Nature Switzerland Cham.

WURZENBERGER, M., KRENN, S., LANDAUER, M., SKOPIK, F., PERNER, C., LÖTJÖNEN, J., PÄIJÄNEN, J., GARDIKIS, G., ALABASIS, N., SAKERMAN, L., et al. (2024). NEWSROOM: Towards automating cyber situational awareness processes and tools for cyber defence. In: Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1–11).

ZHAO, T., GASIBA, T., LECHNER, U., PINTO-ALBUQUERQUE, M. (2024). Thriving in the era of hybrid work: Raising cybersecurity awareness using serious games in industry trainings. Journal of Systems and Software, 210, 111946.

ZHAO, T., GASIBA, T., LECHNER, U., PINTO-ALBUQUERQUE, M., ONGU, D. (2024). COPYCAT: Applying serious games in industry for defending supply chain attack. In: International Conference on Innovations for Community Services (pp. 321–336). Springer Nature Switzerland Cham.

ZHAO, T., ONGU, D., GASIBA, T., LECHNER, U., PINTO-ALBUQUERQUE, M. (2024). A deep dive into CATS evaluator algorithm: Quantification of the probability in serious game cloud security defense scenarios. In 2024 36th International Conference on Software Engineering Education and Training (CSEE&T) (pp. 1–5). IEEE.

FORSCHUNGSPROJEKTE

LIONS – Ledger Innovation and Operation Network for Sovereignty

Das interdisziplinär ausgerichtete Forschungsprojekt baut eine Plattform für die Erforschung von Distributed-Ledger-Technologie als eine Technologie der Digitalisierung zur Erhöhung von Resilienz und digitaler Souveränität auf. Dazu gehört unter anderem Weiterentwicklung von verteiltem und souveränen Identity Management unter Sicherheits- und Schutzaspekten in Anwendungsbereichen wie IoT, Web-Anwendungen und eGovernance.

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 01/2021–12/2026

MESSEN, TAGUNGEN, SEMINARE

LIONS Symposium am 05. November 2024 an der Universität der Bundeswehr München: https://www.unibw.de/lions/symposium

Prof. Dr.-Ing. Mark Manulis

Forschungsgruppe Privacy and Applied Cryptography Lab

PUBLIKATIONEN

LI, N., LI, Y., MANULIS, M., TIAN, Y., YANG, G.: Practical and secure policy-based chameleon hash for redactable blockchains. The Computer Journal 2024.

MANULIS, M., NGUYEN, J.: Fully Homomorphic Encryption beyond IND-CCA1 Security: Integrity through Verifiability. EUROCRYPT 2024

MENG, L., CHEN, L., TIAN, Y., MANULIS, M.: FABESA: Fast (and Anonymous) Attribute-Based Encryption under Standard Assumption. ACM CCS 2024.

MENG, L., CHEN, L., TIAN, Y., MANULIS, M., LIU, S.: FEASE: Fast and Expressive Asymmetric Searchable Encryption. USENIX Security Symposium 2024.

FORSCHNUNGSPROJEKTE

LIONS – Ledger Innovation and Operation Network for Sovereignty

Das interdisziplinär ausgerichtete Forschungsprojekt baut eine Plattform für die Erforschung von Distributed-Ledger-Technologie als eine Technologie der Digitalisierung zur Erhöhung von Resilienz und digitaler Souveränität auf. Dazu gehört unter anderem Weiterentwicklung von verteiltem und souveränen Identity Management unter Sicherheits- und Schutzaspekten in Anwendungsbereichen wie IoT, Web-Anwendungen und eGovernance.

Gefördert durch: dtec.bw – Zentrum für Digitalisierungs- und Technologieforschung der Bundeswehr. dtec.bw wird von der Europäischen Union – NextGenerationEU finanziert.
Laufzeit: 01/2025–12/2026

PiQASO – Post-Quantum Cryptography As-a-Service for Common Transmission Systems and Infrastructures

Ziel sind optimierte Krypto-Services für Schlüsselkapselung, Signaturen, Schlüsselaustausch, Autorisierung, Identitätsmanagement sowie sichere Berechnungen. Bereitgestellt werden soll eine Public Key Infrastruktur, die gegen Quantencomputerangriffe robust und ohne Spezialhardware integrierbar ist. So sollen quantensichere Verschlüsselungsdienste für bestehende Systeme ermöglicht werden.

Gefördert durch: EU Horizon Europe
Laufzeit: 01/2025–12/2027

SECANT – Security and Privacy Protection in Internet of Things Devices

Im Projekt wird eine innovative Plattform zur Risikobewertung der Cybersicherheit entwickelt, um kaskadierende Cyberbedrohungen zu bekämpfen und die Privatsphäre und den Datenschutz im gesamten vernetzten Ökosystem der IKT zu erhöhen. PACY Lab arbeitet an kryptographischen Protokollen, die sich auf eine Blockchain-Technologie stützen und eine Suche auf verschlüsselten sensiblen Daten ermöglichen.

Gefördert durch: EU H2020
Laufzeit: 09/2021 – 08/2024
Teilnahme über University of Surrey, Vereinigtes Königreich

LEHRVERANSTALTUNGEN

55481 **Modern Cryptography (WT)**

55482 **Research Trends in Cryptography (WT)**

55631 **Private Data Processing (FT)**

55632 **Private Authentication and Messaging (HT)**

55633 **Privacy Enhancing Cryptography in Practice (FT + HT)**

WEITERE FUNKTIONEN

- Associate Editor für IEEE Transactions on Information Forensics and Security (IEEE TIFS)
- Associate Editor für International Journal of Information Security (IJIS), Springer
- Gastprofessor an der University of Surrey, Vereinigtes Königreich

Mitglied des Programmkomitees

- EUROCRYPT 2024
- PKC 2025

Juniorprof. Dr. Maximilian Moll

Operations Research – Prescriptive Analytics

PUBLIKATIONEN

MILANI, R., MOLL, M., DE LEONE, R.(2024). Detection of Important States through an Iterative Q-value Algorithm for Explainable Reinforcement Learning. Proceedings of the 57th Hawaii International Conference on System Sciences, pp. 1401–1408.

PHAM, T. S., NISTOR, M. S., CAO, L., GERSCHBERGER, M., MOLL, M. (2024). Machine Learning in Vehicle Travel Time Estimation: A Brief Technological Perspective and Review. Proceedings of the 57th Hawaii International Conference on System Sciences, pp. 1409–1414.

FORSCHUNGSPROJEKTE

Digitaler Arbeitsplatz und Mensch-KI-gestützte Ausbildung durch Berührung

In Anbetracht der Bedeutung künstlicher Assistenzsysteme untersucht das Projekt deren Einbeziehung in den Trainingsprozess. Dies geschieht aus der Perspektive des menschlichen Lernens (Kognitionswissenschaften), des maschinellen Lernens (Computerwissenschaften) und durch die Analyse des Vertrauens in KI-Partner (Philosophie).

Gefördert durch: Bayerisches Forschungsinstitut für Digitale Transformation (bidt)
Laufzeit: 04/2022–03/2024

LEHRE

10361 **Operations Research (WT)**

14901 **Ausgewählte Kapitel des Operations Research und der Entscheidungstheorie (HT)**

29941 **Ausgewählte Kapitel des Data-driven Optimization (HT)**

22942 **Quantum Machine Learning & Optimization (FT)**

3396 **Data Mining (WT)**

WEITERE FUNKTIONEN

- Fellow der der Bayerischen Wissenschaftsallianz für Friedens-, Konflikt- und Sicherheitsforschung
- Koordinator Hochbegabtenförderung an der Universität der Bundeswehr München
- Arbeitsgruppenleiter „Simulation und Optimierung komplexer Systeme“, Deutsche Gesellschaft für OR

Prof. Dr. Eirini Ntoutsi

Open Source Intelligence

PUBLIKATIONEN

ALVAREZ, J. M., COLMENAREJO, A. B., ELOBAID, A., FABBRIZZI, S., FAHIMI, M., FERRARA, A., GHODSI, S., MOUGAN, C., PAPAGEORGIOU, I., REYERO, P., et al. (2024). Policy advice and best practices on bias and fairness in AI. Ethics and Information Technology, 26(2):31.

GHODSI, S., SEYEDI, S. A., NTOUTSI, E. (2024). Towards cohesion-fairness harmony: Contrastive regularization in individual fair graph clustering. In: Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD), pp. 284–296. Springer.

HUUK, J., DHINGRA, A., NTOUTSI, E., DENKENA, B. (2024). Shape error prediction in 5-axis machining using graph neural networks. In: 18th CIRP ICME Conference on Intelligent Computation in Manufacturing Engineering.

KUMAR, V., NTOUTSI, E., RAJAWAT, P. S., MEDDA, G., RECUPERO, D. R. (2024). Unlocking LLMs: Addressing scarce data and bias challenges in mental health. In: 1st International Conference on Natural Language Processing and Artificial Intelligence for Cyber Security (NL-PAICS).

PANAGIOTOU, E., HEURICH, M., LANDGRAF, T., NTOUTSI, E. (2024a). TABCF: Counterfactual explanations for tabular data using a transformer-based VAE. In Proceedings of the 5th ACM International Conference on AI in Finance (ICAIF), pp. 274–282.

PANAGIOTOU, E., ROY, A., NTOUTSI, E. (2024b). Synthetic tabular data generation for class imbalance and fairness: A comparative study. In: BIAS Workshop co-located with ECML PKDD 2024.

QIAN, H., PANAGIOTOU, E., PENG, M., NTOUTSI, E., KANG, C., MARX, S. (2024). A novel dataset and feature selection for data-driven conceptual design of offshore jacket substructures. Ocean Engineering, 303:117679.

RAMANAIK, C. K., ROY, A., NTOUTSI, E. (2024a). Adversarial robustness of vaes across intersectional subgroups. In: BIAS Workshop co-located with ECML PKDD 2024.

RAMANAIK, C. K., WILLMANN, A., SUAREZ CARDONA, J.- E., HANFELD, P., HOFFMANN, N., HECHT, M. (2024b). Ensuring topological data-structure preservation under autoencoder compression due to latent space regularization in Gauss–Legendre nodes. Axioms, 13(8):535.

ROY, A., KOUTLIS, C., PAPADOPOULOS, S., NTOUTSI, E. (2024). Fairbranch: Mitigating bias transfer in fair multi-task learning. In: 2024 International Joint Conference on Neural Networks (IJCNN), pp. 1–8. IEEE.

SWATI, S. MLADENÍC, D. (2024). LLNewsBias: A multilingual news dataset for lifelong learning. In: Proceedings of the 27th International Multiconference Information Society (IS) 2024, volume C, pp. 97–100.

SWATI, S., ROY, A., NTOUTSI, E. (2024). Exploring Fusion Techniques in Multimodal AI-Based Recruitment: Insights from FairCVdb. In: Third European Workshop on Algorithmic Fairness (EWAF).

FORSCHUNGSPROJEKTE

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

Das Projekt zielt darauf ab, ein Framework für eine lernbasierte 5-Achsen-Kompensation von Formfehlern in Fräsprozessen zu erforschen, basierend auf einer prozessparallelen Materialabtragssimulation und fortschrittlichen maschinellen Lernstrategien (ML). Darüber hinaus soll die Fähigkeit des Wissenstransfers zwischen verschiedenen Werkstückgeometrien, Fräswerkzeugen und Maschinenwerkzeugen zur Verbesserung der Prozessplanung untersucht werden.

Gefördert durch: DFG
Laufzeit: 04/2021–05/ 2025

MAMMoth – Multi-Attribute, Multimodal Bias Mitigation in AI Systems

MAMMoth konzentriert sich auf die Identifikation und Bekämpfung von (multi-) Diskriminierung in KI-Systemen in Bezug auf verschiedene geschützte Merkmale. Dabei werden sowohl konventionelle tabellarische Daten als auch komplexere Netzwerk- und Bilddaten berücksichtigt. Die entwickelten Lösungen werden in drei relevanten Anwendungsbereichen pilotgetestet: a) Finanz- und Kreditvergabeverfahren, b) Identitätsprüfungssysteme und c) akademische Bewertung.

Gefördert durch: EU
Laufzeit: 09/2022–08/2025

STELAR – Spatio-Temporal Linked Data Tools for the Agri-Food Data Space

STELAR wird ein innovatives Knowledge Lake Management System (KLMS) entwerfen, entwickeln, evaluieren und präsentieren, um einen ganzheitlichen Ansatz für FAIR-Daten (auffindbar, zugänglich, interoperabel, wiederverwendbar) und KI-bereite Daten (hochwertig, zuverlässig gekennzeichnet) zu unterstützen und zu erleichtern. Dieses System wird in vielfältigen, praxisnahen Anwendungsfällen im Agrar- und Lebensmitteldatenbereich pilotgetestet.

Gefördert durch: EU
Laufzeit: 09/2022–08/2025

LEHRE

2319 **Artificial Intelligence (WT)**

2320 **Responsible Artificial Intelligence (HT)**

2534 **Machine Learning (FT)**

MESSEN, TAGUNGEN, SEMINARE

- European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases (ECML PKDD 2024)(Program Co-Chair)
- 1st Workshop on Responsible AI, co-located with Hellenic Conference on Artificial Intelligence (SETN)(Co-Organizer)
- European Summer School on Artificial Intelligence (ESSAI) – Course on Fairness and Explainability: Models, Measurements and Mitigation Strategies
- AI@LMU lecture series – Guest lecture on AI bias and fairness
- INDOR lecture sereis "Maschinen wie wir", UniBwM – Invited talk: Bias in AI and why we should care?
- 2nd EMERGENCY-VRD workshop on Moral and Legal Aspects of Autonomous Systems, UniBwM – Invited talk: Technical aspects of autonomous systems
- Workshop on fostering a fair algorithmic environment: Presenting the MAMMOth AI bias solutions, Complexity Science Hub, Vienna – Invited talk: The multifaced nature of bias in AI
- Workshop on unmasking biases in data collection, University of Toronto (online) – Invited talk: Bias and discrimination in AI systems
- Panel on Weaving An Ethical and Human-Centric Web, International Conference on Web Engineering (ICWE), Tampere, Finland
- Panel discussion: AI vs Human at Versus Festival, Austria
- Summer workshop on KI in Aktion: Chancen und Grenzen lernfähiger Maschinen, UniBw M

WEITERE FUNKTIONEN

- Member of the program committee Master's in Cyber Security
- Faculty representative for the Fakultätentag Informatik (FTI)
- Expert for the European Commission
- Expert for the Luxembourg National Research Fund
- Expert for the Swedish Research Council
- External advisory board member for the EU project ExtremeXP
- Co-Affiliation L3S Research Center, Hannover.

Mitglied des Programmkomitees

- International Joint Conference on Artificial Intelligence (IJCAI)
- ACM Conference on Fairness, Accountability, and Transparency (FAccT)

Prof. Dr. Stefan Pickl

Operations Research – Forschungsgruppe COMTESSA

LEHRE

10245 **Praktikum Operations Research – Entscheidungsunterstützung (WT + FT + HT)**

10252 **Seminar Ausgewählte Kapitel des Operations Research I (WT + FT + HT)**

10371 **Einführung in die Wirtschaftsinformatik (HT)**

10372 **Grundlagen der Informations- und Kommunikationstechnik (HT)**

10401 **Einführung in Business Intelligence (FT)**

12311 **Data Mining und IT-basierte Entscheidungsunterstützung (WT)**

12325 **Praktikum Operations Research – Entscheidungsunterstützung II (WT + FT + HT)**

12326 **Seminar Ausgewählte Kapitel des Operations Research II (FT)**

2038-V1 **KI und datenbasierte Optimierung (FT)**

3481-V1 **Datenwissenschaft und -analyse (FT)**

ICE Lecture 2024

Intelligence College in Europe together with Gehard Conrad and Maximilian Moll „Cyber and its Implications for Intelligence, Analysis and Decision Making"

WEITERE FUNKTIONEN

- Vize-Präsident Deutsches Komitee für Katastrophenvorsorge DKKV
- Beiratsvorsitzender der Deutschen OR Gesellschaft
- Mitglied des DEU NATO SAS Panel
- Mitglied der Munich Aerospace
- Kuratoriumsmitglied der Hessischen Schülerakademie
- Präsidiumsmitglied des VOICE – Bundesverband der IT-Anwender e.V.
- Mitglied der Deutschen Akademie für Technikwissenschaften ACATECH

Prof. Dr. Daniel Slamanig

Kryptologie

PUBLIKATIONEN

ABDOLMALEKI, B., GLAESER, N., RAMACHER, S., SLAMANIG, D.: Circuit-Succinct Universally-Composable NIZKs with Updatable CRS. 37th IEEE Computer Security Foundations Symposium, CSF 2024, Enschede, Netherlands, July 8–12, 2024, IEEE Computer Society Digital Library.

CAPUANO, L., MULA, M., TERRACINI, L.: Quarternionic p-adic continued fractions. Communications in Algebra, 2024, Taylor & Francis.

CELI, S., GRIFFY, S., HANZLIK, L., PEREZ KEMPNER, O., SLAMANIG, D.: SoK: Signatures With Randomizable Keys. 28th International Conference on Financial Cryptography and Data Security – FC 2024.

CINI, V., RAMACHER, S., SLAMANIG, D., STRIECKS, C., TAIRI, E.: (Inner-Product) Functional Encryption with Updatable Ciphertexts. Journal of Cryptology, 37, 8, 2024, Springer.

DERLER, D., SAMELIN, K., SLAMANIG, D.: Bringing Order to Chaos: The Case of Collision-Resistant Chameleon-Hashes. Journal of Cryptology, 37, 29, 2024, Springer.

GARCÍA-RODRÍGUEZ, J., KRENN, S., SLAMANIG, D.: To Pass or Not to Pass: Privacy-Preserving Physical Access Control. In: Computers & Security, 2024, Elsevier.

GRIFFY, S., LYSYANSKAYA, A., MIR, O., PEREZ KEMPNER, O., SLAMANIG, D.: Delegatable Anonymous Credentials From Mercurial Signatures With Stronger Privacy. 30th Annual International Conference on the Theory and Application of Cryptology and Information Security – ASIACRYPT 2024.

MITROKOTSA, K., MUKHERJEE, S., SEDAGHAT, M., SLAMANIG, D., TOMY, J.: Threshold Structure-Preserving Signatures: Strong and Adaptive Security under Standard Assumptions. 27th IACR International Conference on Practice and Theory of Public-Key Cryptography – PKC 2024.

MULA, M., MURRU, N., PINTORE, F.: On Random Sampling of Supersingular Elliptic Curves. Annali di Matematica Pura ed Applicata (1923 -), 2024, Springer.

SKOPIK, F., BONITZ, A., SLAMANIG, D., KIRSCHNER, M., HACKER, W.: Towards a single device for multiple security domains. Journal of Universal Computer Science 30(5): 563-589.

LEHRE

10251 **Seminar Kryptologie (Bachelor) (FT + HT)**

39311 **Introduction to Post-Quantum Cryptography (HT)**

55011 **Seminar Kryptologie (Master) (FT + HT)**

MESSEN, TAGUNGEN, SEMINARE

- 43rd Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2024), Zürich
- Workshop on Foundations and Applications of Zero-Knowledge Proofs, Edinburgh
- Leuven Isogeny Days 5, Leuven
- Leuven I-sage-ny Days, Leuven
- Cifris 24 Workshop on Number Theory and Cryptography (NTC24), Rom
- QSI PQC Spring School 2024, Porto
- Math PQC Conference, Budapest
- Young Researcher Crypto Seminar Spring 2024, Paderborn

WEITERE FUNKTIONEN

- Gutachter für die Europäische Kommission
- Gutachter für die Deutsche Forschungsgemeinschaft (DFG)
- Academic Editor für IET Information Security
- Editor fr Journal of Universal Computer Science
- Keynote Speaker an der 19th IFIP Summer School on Privacy and Identity Management 2024
- Invited Speaker am "AB+ – Attributes and Blindness" Workshop co-located mit der EUROCRYPT 2024
- Teilnahme am Panel "Cyber Security", Technologie- und Innovationsforum Salzburg (salz21), Salzburg

Mitglied des Programmkomitees

- 44th Annual International Cryptology Conference (CRYPTO 2024)
- 31st Annual ACM Conference on Computer and Communications Security (ACM CCS 2024)
- 22nd International Conference on Applied Cryptography and Network Security (ACNS 2024)
- 30th Australasian Conference on Information Security and Privacy (ACISP 2024)
- 39th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2024)
- 18th International Conference on Provable and Practical Security (ProvSec 2024)
- 19th International Workshop on Security (IWSEC 2024)
- 11th ACM Asia Public-Key Cryptography Workshop (APKC 2024)
- 24th Central European Conference on Cryptology (CECC 2024)

Prof. Dr. Gunnar Teege

Formale Methoden für die Sicherheit von Dingen (FOMSET)

LEHRE

1016 **Einführung in Betriebssysteme (WT)**

1026 **Verteilte Systeme (HT)**

1031 **Virtualisierung (HT)**

5505 **Betriebssystemsicherheit (FT)**

WEITERE FUNKTIONEN

- Mitglied im Prüfungsausschuss Master Cybersicherheit
- Mitglied in der Studiengangskommission Master Cybersicherheit
- Mitglied im Prüfungsausschuss Informatik
- Mitglied im Prüfungsausschuss Wirtschaftsinformatik

Prof. Dr. Arno Wacker

Datenschutz und Compliance

PUBLIKATIONEN

KLEINE, S., MÜLLER, K.: On the growth of the Jacobians in $\mathbb{Z}_p^l$-voltage covers of graphs, Algebraic Combinatorics, Volume 7 (2024) no. 4, pp. 1011–1038. doi: 10.5802/alco.366.

SCHLOLAUT, M., KIESELMANN, O., WACKER, A.: Comparing Nudges and Deceptive Patterns at a Technical Level. 2024 Mobilizing Research and Regulatory Action on Dark Patterns and Deceptive Design Practices (DDPCHI 2024), Honolulu, HI, USA. https://ceur-ws.org/Vol-3720/paper12.pdf.

LEHRE

3480 **Sichere Netze und Protokolle (FT)**

55011 **Seminar Vulnerabilities and Attack Vectors (FT + HT)**

55041 **Datenschutz (WT)**

55042 **Privacy Enhancing Technologies (WT)**

55061 **Einführung in die Kryptographie (WT)**

55062 **Kryptoanalyse**

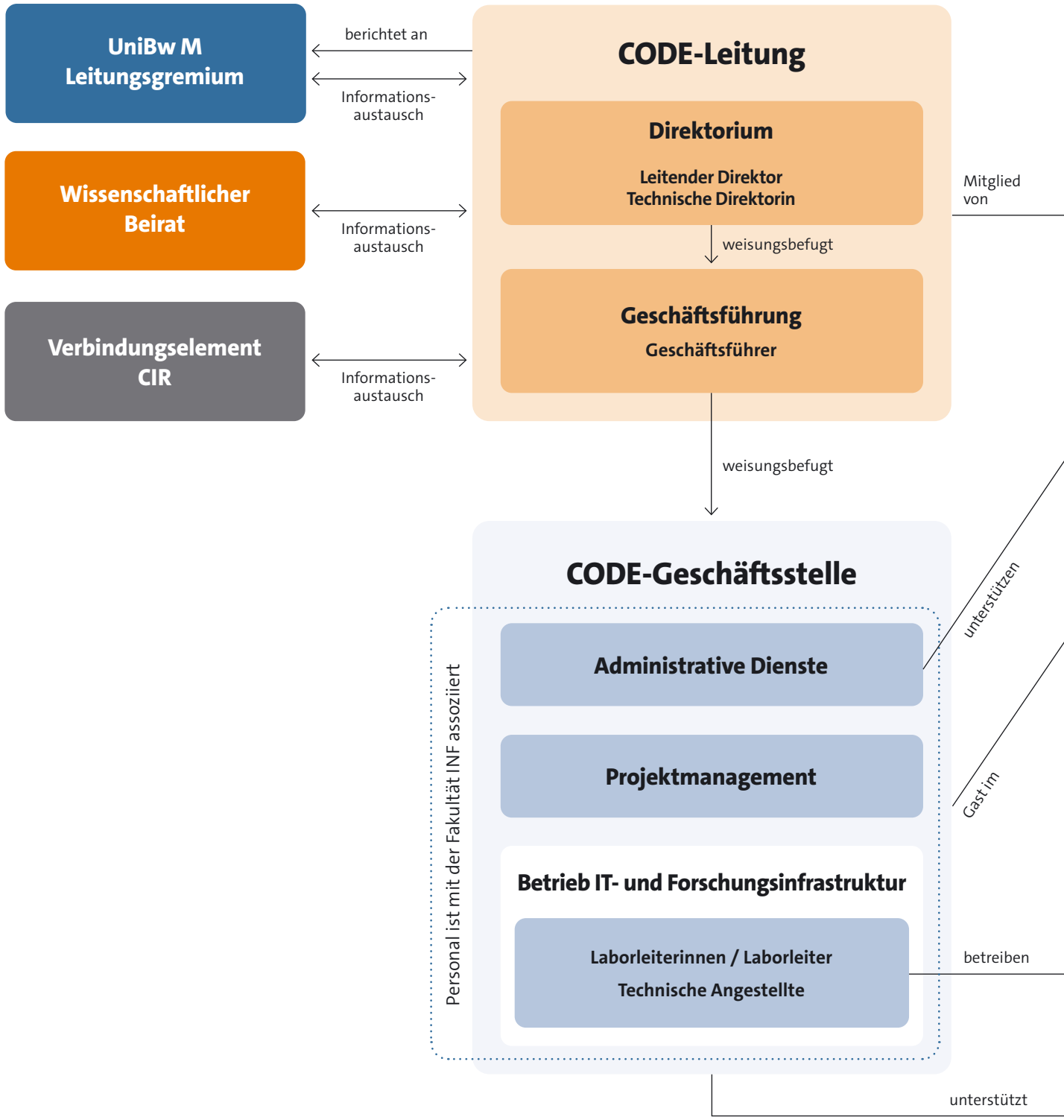
55091 **Penetration Testing (HT)**

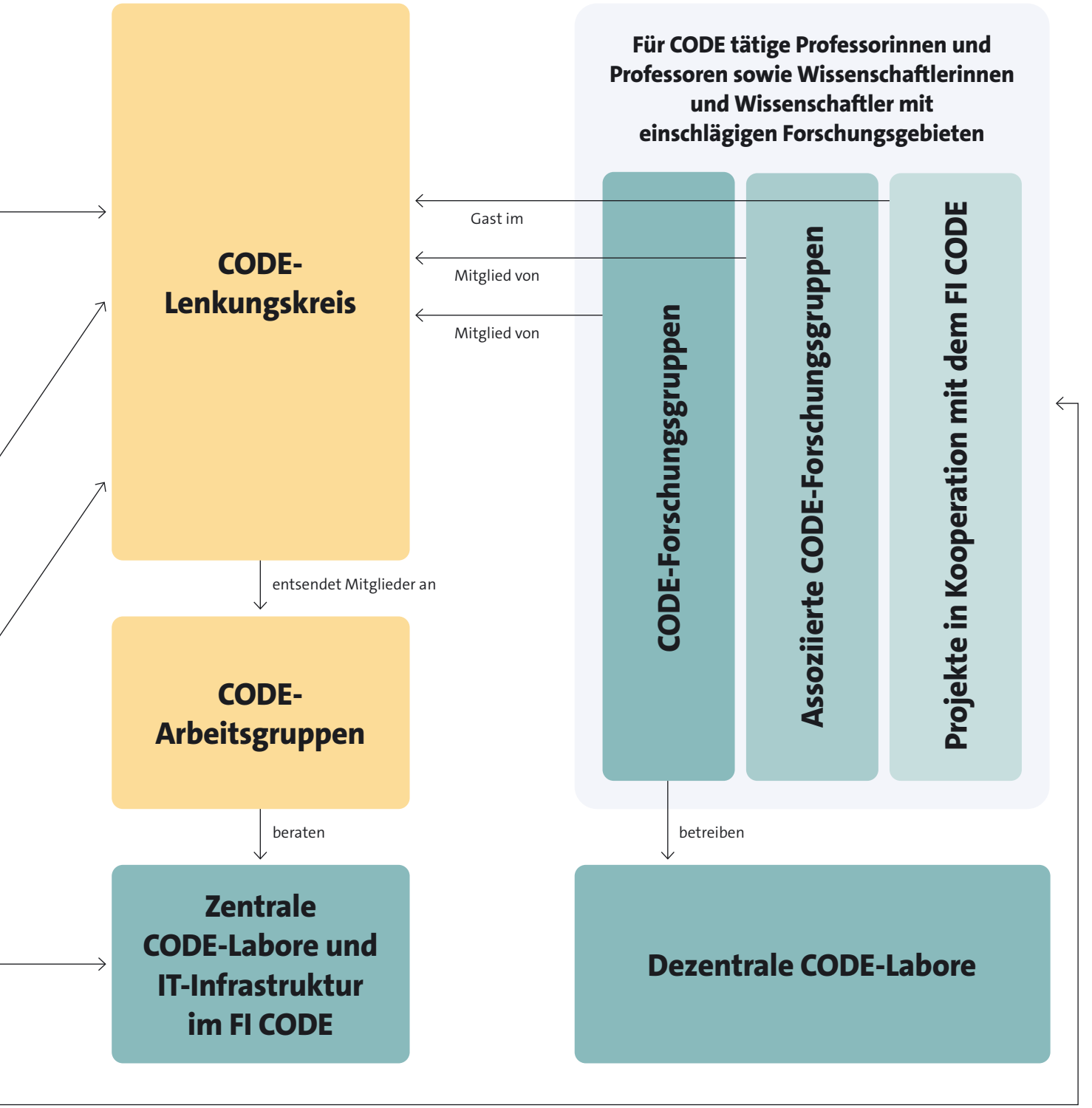
55093 **Praktikum Penetration Testing (WT + FT)**

WEITERE VERANSTALTUNGEN

- 24.04.2024, Vortrag bei der Innovationsrunde der EAD Energieabrechnungs-Systeme GmbH in Erfurt
  - Mathias Schlolaut gab einen Einblick zu Passwörtern und Phishingangriffen, ergänzt durch praktische Beispiele.
- 28.10.2024, Tagung "Algebraic Number Theory – A workshop for young researchers" an der Universität der Bundeswehr München
  - Sören Kleine war Mitorganisator der Veranstaltung, bei der die überwiegend jungen Teilnehmenden die Gelegenheit hatten, ihre Forschung einem breiteren Publikum vorzustellen.

Organisation des FI CODE




CODE-Lenkungskreis
Für CODE tätige Professorinnen und Professoren sowie Wissenschaftlerinnen und Wissenschaftler mit einschlägigen Forschungsgebieten
Gast im
Mitglied von
Mitglied von
CODE-Forschungsgruppen
Assoziierte CODE-Forschungsgruppen
Projekte in Kooperation mit dem FI CODE
entsendet Mitglieder an
CODE-Arbeitsgruppen
beraten
betreiben
Zentrale CODE-Labore und IT-Infrastruktur im FI CODE
Dezentrale CODE-Labore

So erreichen Sie uns

Forschungsinstitut Cyber Defence und Smart Data (CODE)
Universität der Bundeswehr München
Carl-Wery-Straße 18
81739 München

code@unibw.de
+49 89 6004 7300
www.unibw.de/code

LinkedIn: Forschungsinstitut Cyber Defence (CODE)
YouTube: Forschungsinstitut Cyber Defence

Lageplan

Impressum

HERAUSGEBER

Prof. Dr. Wolfgang Hommel,
Prof. Dr. Michaela Geierhos,
Marcus Knüpfer,
Benjamin Bellgrau

Forschungsinstitut CODE
Universität der Bundeswehr München
Carl-Wery-Str. 18
81739 München

LEITUNG DES FI CODE

Prof. Dr. Wolfgang Hommel,
Leitender Direktor

Prof. Dr. Michaela Geierhos,
Technische Direktorin

Marcus Knüpfer, M. Sc.,
Geschäftsführer

PROFESSUREN AM FI CODE

Prof. Dr. Florian Alt,
Professor für Usable Security and Privacy (bis 10/2024)

Prof. Dr. Harald Baier,
Professor für Digitale Forensik

Prof. Dr. Stefan Brunthaler,
Professor für sichere Software-Entwicklung

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

Prof. Dr. Gabi Dreo Rodosek,
Professorin für Kommunikationssysteme und Netzsicherheit

Prof. Dr. Michaela Geierhos,
Professorin für Data Science

Prof. Dr. Marta Gomez-Barrero,
Studiendekanin der Fakultät für Informatik an der UniBw M,
Professorin für Maschinelles Lernen

Prof. Dr. Udo Helmbrecht,
Honorarprofessor am FI CODE

Prof. Dr. Wolfgang Hommel,
Dekan der Fakultät für Informatik an der UniBw M,
Professor für IT-Sicherheit von Software und Daten

Prof. Dr. Ulrike Lechner,
Professorin für Wirtschaftsinformatik

Prof. Dr.-Ing. Mark Manulis,
Prodekan der Fakultät für Informatik an der UniBw M,
Professor für Privacy

Juniorprof. Dr. Maximilian Moll,
Juniorprofessor für Operations Research – Prescriptive Analytics

Prof. Dr. Eirini Ntoutsi,
Professorin für Open Source Intelligence

Prof. Dr. Stefan Pickl,
Professor für Operations Research

Prof. Dr. Daniel Slamanig,
Professor für Kryptologie

Prof. Dr. Gunnar Teege,
Professor für Verteilte Systeme

Prof. Dr. Arno Wacker,
Professor für Datenschutz und Compliance

MITGLIEDER DES BEIRATS (IM JAHR 2024)

Aus der Fakultät für Informatik der Universität der Bundeswehr München

Prof. Klaus Buchenrieder, PhD

Prof. Dr. Ulrike Lechner

Prof. Dr.-Ing. Helmut Mayer

Prof. Dr. Oliver Rose

Prof. Dr. Gunnar Teege

Weitere Mitglieder

Wolfgang Sachs,
Referatsleiter CIT I 2, Bundesministerium der Verteidigung

Norbert Gaus,
Executive Vice President der Siemens AG (bis 06/2024)

Dr. Ralf Wintergerst,
Vorsitzender der Geschäftsführung von
Giesecke+Devrient GmbH (bis 06/2024)

Dr.-Ing. Christian Keimel,
Airbus Defence and Space (ab 07/2024)

Dr. Kai Martius,
Chief Technology Officer, secunet Security Networks AG
(ab 07/2024)

Prof. Dr. Johann Pongratz,
TU Dortmund

REDAKTION & KOORDINATION

Benjamin Bellgrau, M. Sc.,
Referent für Öffentlichkeitsarbeit

ART DIRECTION

Tausendblauwerk, Agentur für Gestaltung
Michael Berwanger

www.tausendblauwerk.de

LEKTORAT

Dr. Michelle Ruth Büscher,
Fachübersetzerin/Lektorin

DRUCK

druckhaus köthen

https://koethen.de

REGULARIEN

Redaktionsschluss: März 2025

Titelabbildung: Adobe Stock / Alexey

ISBN: 978-3-943207-91-0 | ISSN: 2748-8780

Auch erschienen als elektronische Publikation
(ISBN: 978-3-943207-92-7 | ISSN: 2748-8799)
sowie in englischer Sprache
(ISBN: 978-3-943207-93-4 | ISSN: 2748-9485).


der Bundeswehr
Universität München
FI
CODE
Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München